Microsoft

Microsoft Windows Server® 2012 R2

ХРАНЕНИЕ, БЕЗОПАСНОСТЬ, СЕТЕВЫЕ КОМПОНЕНТЫ

Уильям Р. Станек

Справочник администратора

РУССКАЯ РЕДАКЦИЯ Microsoft bhv®

Microsoft

Windows Server 2012 R2: Storage, Security, & Networking

Pocket Consultant

William R. Stanek
Author and Series Editor

Microsoft Windows Server® 2012 R2

ХРАНЕНИЕ, БЕЗОПАСНОСТЬ, СЕТЕВЫЕ КОМПОНЕНТЫ

Справочник администратора

Уильям Р. Станек

РУССКАЯ РЕДАКЦИЯ

bhv®

2015

УДК 004.451
ББК 32.973.26-018.2
С76

Станек У. Р.

С76 Microsoft Windows Server® 2012 R2: хранение, безопасность, сетевые компоненты. Справочник администратора: Пер. с англ. — М.: Издательство «Русская редакция»; СПб.: «БХВ-Петербург», 2015. — 416 с.: ил. — (Справочник администратора)

ISBN 978-5-7502-0436-6 («Русская редакция»)
ISBN 978-5-9775-3558-8 («БХВ-Петербург»)

Данная книга — краткий и исчерпывающий справочник по администрированию Windows Server 2012 R2. Описаны управление файловыми системами и дисками, настройка носителей данных, общий доступ к данным и избыточность, безопасность данных и аудит, улучшение безопасности компьютера, управление пользователями и компьютерами с помощью групповой политики, управление TCP/IP-сетью, запуск DCHP-клиентов и серверов, оптимизация DNS, администрирование сетевых принтеров и служб печати, резервное копирование и восстановление данных.

Для квалифицированных пользователей и системных администраторов

УДК 004.451
ББК 32.973.26-018.2

Уильям Р. Станек

Microsoft Windows Server® 2012 R2: хранение, безопасность, сетевые компоненты. Справочник администратора

Перевод с английского языка Дениса Колисниченко

Совместный проект издательства «Русская редакция» и издательства «БХВ-Петербург»

РУССКАЯ РЕДАКЦИЯ bhv®

Подписано в печать 28.11.14.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 33,54.
Тираж 1000 экз. Заказ №

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-0-7356-8259-7 (англ.)
ISBN 978-5-7502-0436-6 («Русская редакция»)
ISBN 978-5-9775-3558-8 («БХВ-Петербург»)

Оглавление

Благодарности

Моим читателям — благодарю вас за то, что были со мной в течение всех этих лет и всех этих книг. Для меня было большой честью предоставлять вам "услуги карманного справочника".

Моей жене — благодарю тебя за то, что на протяжении многих книг, многих миллионов слов и многих тысяч страниц была рядом со мной, помогая и поддерживая, создавая домашний уют в каждом месте, в котором мы жили.

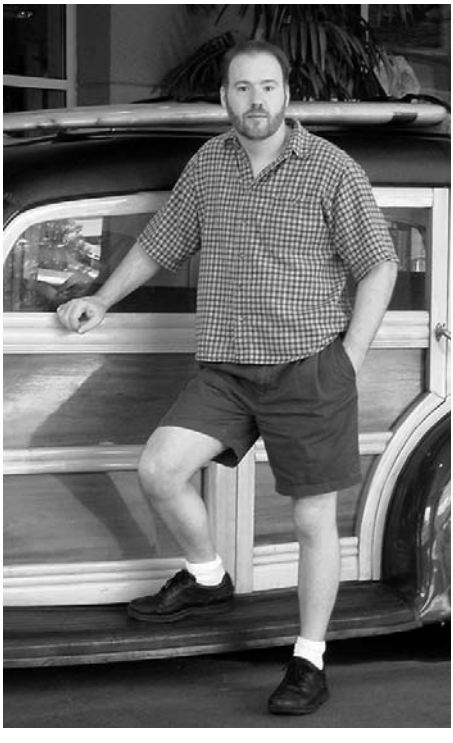
Я также благодарю моих детей, за их помощь видеть мир по-новому, за их исключительное терпение и безграничную любовь, а также за то, что они превращают каждый день в приключение.

Также благодарю Анну, Карину, Мартина, Люсинду, Джулиану и многих других, которые помогали мне как в малом, так и в большом.

Особая благодарность моему сыну Уиллу за то, что он не только устанавливал и обслуживал всестороннюю лабораторную поддержку для всех моих книг, начиная с "Microsoft Windows 8. Справочник администратора", но также вычитывал все эти книги.

Уильям Р. Станек

Об авторе



УИЛЬЯМ СТАНЕК (William Stanek, **www.williamstanek.com**) — автор отмеченных наградами книг и редактор бестселлерной серии книг "Карманный справочник" (Pocket Consultant). Уильям является одним из мировых экспертов по передовым технологиям и имеет за плечами более 20 лет практического опыта работы в области продвинутого программирования и разработки. На протяжении многих лет он своими практическими советами помогал миллионам программистов, разработчиков и сетевых инженеров по всему миру. В 1996 году журнал "The Olympian" назвал его "одним из движителей будущего", и Уильям доказал, что он действительно является таковым, написав более чем за 20 лет множество книг в области продвинутых технологий. В 2013 году вышла 150-я книга Уильяма, а его работы прочитали более чем 7,5 млн человек. Среди последних книг Уильяма такие как "Exchange Server 2013: Configuration & Clients", "Windows Server 2012 R2 Pocket Consultant: Essentials & Configuration и Windows Server 2012 Inside Out".

Уильям участвует в разработке коммерческих интернет-проектов с 1991 года. Свой основной опыт в бизнесе и технологии он накопил за 11 с лишним лет службы в армии. Он обладает обширным опытом в области разработки серверных технологий, шифрования и интернет-решений. Он является автором многих технических докладов и учебных курсов по широкому кругу предметов. Его часто приглашают в качестве эксперта и консультанта в предметной области.

Уильям обладает степенью магистра информационных систем и имеет диплом бакалавра информатики. Он гордится своей службой в армии во времена конфликта в Пер-

сидском заливе в качестве члена экипажа самолета радиоэлектронного противоборства. Он участвовал во многих боевых заданиях в Ираке и был награжден девятью медалями за свою военную службу, включая одну из наивысших наград военно-воздушных сил США — крест "За летные боевые заслуги". В настоящее время он проживает со своей женой и детьми на тихоокеанском северо-западе в США.

Недавно Уильям снова начал увлекаться природным туризмом. Когда он не работает над очередной книгой, то совершает пешие прогулки на лоне природы, велосипедные поездки, турпоходы с ночевкой, путешествует или странствует со своей семьей в поисках приключений.

Уильяма можно найти на Twitter под ником WilliamStanek и на Facebook по адресу **www.facebook.com/William.Stanek.Author**. Посетив веб-сайт **www.Pocket-Consultant.com**, вы получите возможность познакомиться с другими работами Уильяма.

Введение

Данная книга призвана стать кратким и полезным ресурсом для администраторов Windows, разработчиков, программистов и всех тех, кому нужно использовать средства хранения, сети и защиту операционной системы Windows Server 2012 R2. Это руководство по ресурсам, которое всегда будет на вашем столе. В книге рассмотрены все основные задачи. Поскольку книга является именно компактным справочникам, вам не придется пробираться через сотни страниц посторонней информации, чтобы найти нужные сведения. Вместо этого вы получите точные инструкции того, что следует сделать.

Короче говоря, предполагается, что эта книга станет единственным ресурсом, с которым вы будете консультироваться при настройке Windows Server 2012 R2. В ней внимание читателей концентрируется на параметрах конфигурации, часто используемых задачах, реальных примерах. Одна из целей этой книги — предоставить читателю как можно больше информации, чтобы сделать ее ценным ресурсом, и представить книгу в компактной и удобной для просмотра форме.

Любой администратор, обновивший операционную систему со старой версии Windows Server до Windows Server 2012 R2, будет приятно удивлен тонкими и существенными изменениями, которые произошли в ОС. Как и Windows Server 2012, Windows Server 2012 R2 поддерживает сенсорный пользовательский интерфейс в дополнение к традиционным мыши и клавиатуре.

Вряд ли Windows Server 2012 R2 будет устанавливаться на компьютеры с сенсорным интерфейсом, но можно управлять Windows Server 2012 R2 и с такого компьютера. Понимание принципов работы с сенсорным интерфейсом является залогом вашего успеха. Но в этой книге также рассмотрена и работа традиционным способом — с помощью мыши и клавиатуры.

При работе с компьютерами, обладающими возможностями сенсорного интерфейса, элементами на экране можно управлять такими способами, какие ранее были невозможны. В частности, можно выполнять следующие управляющие действия.

- **Нажатие.** Нажмите элемент, коснувшись его пальцем. Нажатие или двойное нажатие элемента на экране обычно эквивалентно одинарному или двойному щелчку левой кнопкой мыши.

- **Длительное нажатие.** Коснитесь пальцем элемента и удерживайте нажатие в течение 2–3 секунд. Этот жест эквивалентен щелчку правой кнопкой мыши.
- **Скольжение вниз (выбор).** Слегка проведите пальцем вниз по элементу. Этот жест выбирает элемент и открывает его контекстное меню. Если жест длительного нажатия не открывает контекстное меню элемента, попробуйте открыть его этим жестом.
- **Скольжение от края экрана.** Проведите пальцем от края экрана к центру. Скольжение от правого края открывает боковую кнопочную панель (Charms bar). А скольжение от левого края позволяет переключаться между открытыми приложениями, подобно использованию комбинации клавиш <Alt>+<Tab>. Скольжение от нижнего или верхнего края отображает команды для активного элемента.
- **Щипок.** Коснитесь элемента двумя пальцами, а затем сведите пальцы вместе. Этот жест уменьшает масштаб элемента.
- **Растяжение.** Коснитесь элемента двумя пальцами, а затем разведите пальцы. Этот жест увеличивает масштаб элемента.

Также у вас есть возможность ввести текст с использованием экранной клавиатуры. Хотя изменения в интерфейсе пользователя весьма велики, они не являются самыми значительными изменениями в операционной системе. Наиболее существенные изменения влияют на базовую архитектуру и обеспечивают много новых функций. Некоторые из этих новых функций настолько революционны, что навсегда изменяют способ, которым мы используем Windows.

В сети и в других информационных источниках имеется много сведений о Windows Server 2012 R2. Можно найти руководства, сайты-справочники, дискуссионные группы, что сделает использование Windows Server 2012 R2 проще. Однако преимущество этой книги в том, что в ней заключена и обработана большая часть необходимой информации о Windows Server 2012 R2. В этой книге есть все необходимое для настройки установки Windows Server 2012 R2, основных конфигураций этой ОС и обслуживания серверов на базе Windows Server 2012 R2.

В этой книге я рассказываю, как работают компоненты, почему они работают именно так и как настроить их в соответствии со своими потребностями. В книге представлены некоторые примеры того, как определенные компоненты могут соответствовать вашим потребностям, и как можно использовать другие компоненты для решения ваших задач. К тому же эта книга предоставляет советы и примеры, помогающие оптимизировать Windows Server 2012 R2. Она не только рекомендует, как настроить Windows Server 2012 R2, она учит, как выжать из него все и использовать все предоставляемые ним функции и опции.

В отличие от многих других книг по администрированию Windows Server 2012 R2, данная книга фокусирует внимание читателя на определенном уровне пользователя. Эта не простая книга для новичков. Независимо от того, является ли читатель начинающим администратором или настоящим профессионалом, многие концепции в этой книге будут применимы к любому уровню подготовки, и ими можно легко воспользоваться при своей установке Windows Server 2012 R2.

Для кого предназначена эта книга

Книга охватывает все редакции Windows Server 2012 R2 и предназначена для:

- действующих системных администраторов Windows;
- опытных пользователей, выполняющих некоторые обязанности администратора;
- администраторов, выполняющих обновление систем с предыдущих версий до Windows Server 2012 R2;
- администраторов, переходящих с других платформ.

Чтобы не тратить время и силы на описание элементарных операций, я вынужден сделать предположение, что у читателя есть основные навыки работы с сетью и базовое понимание Windows Server. В этой книге нет глав, посвященных объяснению архитектуры Windows Server, его запуску и завершению работы, а также агитации, почему нужно использовать Windows Server. Здесь описана конфигурация Windows Server, групповая политика, аудит, резервное копирование данных, восстановление системы и многое другое.

Я также предполагаю, что читатель знаком с командами и процедурами Windows, а также с графическим интерфейсом этой ОС. Если есть необходимость в изучении основ Windows, нужно обратиться к другим ресурсам (многие из них доступны с сайта издательства "Microsoft Press").

Организация книги

Рим строился не за один день, и эта книга не рассчитана на то, что она будет прочитана за один день, за одну неделю и даже за один месяц. В идеале, эту книгу нужно читать в собственном темпе, каждый день понемногу, в процессе работы с Windows Server 2012 R2. Данная книга состоит из 11 глав. Главы выстроены в логической последовательности, начиная от задач планирования и развертывания до задач обслуживания и настройки.

Простота организации — конек этой книги. Данная книга обладает расширенным оглавлением и обширным индексом для быстрого поиска решения. В ней есть множество ссылок, а также быстрые пошаговые процедуры, списки, таблицы, перекрестные ссылки.

Типографские соглашения

В книге используются разные способы придания тексту ясности и удобочитаемости. В частности, листинги кода, вводимые команды и значения параметров оформлены моноширинным шрифтом. Элементы графического интерфейса, например название кнопок, команд или окон, а также интернет-адреса выделены **жирным шрифтом**. Новые термины даются *курсивом*.

> ***Примечание***
>
> Групповая политика теперь состоит из политики и предпочтений. Под узлами **Конфигурация компьютера** и **Конфигурация пользователя** теперь вы найдете два узла: **Политики**

> и **Предпочтения**. Параметры общих предпочтений приводятся под узлом **Предпочтения**. При установке параметров в узле **Политики** я иногда использую записи вроде **Конфигурация пользователя\Административные шаблоны\Компоненты Windows** или указываю, что политики найдены в **Административных шаблонах** для **Конфигурации пользователя** под **Компонентами Windows**. Обе ссылки говорят, что политика устанавливается в узле **Конфигурация пользователя**, а не в узле **Конфигурация компьютера**, и могут быть найдены в узле **Административные шаблоны\Конфигурация Windows**.

Кроме этого, используются следующие текстовые вставки.

- **Рекомендации.** Описание наилучших методов для работы с расширенными возможностями настройки и обслуживания.
- **Осторожно!** Предупреждение о возможных проблемах, с которыми следует быть настороже.
- **Дополнительная информация.** Предоставление дополнительной информации по рассматриваемому предмету.
- **Примечание.** Предоставление дополнительных подробностей по определенному вопросу.
- **Практический совет.** Практические рекомендации при обсуждении сложных тем.
- **Внимание!** Выделение важных вопросов безопасности.
- **Совет.** Полезные советы или дополнительная информация.

Я искренне надеюсь, что в этой книге читатель быстро и эффективно (настолько, насколько это возможно) найдет все, что ему необходимо для осуществления задач администрирования Windows-серверов. Свои пожелания можно отправить мне по адресу **williamstanek@aol.com**. Меня можно найти на Twitter под ником WilliamStanek и на Facebook по адресу **www.facebook.com/William.Stanek.Author**.

Прочие ресурсы

Не существует какого-то волшебного способа изучить все, что есть по Windows Server 2012 R2. Несмотря на то, что есть книги, написанные по принципу "все в одном", практически невозможно собрать всю информацию в одной книге. Помня об этом, я надеюсь, что читатель будет использовать данную книгу по назначению — в качестве краткого и удобного в работе ресурса. Он охватывает основные задачи администратора Windows Server, но при этом не является исчерпывающим.

Текущие знания читателя определяют, будет ли успешной работа с этим или любым другим Windows-ресурсом или книгой. Поскольку в этой книге читатель столкнется с новыми темами, настоятельно рекомендую найти время для практики, чтобы закрепить прочитанный материал. По мере необходимости ищите дополнительную информацию — можно найти практическое ноу-хау и получить необходимые знания.

Я рекомендую регулярно посещать раздел сайта Microsoft, посвященный Windows Server (**microsoft.com/windowsserver/**), а также сайт **support.microsoft.com**, чтобы быть в курсе последних изменений. Чтобы извлечь максимальную пользу из этой книги, посетите мой веб-сайт **williamstanek.com/windows**. Он содержит информацию о Windows Server 2012 R2 и обновления для книги.

Список опечаток и поддержка книги

Мы прилагаем все усилия, чтобы предоставить читателям правильные сведения. Все ошибки, о которых стало известно после выхода этой книги, изложены на сайте:

http://aka.ms/WSR2PC2/errata

Если вы обнаружите ошибку, которой нет в этом списке, вы можете сообщить нам о ней на этой же странице.

Если вам требуется дополнительная помощь, отправьте свой запрос в службу поддержки книг издательства "Microsoft Press" по адресу **mspinput@microsoft.com**.

Обратите внимание, что поддержка программного обеспечения корпорации Microsoft по данному адресу не предоставляется.

Ваше мнение о книге

Для издательства "Microsoft Press" мнение читателей является высшим приоритетом, и ваши отзывы и отклики на наши книги представляют для нас большую ценность. Дайте нам знать, что вы думаете об этой книге в опросе по следующему адресу:

http://aka.ms/tellpress

Участие в этом опросе не отнимет у вас много времени, а мы читаем все ваши замечания и предложения. Заранее благодарим вас за ваше мнение.

Не пропадайте!

Давайте продолжим наше общение. Мы в Twitter: **http://twitter.com/MicrosoftPress**.

ГЛАВА 1

Управление файловыми системами и дисками

Жесткий диск — наиболее часто используемое устройство хранения данных, установленное на рабочих станциях и серверах сети. Пользователи зависят от жестких дисков, поскольку хранят на них текстовые документы, электронные таблицы и данные других типов. Диски организованы в файловые системы, к которым пользователи могут получить доступ либо локально, либо удаленно.

Локальные файловые системы имеются на компьютерах пользователей, и доступ к ним может быть получен без установки удаленных сетевых соединений. Диск C:, доступный на большинстве рабочих станций и серверов, является примером локальной файловой системы. Получить доступ к диску C: можно с использованием пути C:\.

С другой стороны, получить доступ к удаленным файловым системам можно с помощью сетевого соединения с удаленным ресурсом. А подключиться к удаленной файловой системе можно, нажав кнопку **Подключить сетевой диск** (Map Network Drive) в Проводнике.

Одна из задач системного администратора — управление всеми дисковыми ресурсами. Инструменты и методы, используемые для управления файловыми системами и дисками, обсуждаются в этой главе. В *главе 2* мы поговорим о настройке томов и RAID-массивов для обеспечения отказоустойчивости.

Управление ролью *Файловые службы и службы хранилища*

Файловый сервер предоставляет централизованное место для хранения и совместного использования файлов по сети. Когда много пользователей нуждается в доступе к одним и тем же файлам и данным приложений, необходимо настроить файловые серверы в домене. Хотя все серверы сконфигурированы с базовыми файловыми службами, вам нужно настроить роль **Файловые службы и службы хранилища** (File and Storage Services) и добавить любые дополнительные службы роли, которые будут необходимы.

В табл. 1.1 предоставлен обзор служб роли, связанных с ролью **Файловые службы и службы хранилища**. При установке любой дополнительной службы роли может пона-

добиться также установка следующих дополнительных компонентов, доступных в мастере добавления компонентов (Add Roles and Features Wizard):

- **Система архивации данных Windows Server** (Windows Server Backup) — стандартная утилита архивации, входящая в состав Windows Server 2012;
- **Enhanced Storage** — предоставляет дополнительные функции устройств с поддержкой аппаратного шифрования и расширенного хранения. Такие устройства используют стандарт IEEE 1167 (Institute of Electrical and Electronic Engineers) для предоставления расширенной безопасности, которая может включать аутентификацию на аппаратном уровне устройства хранения данных;
- **Multipath I/O** — предоставляет поддержку для использования множественных путей данных между файловым сервером и устройством хранения данных. Серверы используют пути ввода-вывода для избыточности в случае сбоя пути и для повышения производительности передачи данных.

Таблица 1.1. *Службы ролей для файловых служб*

Служба роли	Описание
Служба BranchCache для сетевых файлов (BranchCache For Network Files)	Позволяет компьютерам в филиале кэшировать часто используемые файлы в совместно используемых папках. Такое решение использует методы дедупликации данных, чтобы оптимизировать передачу данных по глобальным сетям (WAN) к филиалам
Дедупликация данных (Data Deduplication)	Для достижения большей эффективности хранения использует разделение файлов на блоки переменного размера и сжатие. Суть процесса заключается в том, чтобы хранить большее количество данных на меньшем пространстве в небольших (32–128 Кбайт) блоках разного размера, определяя дублирующие блоки и сохраняя одну копию для каждого блока. Оптимизированные файлы хранятся как точки повторного анализа. После дедупликации файлы на томе больше не хранятся как потоки данных, а вместо этого они заменяются заглушками, указывающими на блоки данных, находящиеся в общем хранилище блоков
Пространства имен распределенной файловой системы (DFS) (DFS Namespaces)	Позволяет группировать совместно используемые папки, находящиеся на разных серверах в одном или нескольких логически структурированных пространствах имен. Каждое пространство имен появляется как единственная общая папка с серией подпапок. Однако структура пространства имен может быть получена из совместно используемых папок на множественных серверах в различных сайтах
Репликация DFS (DFS Replication)	Позволяет синхронизировать папки на множественных серверах, находящихся в локальной или глобальной сети с использованием механизма репликации multimaster. Механизм репликации использует протокол RDC (Remote Differential Compression, протокол удаленного дифференцированного сжатия) для синхронизации порций файлов, которые изменились с момента последней репликации. Использовать репликацию DFS допускается с пространствами имен DFS или без них. Когда домен работает в режиме Windows Server 2008 или выше, контроллеры домена используют репликацию DFS для обеспечения большей отказоустойчивой репликации каталога SYSVOL

Таблица 1.1 *(окончание)*

Служба роли	Описание
Файловый сервер (File Server)	Позволяет управлять совместно используемыми файлами, к которым пользователи могут получить доступ по всей сети
Диспетчер ресурсов файлового сервера (FSRM) File Server Resource Manager (FSRM)	Устанавливает набор утилит, которые администраторы могут использовать для лучшего управления хранимыми на сервере данными. Посредством FSRM администраторы могут генерировать отчеты хранения данных, настраивать квоты, определять политики файлов
Служба агента VSS файлового сервера (File Server VSS Agent Service)	Позволяет VSS-совместимым утилитам резервного копирования создавать непротиворечивые теневые копии (снимки) приложений, которые хранят файлы данных на файловом сервере
Сервер цели iSCSI (iSCSI Target Server)	Превращает любой Windows Server в доступное по сети блочное устройство хранения, которое может использоваться для тестирования приложений перед развертыванием SAN-хранилища. Поддерживает совместно используемые хранилища на не-Windows iSCSI-инициаторах и сетевую/бездисковую загрузки для бездисковых серверов
Поставщик целевого хранилища iSCSI (iSCSI Target Storage Provider)	Поддерживает управление виртуальными дисками iSCSI и теневыми копиями (снимками) из iSCSI-инициатора
Сервер для NFS (Server for NFS)	Предоставляет решение обмена файлами для предприятий со смешанной средой Windows и UNIX. После установки служб для сетевой файловой системы (Network File System, NFS) пользователи смогут обмениваться файлами между Windows Server и UNIX с помощью протокола NFS
Службы хранилища (Storage Services)	Позволяет управлять хранилищем, в том числе пулами и пространствами. Пулы хранилищ группируют диски так, что можно создать виртуальные диски из доступной емкости. Каждый созданный вами виртуальный диск — это пространство хранилища
Рабочие папки (Work Folders)	Позволяет пользователям синхронизировать свои корпоративные данные с их устройствами и наоборот. Те устройства могут быть соединены с корпоративным доменом или рабочим местом

Двоичные файлы, необходимые для установки ролей и компонентов, называются *полезными данными* (payloads). В случае с Windows Server 2012 R2 полезные данные хранятся в подпапках папки *%SystemDrive%*\Windows\WinSXS. Если двоичные файлы для инструментов были удалены, вам нужно установить инструменты, указав источник двоичных файлов.

Добавить роль **Файловые службы и службы хранилища** на сервер можно с помощью следующих действий:

1. В окне диспетчера серверов (Server Manager) в меню **Управление** (Manage) выберите команду **Добавить роли и компоненты** (Add roles and features) или щелкните по ссылке **Добавить роли и компоненты** на плитке приветствия. В результате будет запущен мастер добавления ролей и компонентов (Add Roles and Features

Wizard). Если мастер отобразит страницу **Перед началом работы** (Before You Begin), прочитайте текст приветствия и нажмите кнопку **Далее** (Next).

2. На странице **Выбор типа установки** (Installation Type) по умолчанию отмечен переключатель **Установка ролей или компонентов** (Role-based or feature-based installation). Нажмите кнопку **Далее**.

3. На странице **Выбор целевого сервера** (Server Selection) можно указать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите либо сервер из пула серверов, либо сервер, на котором можно смонтировать виртуальный жесткий диск (virtual hard disk, VHD). Если роли и компоненты добавляются на VHD, нажмите кнопку **Обзор** (Browse), а затем используйте окно **Обзор виртуальных жестких дисков** (Browse for Virtual Hard Disks) для выбора виртуального жесткого диска. Когда будете готовы продолжить, нажмите кнопку **Далее**.

   Примечание

   В списке диспетчера серверов приводятся только серверы, работающие под управлением Windows Server 2012 R2, и те, которые вы добавили вручную в диспетчере серверов.

4. На странице **Выбор ролей сервера** (Server Roles) выберите роль **Файловые службы и службы хранилища** (File and Storage Services). Разверните соответствующий узел и выберите дополнительные службы роли для установки. Если для установки роли требуются дополнительные компоненты, будет отображено еще одно диалоговое окно. Нажмите кнопку **Добавить компоненты** (Add Features) для добавления необходимых компонентов в инсталляцию сервера. Нажмите кнопку **Далее** для продолжения.

5. На странице **Выбор компонентов** (Features) укажите один или несколько компонентов для установки. Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, будет отображено вспомогательное диалоговое окно. Нажмите кнопку **Добавить компоненты** для закрытия этого окна и установки требуемых компонентов на сервер. По окончанию выбора компонентов нажмите кнопку **Далее**. В зависимости от выбранных компонентов могут появиться дополнительные шаги, прежде, чем вы увидите страницу **Подтверждение установки компонентов** (Confirm).

6. На странице **Подтверждение установки компонентов** (Confirm) щелкните по ссылке **Экспорт параметров конфигурации** (Export configuration settings) для создания отчета установки, который можно просмотреть в Internet Explorer.

   Практический совет

   Если сервер, на котором необходимо установить роли или компоненты, не обладает всеми необходимыми двоичными файлами, сервер получит их через Windows Update (по умолчанию) или из местоположения, указанного групповой политикой.

   Также можно указать альтернативный источник для файлов. Чтобы сделать это, щелкните по ссылке **Указать альтернативный исходный путь** (Specify an alternate source path), в появившемся окне укажите альтернативный путь и нажмите кнопку **OK**. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer25\WinServer2012R2\. Для смонтированных образов введите WIM-путь с префиксом "WIM" и индексом используемого образа, например, WIM:\\CorpServer25\WinServer2012R2\install.wim:4.

7. После просмотра опций установки (и их сохранения при необходимости) нажмите кнопку **Установить** (Install) для начала процесса установки. Страница **Ход установки** (Installation Progress) позволяет отслеживать процесс инсталляции. Если окно мастера было закрыто, щелкните по значку **Уведомления** (Notifications) в окне **Диспетчер серверов**, а затем по ссылке, предназначенной для повторного открытия мастера.
8. Когда мастер закончит установку выбранных ролей и компонентов, страница **Ход установки** сообщит об этом. Просмотрите подробности установки и убедитесь, что все фазы инсталляции завершены успешно. Обратите внимание на любые действия, которые могут потребоваться для завершения установки, например перезагрузка сервера или осуществление дополнительных инсталляционных задач. Если какая-либо часть установки не увенчалась успехом, запомните причину сбоя. Просмотрите записи в окне **Диспетчер серверов**, чтобы понять суть проблемы, и примите соответствующие корректирующие действия.

Если роль **Файловые службы и службы хранилища** уже присутствует на сервере и необходимо установить дополнительные службы для файлового сервера, то добавить службы роли на сервер можно аналогичным способом.

Добавление жестких дисков

Прежде чем сделать жесткий диск доступным для пользователей, необходимо настроить его и определить, как он будет использоваться. Windows Server 2012 R2 позволяет настроить жесткие диски несколькими способами. Выбранный метод зависит, прежде всего, от типа данных, с которыми приходится работать, и от нужд сетевой среды. Для общих пользовательских данных, хранящихся на рабочих станциях, можно настроить отдельные диски как автономные устройства хранения. В этом случае пользовательские данные хранятся на жестком диске рабочей станции, где к ним осуществляется локальный доступ.

Несмотря на то, что хранить данные на единственном диске удобно, это не самый надежный способ хранения данных. Для повышения надежности и производительности необходимо заставить работать вместе набор дисков. ОС Windows Server 2012 R2 поддерживает наборы дисков и массивы с использованием технологии RAID (Redundant Array of Independent Disks, избыточный массив независимых жестких дисков), встроенной в операционную систему.

Физические диски

Используются ли отдельные диски или целые наборы дисков, нам нужны физические диски. Физические диски — устройства, которые служат для хранения данных. Объем записанных на диск данных зависит от его размера и от того, используется ли сжатие. ОС Windows Server 2012 R2 поддерживает диски стандартного и усовершенствованного форматов. У дисков стандартного формата размер физического сектора равен 512 байтов, и такие диски также называются *дисками 512b*. Физический размер сектора дисков усовершенствованного формата — 4096 байтов, и они также называются *дис-*

ками 512e. Формат 512e представляет качественный сдвиг в области технологий хранения больших, многотерабайтных объемов данных на жестких дисках.

Диски выполняют обновление физических носителей в зависимости от размера сектора. Диски 512b работают с 512 байтами данных за один раз; а диски 512e — с 4096 байтами данных за один раз. Для определения размера сектора нужно использовать утилиту командной строки Fsutil:

```
Fsutil fsinfo ntfsinfo DriveDesignator
```

Здесь *DriveDesignator* — буква диска, информацию о котором нужно получить:

```
Fsutil fsinfo sectorinfo c:
```

Наличие сектора большего физического размера позволяет перейти на новый уровень пределов физической емкости. При ограничении записи только 512 байтами за раз жесткие диски должны выполнить несколько операций записи, чтобы завершить запись. Для лучшей производительности нужно обновить приложения, чтобы обеспечить запись и чтение данных на новом уровне (4096 байт).

ОС Windows Server 2012 R2 поддерживает много разных интерфейсов дисков, в том числе:

- Small Computer System Interface (SCSI);
- Parallel ATA (PATA), также известен как IDE;
- Serial ATA (SATA).

Термины SCSI, IDE и SATA означают тип интерфейса жестких дисков, который используется для связи с контроллером диска. SCSI-диски используют SCSI-контроллеры, IDE-диски — IDE-контроллеры и т. д.

SCSI — это один из наиболее часто используемых интерфейсов, здесь есть множество дизайнов шины и типов интерфейса. Параллельный SCSI (так же называемый SPI), хоть и популярный, но уступает последовательному SCSI (Serial Attached SCSI, SAS). Интерфейс iSCSI (Internet Small Computer System Interface) базируется на архитектурной модели SCSI, но для транспорта использует TCP/IP, а не обычную физическую реализацию.

Интерфейс SATA был разработан для замены IDE. Диски SATA все более и более популярны как дешевая альтернатива SCSI. Наиболее распространены интерфейсы SATA II и SATA III, они могут передавать данные со скоростью 3 и 6 Гбит/с соответственно. ESATA (так же известный как внешний SATA, external SATA) предназначен для подключения внешних жестких дисков.

> ***Примечание***
>
> Операционная система Windows Server 2012 содержит расширения для улучшенной поддержки SATA-дисков, уменьшающие несогласованность метаданных и позволяющие дискам более эффективно кэшировать данные. Улучшенное кэширование помогает защищать кэшированные данные в случае неожиданных потерь питания.

При установке нового сервера нужно уделить пристальное внимание настройке диска. Начните с выбора дисков или систем хранения, предоставляющих надлежащий уровень производительности. Действительно, среди различных спецификаций диска есть существенные различия в скорости и производительности.

Нужно рассматривать не только емкость диска, но также и следующие его параметры:

- скорость вращения — мера того, как быстро вращается диск;
- среднее время поиска — показывает, сколько времени нужно для поиска между дорожками диска во время последовательных операций ввода-вывода.

Вообще говоря, при сравнении дисков, соответствующих той же спецификации, что и Ultra640 SCSI или SATA III, чем выше скорость вращения (измеряется в тысячах вращений в минуту — rotations per minute, RPM) и ниже среднее время поиска (измеряется в миллисекундах, мс), тем лучше. Например, диск со скоростью вращения 15 000 RPM на 45–50% быстрее среднего диска на 10 000 RPM при прочих равных условиях. Диск со временем поиска 3,5 мс обеспечивает лучшее время отклика на 25–30% по сравнению с диском со временем поиска 4,7 мс.

Другие факторы, на которые нужно обратить внимание:

- *максимальная устойчивая скорость передачи данных* показывает, сколько данных диск может передавать постоянно;
- *среднее время наработки на отказ* (mean time to failure, MTTF) — через сколько часов работы следует ожидать отказ диска, перед тем как он перестанет работать;
- *нерабочие температуры* — при каких температурах происходит сбой диска.

У большинства дисков сопоставимого качества скорость передачи данных и MTFF подобны. Так, если сравнивать диски SCSI Ultra320 со скоростью вращения 15 000 об./мин различных производителей, у многих дисков будут подобные скорости передачи и MTTF. Скорости передачи данных могут быть также выражены в гигабитах в секунду (Гбит/с). Уровень 1,5 Гбит/с эквивалентен скорости передачи данных 187,5 Мбайт/с, а 3,0 Гбит/с эквивалентно 375 Мбайт/с. Иногда указывается максимальная скорость внешней передачи (на спецификацию, к которой относится диск) и средняя длительная скорость передачи.

> ***Примечание***
>
> Не путайте единицы измерения Мбайт/с и Мбит/с. Мбайт/с — это мегабайт в секунду, Мбит/с — мегабит в секунду. Поскольку в байте 8 бит, частота передачи 100 Мбайт/с эквивалентна частоте 800 Мбит/с.

Температура — другой важный фактор, на который нужно обратить внимание при выборе диска, но его принимают во внимание немногие администраторы. Как правило, чем быстрее вращается диск, тем больше он греется. Это не всегда так, но при выборе диска нужно рассмотреть и фактор температуры. Например, диски со скоростью 15K более горячие, и необходимо убедиться, что температура тщательно контролируется. Для типичных 15K-дисков температура отказа составляет 70 °C и выше (как и в случае с большинством других дисков).

Операционная система Windows Server 2012 R2 поддерживает диски с аппаратным шифрованием (они также называются зашифрованными жесткими дисками). У зашифрованных жестких дисков есть встроенные процессоры, перемещающие функции шифрования с операционной системы на аппаратные средства, освобождая ресурсы операционной системы. ОС Windows Server 2012 R2 будет использовать аппаратное шифрование с BitLocker, если это возможно. Другие средства защиты, доступные

в Windows Server 2012 R2, включают *защищенную загрузку* (Secure Boot) и *разблокировку по сети* (Network Unlock). Защищенная загрузка обеспечивает целостность начальной загрузки с проверкой настройки BCD (Boot Configuration Data) согласно настройкам профиля проверки TPM (Trusted Platform Module). Разблокировка по сети может быть использована для автоматической разблокировки диска операционной системы на компьютерах, присоединенных к домену. Получить подробную информацию о TPM, BitLocker, разблокировке по сети и зашифрованных жестких дисках можно в главе 11 книги "Microsoft® Windows 8. Справочник администратора"[1].

Подготовка физического диска для использования

После установки диска его необходимо настроить для использования. При этом осуществляется разбивка диска на разделы, создание файловых систем на этих разделах. *Раздел* — это секция физического диска, функционирующая как отдельная единица. После формирования раздела на нем нужно создать файловую систему.

Стили разделов MBR и GPT

На дисках используются разделы двух типов: главная загрузочная запись (Master Boot Record, MBR) и таблица разделов GUID (GUID partition table, GPT). MBR содержит таблицу разделов, которая описывает расположение разделов на диске. При использовании MBR первый сектор на жестком диске содержит главную загрузочную запись, а файл двоичного кода называется *главным загрузочным кодом*, который используется для загрузки операционной системы. Этот сектор неделим и скрыт от просмотра для защиты системы.

В случае MBR диски поддерживают тома до 4 Тбайт и используют один из двух типов разделов: первичный или расширенный. У каждого MBR-диска может быть до четырех первичных (основных) разделов или три первичных и один расширенный раздел. Первичные разделы — это разделы диска, к которым можно получить доступ непосредственно для файлового хранилища. После создания файловой системы первичный раздел станет доступным для пользователей. Получить прямой (непосредственный) доступ к расширенному разделу нельзя. Вместо этого в расширенном разделе создается один (или больше) логический диск, который используется для хранения файлов. Учитывая, что можно разделить расширенный раздел на логические диски, физический диск можно разделить больше, чем на четыре раздела.

Таблица разделов GPT была первоначально разработана для высокоэффективных компьютеров на базе процессора Itanium. Основная разница между MBR и GPT — в способе хранения данных. В случае с GPT критические данные раздела хранятся на разных разделах, для улучшенной структурной целостности используются избыточные основные и резервные таблицы разделов. Также GPT-диски поддерживают тома до 18 Эбайт и целых 128 разделов. Несмотря на то, что у GPT и MBR есть базовые различия, большинство связанных с диском задач выполняется одинаково.

---

[1] Уильям Р. Станек. Microsoft® Windows 8. Справочник администратора. — СПб.: Microsoft Press, БХВ-Петербург, 2013.

Наследственная и защитная MBR

Большинство современных компьютеров поставляется с UEFI (Unified Extensible Firmware Interface, расширяемый интерфейс прошивки). Хотя UEFI заменяет BIOS и EFI как высокоуровневый интерфейс микропрограммного обеспечения, UEFI не заменяет всю функциональность BIOS или EFI и обычно является "оберткой" вокруг BIOS или EFI. С точки зрения UEFI, GPT — предпочтительная схема выделения разделов, а защитная MBR (protective MBR) может быть расположена на любом диске, который использует дисковое расположение GPT. Наследственная MBR (legacy MBR) и защитная MBR — не одно и то же.

Наследственная MBR расположена в первом логическом блоке на диске, который не использует GPT. Первые 512 байт на MBR-диске имеют следующую разметку.

- MBR начинается 424-байтовым загрузочным кодом, который используется для выбора записи MBR-раздела и загрузки первого логического блока того раздела. Загрузочный код MBR не выполняется UEFI.
- После загрузочного кода следует 4-байтовая уникальная подпись MBR-диска, которая может использоваться операционной системой для идентификации диска и разграничения диска от других дисков системы. Уникальная подпись записывается операционной системой и не используется UEFI.
- После подписи диска следует 2-байтовый разделитель. По байтовому смещению 446 находится массив из четырех записей разделов MBR, каждая запись длиной 16 байтов. Блок 510 содержит 0x55, а блок 511 — 0xAA. Блок 512 зарезервирован.

Каждая из четырех записей разделов определяет первый и последний логические блоки, используемые разделом на диске.

- Каждая 16-байтовая запись MBR-раздела начинается 1-байтовым признаком активного раздела. Например, значение 0x80 указывает, что раздел является активным (загрузочным). Любое другое значение указывает, что этот раздел не является загрузочным. UEFI не использует это значение.
- После признака активности следует 3-байтовый адрес начала раздела. По байтовому смещению 4 находится 1-байтовое значение, которое указывает тип операционной системы, а после него следует 3-байтовое значение, которое задает конец раздела. Эти значения не используются UEFI.
- По байтовому смещению 8 находится 4-байтовое значение, указывающее первый логический блок раздела, а за ним следует 4-байтовое значение, содержащее размер раздела в логических блоках. Оба эти значения используются UEFI.

> ***Примечание***
>
> Если у MBR-раздела значение типа операционной системы равно 0xEF, микропрограммное обеспечение должно добавить GUID системного раздела UEFI к дескриптору для раздела MBR. Это позволяет загрузочным приложениям, загрузчикам операционных систем, драйверам и другим низкоуровневым инструментам определять местоположение системного раздела UEFI, который должен физически находиться на диске.

Защитная MBR может располагаться в первом логическом блоке на диске, который использует GPT. Защитная MBR предшествует заголовку таблицы разделов (Partition

Table Header) GUID и используется для обеспечения совместимости с инструментами, не понимающими структуру разделов GPT. Цель защитной MBR заключается в том, чтобы защитить GPT-разделы от приложений начальной загрузки, загрузчиков операционной системы, драйверов и других низкоуровневых инструментов, которые не понимают стиль разделов GPT. Защитная MBR определяет поддельный раздел, охватывающий весь диск. Когда у диска есть защитная MBR, первые 512 байтов выглядят так:

- защитная MBR начинается с 424-байтового загрузочного кода, который не выполняется UEFI;
- после загрузочного кода следует 4-байтовая подпись диска, которая установлена в 0 и не используется UEFI;
- после подписи диска следует 2-байтовый разделитель, который также установлен в 0 и не используется UEFI;
- по байтовому смещению 446 находится массив из четырех записей разделов MBR, длина каждой записи — 16 байт. Используется только первая запись раздела — запись защитного раздела. Остальные записи установлены в 0;
- блок 510 содержит 0x55, а блок 511 — 0xAA. Блок 512 зарезервирован.

Защитная запись раздела резервирует все пространство на диске после первых 512 байт для структуры диска GPT. Защитная запись раздела начинается 1-байтовым индикатором активного раздела, который установлен в 0x00, что указывает на неактивный раздел. После него следует 3-байтовый адрес, указывающий, что раздел начинается с позиции 0x000200, и это является первым доступным для использования блоком на диске.

По байтовому смещению 4 находится 1-байтовое значение, установленное в 0xEE и указывающее тип операционной системы — GPT Protective. После него следует 3-байтовое значение, задающее последний используемый блок на диске, который является концом раздела (или 0xFFFFFF, если невозможно представить это значение).

По байтовому смещению 8 находится 4-байтовое значение, установленное в 0x00000001, которое идентифицирует логический адрес блока заголовка раздела GPT. Оно сопровождается 4-байтовым значением, указывающим размер диска минус один блок (или 0xFFFFFFFF, если размер диска слишком большой, чтобы быть представленным).

Типы дисков и файловые системы

В дополнение к типу раздела у физических дисков есть еще один параметр — тип диска, который может быть либо базовым, либо динамическим, как будет показано далее. После установки типа раздела для физического диска можно отформатировать свободные области диска для создания логических дисков. Форматирование создает файловую систему на разделе. ОС Windows Server 2012 R2 поддерживает следующие файловые системы:

- FAT;
- FAT32;
- exFAT;

- NTFS;
- ReFS.

В случае с FAT число битов, используемых в таблице размещения файлов, определяет используемый вариант FAT и максимальный размер тома. Файловая система FAT16, также известная как просто FAT, определяет, что ее таблица размещения файлов использует 16 бит. Тома с размером 4 Гбайт или меньше форматируются как FAT16.

В случае с FAT32 таблица размещения файлов использует 32 бита, и допускается создавать FAT32-тома с объемом 32 Гбайт или меньше посредством утилиты форматирования Windows. Хотя Windows может монтировать FAT32-тома большего размера, созданные сторонними утилитами, для томов размером больше 32 Гбайт необходимо использовать NTFS.

Файловая система Extended FAT (exFAT) — расширенная версия FAT. Технически, exFAT может называться FAT64 (и действительно так называется некоторыми пользователями). Файловая система exFAT определяет свои таблицы размещения файлов, используя 64 бита. Это позволяет exFAT преодолевать предел размера файла в 4 Гбайт и предел размера тома в 32 Гбайт, который был в FAT32. Файловая система exFAT поддерживает размеры кластера до 128 Кбайт для томов до 256 Тбайт.

У томов NTFS совсем иная структура и другой набор функций. Первая область тома — это загрузочный сектор, хранящий информацию о разметке диска и программу самозагрузки, которая выполняется при запуске и загружает операционную систему. Вместо таблицы размещения файлов, NTFS использует реляционную базу данных для хранения информации о файлах. Эту базу данных называют *главной файловой таблицей* (Main File Table, MFT).

MFT хранит файловую запись каждого файла и папки тома, информацию о томе и сведения о самой MFT. Файловая система NTFS предлагает много расширенных опций, в том числе поддержку шифрованной файловой системы (Encrypting File System), сжатия, возможность создания отчетов экранирования и хранения файла, которые станут доступны при добавлении службы роли **Диспетчер ресурсов файлового сервера** (FSRM) как части роли **Файловые службы** (File Services).

Файловая система ReFS (Resilient File System) — следующее поколение NTFS. Она остается совместимой с базовыми функциями NTFS при сокращении дополнительных функций, чтобы сфокусироваться на надежности. Это означает, что квоты дисков, файловая система с шифрованием, сжатие, отчеты экранирования и хранения файлов не доступны, но добавлены встроенные функции надежности.

Одна из основных функций обеспечения надежности файловой системы ReFS — это сканер целостности данных. Он обеспечивает превентивную идентификацию ошибок, изоляцию и коррекцию. Если сканер обнаруживает повреждение данных, используется процесс восстановления, чтобы локализировать область повреждения и выполнить автоматическую онлайн-коррекцию. С помощью процесса автоматического спасения поврежденные области, которые не могут быть восстановлены, например из-за сбойных блоков на физическом диске, удаляются из тома, чтобы они больше не могли оказать негативное влияние на хорошие данные. Поскольку ReFS использует автоматическую проверку и процесс восстановления, ReFS не нуждается в какой-либо дополнительной проверке (следовательно, нет никакой утилиты вроде Check Disk для ReFS).

Примечание

При работе с файловыми службами и службами хранилища можно группировать доступные физические диски в пулы хранилищ, поэтому допускается создание виртуальных дисков из доступной емкости. Каждый созданный виртуальный диск является *пространством хранения* (storage spaces). Поскольку только NTFS и ReFS поддерживают пространства хранения, помните об этом при форматировании тома на файловых серверах. Для получения дополнительной информации о пространствах хранения обратитесь к *главе 2*.

Использование оснастки *Управление дисками*

Оснастка консоли управления Microsoft (MMC) **Управление дисками** (Disk Management) используется для настройки дисков. Оснастка **Управление дисками** позволяет легко работать как с внутренними, так и с внешними дисками на локальной или удаленной системе. Оснастка **Управление дисками** является частью консоли **Управление компьютером** (Computer Management). Данная оснастка может быть добавлена в пользовательскую консоль MMC. В оснастке **Управление компьютером** можно получить доступ к оснастке **Управление дисками** (Disk Management), развернув узел **Запоминающие устройства** (Storage) и затем выбрав узел **Управление дисками** (Disk Management). Альтернативно вы можете получить доступ к ней, выполнив команду `diskmgmt.msc`.

Оснастка обладает тремя представлениями: **Список дисков** (Disk List), **Список томов** (Volume List) и **Графическое представление** (Graphical View). На удаленных системах функциональность оснастки ограничена: разрешается просмотреть подробную информацию о диске, изменить буквы дисков и пути, конвертировать типы дисков. Для съемных дисков удаленно также можно извлечь носитель. Для осуществления расширенной манипуляции с удаленными дисками необходимо использовать утилиту командной строки DiskPart.

Примечание

Перед тем как начать работу с оснасткой **Управление дисками**, необходимо знать несколько вещей. Если создается раздел, но не форматируется, то он отмечается как **Свободное пространство** (Free space). Если часть диска не назначается разделу, эта секция диска помечается как **Не распределена** (Unallocated).

На рис. 1.1 в верхней части окна используется представление **Список томов**, а в нижней части — **Графическое представление**. Изменение представления верхней или нижней панели осуществляется следующим образом:

- для изменения представления верхней панели выберите команду **Вид | Верх** (View | Top), а затем — тип представления;
- для изменения представления нижней панели выберите команду **Вид | Низ** (View | Bottom), а затем — тип представления;
- чтобы скрыть нижнюю панель, выберите команду **Вид | Низ | Скрыть** (View | Bottom | Hidden).

ОС Windows Server 2012 R2 поддерживает четыре типа конфигурации дисков.

- **Базовый** — стандартный тип жесткого диска (фиксированный), используемый в предыдущих версиях Windows. Базовые диски делятся на разделы и являются исходным типом диска для ранних версий Windows.

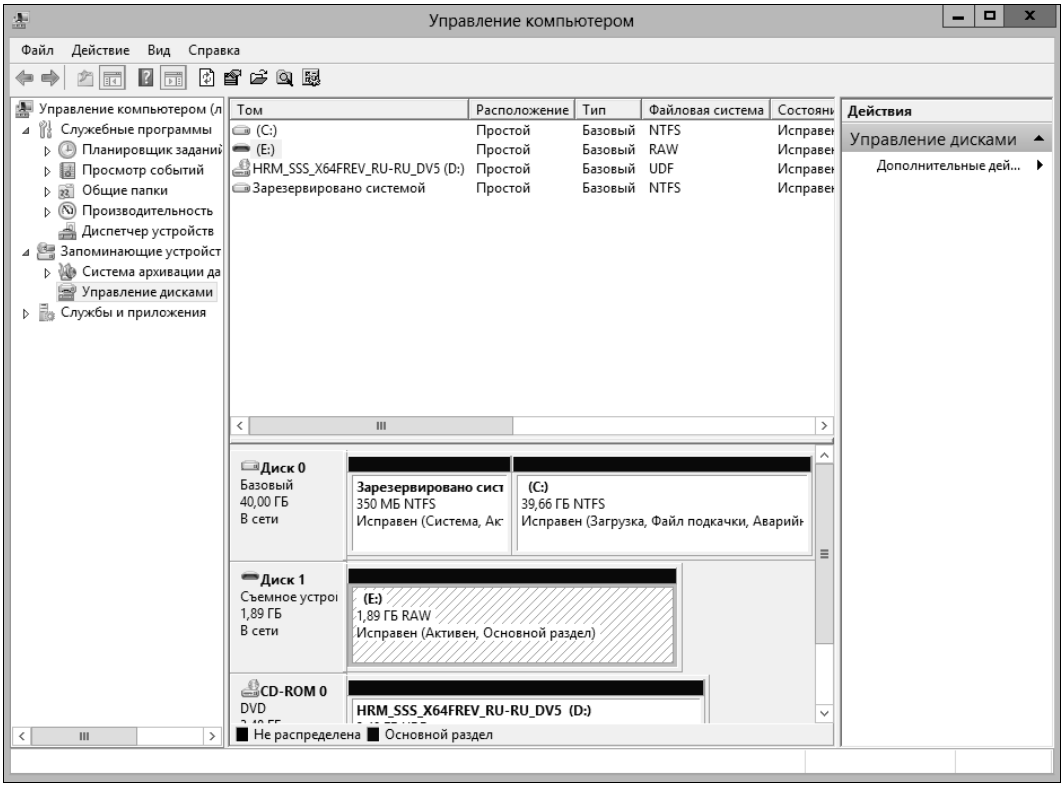


Рис. 1.1. В оснастке **Управление дисками** по умолчанию в верхней панели отображается сводка по всем дискам, а нижняя панель предоставляет обзор этих же дисков

- **Динамический** — расширенный тип жесткого диска (фиксированный), который можно обновлять без необходимости перезапуска системы (в большинстве случаев). Динамические диски делятся на тома.
- **Съемное устройство** — стандартный тип диска, ассоциируемый со сменными устройствами хранения данных.
- **Виртуальный** — тип виртуального жесткого диска (Virtual Hard Disk, VHD), используемый в виртуализации. Компьютеры могут использовать VHD так же, как и обычные жесткие диски, могут даже загружаться с VHD.

Для получения информации о диске щелкните правой кнопкой мыши на нем и выберите команду **Свойства**. Откроется одноименное диалоговое окно. На рис. 1.2 показаны такие окна для двух фиксированных дисков: слева — для диска с файловой системой NTFS, справа — с файловой системой ReFS. Оба окна имеют дополнительные вкладки в зависимости от конфигурации сервера.

Если настроено удаленное управление через диспетчер серверов и MMC, можно использовать оснастку **Управление дисками**, чтобы управлять дисками удаленного компьютера. Имейте в виду, что в этом случае функции управления удаленными дисками отличаются от функций управления локальными дисками.

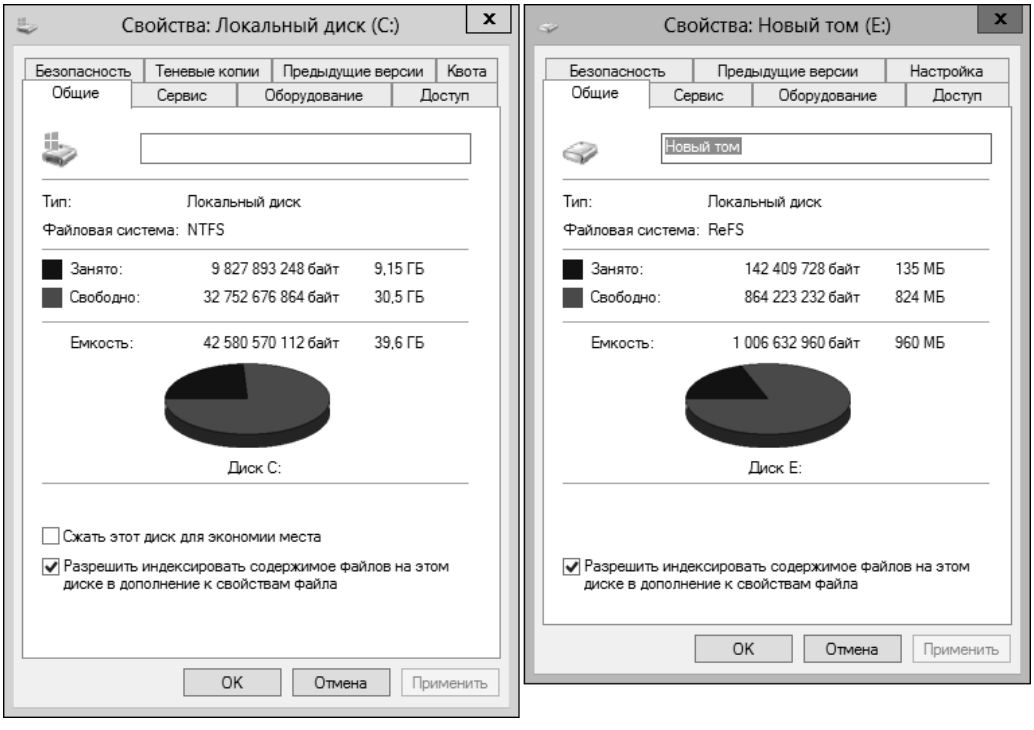


Рис. 1.2. Вкладка **Общие** окна **Свойства** предоставляет подробную информацию о диске

Можно выполнить следующие задачи:

- просмотреть ограниченные свойства диска, но не свойства тома. При просмотре свойств диска доступны только вкладки **Общие** и **Тома**, но не доступны свойства диска;
- изменить букву диска и путь монтирования;
- отформатировать, уменьшить или расширить том. Есть возможность добавить и настроить параметры зеркальных, составных и чередующихся томов;
- удалить том (кроме системных и загрузочных томов);
- создать, присоединить и отключить виртуальный диск. При создании и присоединении VHD необходимо ввести полный путь к файлу, нет возможности выбрать vhd-файл (использовать кнопку **Обзор**).

Некоторые задачи, выполняемые с дисками и томами, основаны на службах Plug and Play и Remote Registry.

Сменные устройства хранения данных

Сменные устройства хранения данных могут быть отформатированы как ReFS, NTFS, FAT, FAT32 или exFAT. Внешние устройства хранения данных подключают к компьютеру вместо того, чтобы устанавливать их внутри компьютера. Это делает использование сменных устройств проще и установку быстрее по сравнению с большинством

фиксированных дисков. Большинство внешних устройств хранения данных подключаются либо по USB, либо с помощью интерфейса FireWire. При работе с USB или FireWire скорость передачи и общая производительность устройства с точки зрения пользователя зависит, прежде всего, от поддерживаемой версии. В настоящее время существует несколько версий USB и FireWire.

USB 2.0 является промышленным стандартом, пока мир переходит на USB 3.0. Устройства USB 2.0 могут быть отмечены как полноскоростные (full speed) — до 12 Мбит/с или как высокоскоростные (high speed) — до 480 Мбит/с. Несмотря на то, что USB 2.0 может передавать данные с максимальной скоростью до 480 Мбит/с, устойчивая скорость передачи данных обычно составляет 10–30 Мбит/с. Фактическая поддерживаемая скорость передачи зависит от многих факторов, в том числе от типа устройства, типа передаваемых данных и скорости компьютера. У каждого USB-контроллера на компьютере есть фиксированная пропускная способность, которую должны совместно использовать все подключенные устройства. Скорость передачи данных значительно меньше, если USB-порт компьютера более ранней версии, чем поддерживается устройством. Например, если устройство USB 2.0 подключается к порту USB 1.0 или наоборот, устройство будет работать со скоростью USB 1.0, что значительно меньше скорости USB 2.0.

Порты USB 1.0, 1.1 и 2.0 выглядят одинаково. Однако у большинства портов USB 3.0 есть специальная окраска, чтобы отличать их от других портов. Лучший способ определить тип портов USB — обратиться к документации, которая поставляется с компьютером. У более новых мониторов есть порты USB 2.0, к которым также можно подключить устройства. При подключении USB-устройства к монитору, монитор действует как USB-хаб. Как и в случае с любым другим USB-хабом, все устройства, подключенные к хабу, совместно используют одну и ту же пропускную способность, при этом общая пропускная способность определена скоростью USB-входа, к которому подключен хаб на компьютере.

Стандарт FireWire (IEEE 1394) — высокопроизводительный стандарт подключения, использующий одноранговую архитектуру, в которой периферийные устройства согласовывают конфликты при обращении к шине для определения, какое устройство может лучше всего управлять передачей данных. Как и в случае с USB, в настоящее время используются несколько версий FireWire. Максимальная скорость длительной передачи данных у FireWire 400 (У IEEE 1394a) составляет до 400 Мбит/с. IEEE 1394b позволяет передавать данные со скоростью 400 (S400), 800 (S800) и 1600 Мбит/с (S1600). Подобно USB, при подключении устройства IEEE 1394b к порту IEEE 1394a устройство будет работать в режиме значительного снижения скорости — до уровня FireWire 400.

Подобно USB-портам, скорость длительной передачи для портов IEEE 1394a и IEEE 1394b будет значительно меньше, чем максимально возможная. Формы портов и кабелей IEEE 1394a и IEEE 1394b отличаются, что упрощает их идентификацию. У кабелей FireWire 400 без питания шины есть четыре контакта и четыре соединителя. У кабелей FireWire 400 с питанием шины — шесть контактов и шесть соединителей. У кабелей FireWire 800 и FireWire 1600 всегда есть питание шины, и они имеют 9 контактов и 9 соединителей.

Можно также использовать внешний SATA (eSATA), который доступен на более новых компьютерах. eSATA — это соединение ультравысокой производительности для передачи данных на устройство хранения данных и с него. eSATA работает на скорости до 3 Гбит/с. Добавить поддержку устройств eSATA можно с помощью установки контроллера eSATA.

При покупке внешнего устройства для компьютера нужно знать, какой интерфейс оно поддерживает. В некоторых случаях устройство поддерживает несколько интерфейсов, например USB 3.0 и eSATA. Устройство с несколькими интерфейсами предоставляет больше возможностей.

Работа со сменными дисками подобна работе с фиксированными дисками.

- Щелкните правой кнопкой мыши по сменному носителю и выберите команду **Открыть** (Open) или **Проводник** (Explore), чтобы исследовать содержимое диска в Проводнике.
- Щелкните правой кнопкой мыши по сменному диску и выберите команду **Форматировать** (Format), чтобы отформатировать сменный диск *(см. разд. "Форматирование разделов" далее в этой главе)*. На сменных дисках, как правило, создается один раздел.
- Щелкните правой кнопкой мыши по сменному диску и выберите команду **Свойства** для просмотра или установки его свойств. На вкладке **Общие** окна **Свойства** можно установить метку тома *(см. главу 2)*.

При работе со сменными дисками есть возможность настроить представления диска и папки. Для этого щелкните на диске и выберите команду **Свойства**, а затем перейдите на вкладку **Настройка** (Customize). Далее нужно указать тип папки по умолчанию. Например, можно установить тип папки **Документы** (Documents) или **Изображения** (Pictures). Также есть возможность установить изображение и значок папки.

Сменные диски поддерживают общий доступ по сети. Настройка общего доступа к сменному диску производится аналогично настройке общего доступа для обычного диска. Настраиваются разрешения доступа, опции кэширования для использования файлов вне сети (оффлайн), ограничивается число одновременно работающих пользователей. Предоставить общий доступ можно как ко всему сменному диску, так и к отдельной папке, хранящейся на таком диске. При необходимости для одного ресурса можно создать несколько экземпляров общего ресурса.

Съемные диски отличаются от стандартных общих NTFS-ресурсов тем, что у них не обязательно есть базовая архитектура безопасности. При использовании файловой системы exFAT, FAT или FAT32 у папок и файлов, хранящихся на этом диске, нет никаких прав доступа или других функций, кроме атрибутов "только чтение" или "скрытый", доступных для установки.

Установка и проверка нового диска

Горячая замена (hot swap) — это функция, позволяющая демонтировать внутренние устройства, не отключая при этом компьютер. Как правило, внутренние диски, поддерживающие горячую замену, устанавливаются и извлекаются с передней части компьютера. Если компьютер поддерживает горячую замену внутренних дисков, разреша-

ется устанавливать новые диски без необходимости выключения компьютера. После установки нового диска откройте оснастку **Управление дисками** и в меню **Действие** (Action) выберите команду **Повторить проверку дисков** (Rescan Disks). Новые найденные диски будут добавлены, а их тип надлежащим образом распознан. Если добавленный диск недоступен, перезагрузите компьютер.

Если компьютер не поддерживает горячую замену внутренних дисков, необходимо выключить компьютер и затем установить новые диски. Далее нужно просканировать диски, как было описано ранее. Новые диски, которые еще не были инициализированы, не имеют меток, и оснастка **Управление дисками** отобразит окно **Инициализация дисков** (Initialize Disk), как только обнаружит новые диски.

Для инициализации дисков выполните следующие действия:

1. Каждый установленный вами диск нуждается в инициализации. Выберите установленный диск или диски.
2. Диски могут использовать тип разделов MBR или GPT. Выберите тип раздела для диска или дисков, которые необходимо инициализировать.
3. Нажмите кнопку **OK**. Если выбрана инициализация дисков, Windows добавит дисковую подпись на диски и инициализирует их как диски базового типа.

Если хотите использовать окно **Инициализация дисков**, закройте его и используйте оснастку **Управление дисками** для просмотра и работы с диском. В представлении **Список дисков** неинициализированные диски отмечаются красной стрелкой вниз, при этом состояние диска будет указано как **Не проинициализирован** (Not Initialized), а тип диска — **Нет данных** (Unknown). Затем щелкните правой кнопкой мыши по значку диска и выберите команду **В сети** (Online). Снова щелкните правой кнопкой мыши по значку диска и выберите команду **Инициализировать диск** (Initialize Disk). Теперь можно инициализировать диск, как было показано ранее.

> ***Примечание***
>
> В командной строке Windows PowerShell, запущенной с правами администратора, вы можете использовать команду `Get-Disk` для получения списка всех доступных дисков и команду `Initialize-Disk` для инициализации новых дисков.

Статус диска

Знание статуса диска полезно при установке новых дисков или разрешении проблем с дисками. Оснастка **Управление дисками** показывает состояние диска в графическом представлении и в представлении **Список томов**. В табл. 1.2 представлены общие значения состояния.

Таблица 1.2. *Общие значения состояния дисков*

Состояние	Описание	Резолюция
В сети (Online)	Нормальное состояние диска. Означает, что диск доступен и с ним нет никаких проблем. Это состояние показывают базовые и динамические диски	У диска нет никаких видимых проблем. Не нужно предпринимать каких-либо корректирующих действий

Таблица 1.2 *(окончание)*

Состояние	Описание	Резолюция
В сети (Ошибки) (Online (Errors))	На динамическом диске были обнаружены ошибки ввода-вывода	Можно попытаться исправить временные ошибки, щелкнув правой кнопкой мыши по диску и выбрав команду **Реактивировать диск** (Reactivate Disk). Если это не поможет, у диска, вероятно, есть физические повреждения или необходимо запустить полную проверку диска
Вне сети (Offline)	Диск недоступен и может быть поврежден или временно недоступен. Если имя диска изменено на **Отсутствует** (Missing), диск больше не может быть идентифицирован в системе	Проверьте наличие проблем с диском, с его контроллером и кабелями. Убедитесь, что к диску подключено питание и он подключен правильно (имеется в виду интерфейсный кабель). Используйте команду **Реактивировать диск**, чтобы вернуть диск в состояние **В сети** (если возможно)
Чужой (Foreign)	Диск был перемещен в компьютер, но не был импортирован для использования. Отказавший диск может иногда выводиться как **Чужой**	Щелкните правой кнопкой мыши по диску и выберите команду **Импорт чужих дисков** (Import Foreign Disks) для добавления диска в систему
Не читается (Unreadable)	Диск в данный момент недоступен, это может произойти, когда диски повторно сканируются. Такое состояние отображают и базовые, и динамические диски	Это состояние отображается на FireWire/USB-кардридерах, если карта памяти не форматирована или неверно форматирована. Также это состояние устанавливается после извлечения карты памяти из кардридера. В противном случае, если диски не сканируются, диск может быть поврежден или иметь ошибки ввода-вывода. Щелкните правой кнопкой мыши по диску и выберите команду **Повторить проверку дисков**, чтобы попытаться исправить проблему. Также можно перезагрузить систему
Не опознан (Unrecognized)	Диск неизвестного типа и не может использоваться в системе. Это состояние могут отображать не-Windows-диски	Если диск относится к другой операционной системе, ничего не делайте. Нельзя применять этот диск на компьютере, поэтому попытайтесь использовать другой диск
Не проинициализирован (Not Initialized)	У диска нет верной подписи. Это состояние может отображать диск с файловой системой, отличной от Windows	Если диск относится к другой операционной системе, ничего не делайте. Этот диск нельзя использовать на компьютере. Для подготовки диска с целью применения в Windows Server 2012 R2 щелкните правой кнопкой мыши по нему и выберите команду **Инициализировать диск**
Нет носителя (No Media)	В DVD или другой съемный дисковод не вставлен носитель или же носитель был удален. Это состояние могут отображать только DVD и другие типы сменных дисков	Чтобы перевести диск в состояние **В сети**, вставьте DVD или сменный диск. С кардридерами (FireWire или USB) это состояние обычно (но не всегда) отображается, когда карта памяти извлечена

Работа с базовыми, динамическими и виртуальными дисками

Операционная система Windows Server 2012 R2 поддерживает базовые, дисковые и виртуальные конфигурации дисков. В этом разделе обсуждаются техники работы с диском каждого типа конфигурации.

Использование базовых и динамических дисков

Базовые, динамические и виртуальные конфигурации диска могут использоваться как с устаревшими (legacy) подходами хранения, так и с подходами, основанными на стандартах (standards-based). Обычно разделы диска Windows Server 2012 R2 инициализируются как базовые диски.

Невозможно создать новые отказоустойчивые наборы дисков, используя базовый тип диска. Необходимо конвертировать базовые диски в динамические и затем создать тома, использующие чередование, зеркалирование или чередование с контролем четности (RAID 0, 1 и 5 соответственно). Отказоустойчивость и возможность смены дисков без необходимости перезапуска компьютера — ключевые возможности, которые отличают динамические диски от базовых. Другие функции дисков зависят от его форматирования.

На одном и том же компьютере могут использоваться базовые и динамические диски. Однако набор томов должен использовать однотипные диски и однотипные разделы. Например, если необходимо зеркалировать диски C: и D:, оба диска должны быть динамическими и использовать одинаковый тип разделов, который может быть или MBR, или GPT. Обратите внимание на то, что оснастка **Управление дисками** позволяет выполнять много задач конфигурации диска независимо от используемого диска. Преимущество в том, что во время процесса конфигурации оснастка **Управление дисками** конвертирует тип диска в динамический тип. Чтобы узнать, как конвертировать диск из базового в динамический, *см. разд. "Изменение типа диска" далее в этой главе*.

Для базовых и динамических дисков можно осуществлять различные задачи конфигурации диска. Над базовыми дисками допустимо выполнять следующие действия:

- форматировать разделы и помечать их как активные;
- создавать и удалять первичные и расширенные разделы;
- создавать и удалять логические диски на расширенных разделах;
- конвертировать тип диска из базового в динамический.

Операции над динамическими дисками:

- создание и удаление простых, чередующихся, составных (spanned), зеркальных томов и томов RAID 5;
- удаление зеркала из зеркального тома;
- расширение простых или составных томов;
- разделение тома на два тома;

- восстановление зеркальных томов или томов RAID 5;
- реактивирование отсутствующих дисков или дисков с состоянием **Вне сети**;
- преобразование обратно к базовому диску (требует удаления томов и восстановления их из резервной копии).

Над дисками любого типа можно выполнить следующие операции:

- просматривать свойства дисков, разделов и томов;
- назначать буквы дискам;
- настраивать безопасность и общий доступ к диску;
- использовать дисковые пространства (storage spaces) для реализации хранилища на основе стандартов.

Особенности базовых и динамических дисков

При работе с основными и динамическими дисками нужно иметь в виду пять специальных типов секций диска.

- **Активен** (Active) — активный раздел или том. Это секция диска, использующаяся для кэширования и запуска системы. Некоторые устройства со сменным носителем могут быть выведены как устройства с активным разделом.
- **Загрузка** (Boot) — загрузочный раздел или том, содержащий операционную систему и ее вспомогательные файлы. Разделы **Система** и **Загрузка** могут быть одним и тем же разделом.
- **Аварийный дамп памяти** (Crash dump) — раздел, на который компьютер пытается записать файлы дампа в случае отказа системы. По умолчанию файлы дампа записываются в папку *%SystemRoot%*, но они могут быть расположены на любом разделе или томе.
- **Файл подкачки** (Page file) — раздел, содержащий файл подкачки, используется операционной системой. Поскольку компьютер может использовать для подкачки несколько дисков, в зависимости от настройки виртуальной памяти, у компьютера может быть несколько разделов/томов этого типа.
- **Система** (System) — системный раздел или том содержит аппаратно-зависимые файлы, необходимые для загрузки операционной системы. Системный раздел не может быть частью составного или чередующегося тома.

> ***Практический совет***
>
> GPT становится основным типом диска для Windows Server. При использовании Windows Server 2012 R2 у типичного нового диска будет стиль разметки GPT с разделом восстановления и системным разделом EFI.

> ***Примечание***
>
> Чтобы пометить раздел как активный, используйте оснастку **Управление дисками**. В этой оснастке щелкните правой кнопкой мыши по базовому разделу, который нужно сделать активным, и выберите команду **Сделать раздел активным**. Динамические диски нельзя пометить как активные. При конвертировании базового диска, содержащего активный раздел, в динамический диск этот раздел автоматически станет обычным томом.

Изменение типа диска

Вы можете использовать динамические диски в любой текущей версии Windows и во многих других операционных системах, в том числе в большинстве вариантов UNIX. Однако помните, что вам нужно создавать отдельные тома для каждой операционной системы, отличной от Windows.

Нельзя использовать динамические диски на портативных компьютерах. Когда вы работаете на стационарных компьютерах и серверах, то можете использовать динамические диски только на носителях, соединенных с внутренними контроллерами (а также с некоторыми eSATA-контроллерами). Хотя нельзя использовать динамические диски на портативных и съемных носителях на этих компьютерах, вы можете подсоединить такой диск к внутреннему контроллеру или допустимому eSATA-контроллеру, а затем использовать оснастку **Управление дисками**, чтобы импортировать диск.

Операционная система Windows Server 2012 R2 предоставляет средства, необходимые для конвертирования базового диска в динамический и обратно в базовый. При конвертировании диска в динамический разделы автоматически становятся томами надлежащего типа. Обратно преобразовать эти тома в разделы невозможно. Вместо этого необходимо удалить тома на динамическом диске, а затем преобразовать диск в базовый. Удаление томов уничтожает всю информацию на диске.

Конвертирование базового диска в динамический

Перед конвертированием базового диска в динамический нужно убедиться, что больше не понадобится загружать компьютер в старых версиях Windows. В случае с MBR-дисками также нужно удостовериться, что диск имеет хотя бы 1 Мбайт свободного места в конце диска. Хотя оснастка **Управление дисками** резервирует это пространство при создании разделов и томов, средства управления дисками других операционных систем могут этого не делать. Без свободного пространства в конце диска конвертировать диск не получится.

В случае с GPT нужно иметь непрерывные, распознанные разделы данных. Если GPT-диск содержит разделы, которые Windows не распознала, например, созданные другой операционной системой, невозможно конвертировать этот диск в динамический.

Следующее верно для диска любого типа.

- Должен быть как минимум 1 Мбайт свободного места в конце диска. Оснастка **Управление дисками** резервирует это пространство автоматически, средства управления дисками других операционных систем могут этого не делать.
- Невозможно использовать динамические диски на портативных компьютерах или на сменных носителях. Нельзя настроить эти диски только как базовые с первичными разделами.
- Невозможно конвертировать диск, если он содержит несколько инсталляций операционной системы Windows, если это так и сделать, можно будет запустить только систему, которая выполнила преобразование.

Для конвертирования базового диска в динамический выполните следующие действия:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши на базовом диске, который необходимо конвертировать (без разницы, какой режим использует-

ся — **Список дисков** или **Графическое представление**). Затем выберите команду **Преобразовать в динамический диск** (Convert To Dynamic Disk).

2. В окне **Преобразование в динамические диски** (Convert To Dynamic Disk) отметьте флажки напротив дисков, которые необходимо конвертировать. Нажмите кнопку **OK** для продолжения. Будет отображено окно **Диски для преобразования** (Disks To Convert), показывающее диски, которые будут конвертированы. Здесь имеются следующие кнопки и колонки:
   - **Имя** (Name) — номер диска;
   - **Оглавление диска** (Disk Contents) — тип и состояние разделов, например загрузочный раздел, активный раздел или используемый;
   - **Будет преобразован** (Will Convert) — будет ли диск преобразован. Если диск не соответствует критериям, он не будет преобразован, и нужно внести корректирующие действия, описанные ранее;
   - **Сведения** (Details) — тома на выбранном диске;
   - **Преобразовать** (Convert) — начинает преобразование.
3. Для начала преобразования нажмите кнопку **Преобразовать**. Оснастка **Управление дисками** предупредит, что после завершения преобразования будет невозможно загрузить предыдущие версии Windows с томов на выбранных дисках. Нажмите кнопку **Да** для продолжения.
4. Оснастка **Управление дисками** перезагрузит компьютер, если выбранный диск содержит загрузочный раздел, системный раздел или используется.

Преобразование динамического диска обратно в базовый

Перед преобразованием динамического диска в базовый необходимо удалить все динамические тома на этом диске. После этого щелкните правой кнопкой мыши на диске и выберите команду **Преобразовать в базовый диск** (Convert To Basic Disk). Это действие изменит тип диска на базовый. Затем можно создать новые разделы и логические диски.

Повторная активация диска

Если состояние динамического диска — **В сети (ошибки)** или **Вне сети**, повторная активация диска часто помогает решить проблему. Реактивировать диск можно так:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши по динамическому диску и выберите команду **Реактивировать диск**.
2. Если состояние диска не изменилось, перезагрузите компьютер. Если это не помогло решить проблему, проверьте сам диск, его контроллер и кабели. Также убедитесь, что диск правильно подключен и к нему поступает питание.

Повторная проверка дисков

Повторная проверка всех дисков в системе обновляет информацию о дисках на компьютерах. Повторная проверка иногда помогает решить проблему с дисками со стату-

сом **Не читается**. Пересканировать диски можно с помощью команды **Повторить проверку дисков** (Rescan Disks), выбранной из меню **Действие** оснастки **Управление дисками**.

Перемещение динамического диска в новую систему

Важное преимущество динамических дисков над базовыми заключается в том, что такие диски можно легко переместить с одного компьютера на другой. Например, если после установки компьютера обнаружится, что на этом компьютере не нужен дополнительный жесткий диск, можно переместить его в другой компьютер, где он будет использоваться рациональнее.

Операционная система Windows Server 2012 R2 значительно упрощает задачу перемещения дисков в новую систему. Перед перемещением дисков необходимо выполнить следующие действия:

1. Откройте оснастку **Управление дисками** в системе, где в данный момент установлены динамические диски. Проверьте состояние дисков и убедитесь, что все они находятся в состоянии **Исправен** (Healthy). Если состояние отличается от **Исправен**, нужно исправить все ошибки перед перемещением дисков.

   Примечание

   Диски с технологией BitLocker Drive Encryption не могут быть перемещены этим методом. Шифрование BitLocker Drive Encryption изолирует любое оффлайн-вмешательство в диск, в результате диск будет недоступен, пока администратор не разблокирует его.

2. Проверьте подсистемы жестких дисков исходного компьютера и компьютера, на который нужно перенести диски. Оба компьютера должны иметь одинаковые подсистемы. Если это не так, идентификатор Plug and Play системного диска исходного компьютера не совпадет с тем, что ожидает компьютер-назначение. В результате целевой компьютер не сможет загрузить правильные диски, и попытка загрузки не удастся.
3. Проверьте, являются ли динамические диски, которые необходимо переместить, частью составного, расширенного и чередующегося набора. Если это так, то нужно переместить весь набор вместе. При перемещении только части набора необходимо знать о последствиях. Для составных, расширенных или чередующихся томов перемещение только части набора сделает все связанные тома недоступными, как на исходном компьютере, так и на компьютере, куда перемещается диск.

После выполнения предыдущих, подготовительных, действий нужно выполнить следующие:

1. На исходном компьютере запустите оснастку **Управление компьютером**. Затем на левой панели выберите **Диспетчер устройств** (Device Manager). В списке устройств разверните узел **Дисковые устройства** (Disk Drives). Будет отображен список всех физических дисков компьютера. Щелкните на диске, который необходимо переместить, и выберите команду **Удалить** (Uninstall). Если вы не уверены, какие диски нужно удалить, щелкните правой кнопкой мыши по каждому диску и выберите команду **Свойства**. В окне **Свойства** перейдите на вкладку **Тома** (Volumes) и на-

жмите кнопку **Заполнить** (Populate). После этого будут отображены тома на выбранном диске.

2. Далее на исходном компьютере выберите узел **Управление дисками** в оснастке **Управление компьютером**. Если диск или диски, которые необходимо переместить, все еще перечислены в списке, щелкните правой кнопкой мыши на каждом из них и выберите команду **Изъять диск** (Remove Disk).
3. После выполнения этих процедур можно переместить динамические диски. Если диски являются дисками горячей замены и горячая замена поддерживается обоими компьютерами, извлеките диски из исходного компьютера и поместите их в целевой компьютер. В противном случае выключите оба компьютера, извлеките диски из исходного компьютера и затем установите их в компьютер назначения. По окончанию перезагрузите компьютеры.
4. На целевом компьютере запустите оснастку **Управление дисками** и выберите команду **Повторить проверку дисков** (Rescan Disks) в меню **Действие**. Когда оснастка **Управление дисками** завершит сканирование дисков, щелкните правой кнопкой мыши на каждом диске, помеченном как **Чужой**, и выберите команду **Импорт чужих дисков**.

> ***Примечание***
>
> В большинстве случаев тома на динамических дисках должны сохранить буквы дисков, которые им были присвоены на исходном компьютере. Однако если буква диска уже используется на целевом компьютере, том получит следующую доступную букву диска. Если у динамического тома ранее не было буквы диска, он не получит букву после перемещения в целевой компьютер. Вдобавок, если автомонтирование выключено, тома автоматически не будут смонтированы, и администратору нужно смонтировать их вручную и присвоить им буквы дисков.

Управление виртуальными дисками

Оснастка **Управление дисками** позволяет создавать, присоединять и отсоединять виртуальные жесткие диски. Создать виртуальный диск можно командой **Действие | Создать виртуальный жесткий диск** (Action | Create VHD). В окне **Создать и присоединить виртуальный жесткий диск** (Create And Attach Virtual Hard Disk) нажмите кнопку **Обзор**. Используйте окно **Просмотр файлов виртуального диска** (Browse Virtual Disk Files) для выбора места, в котором будет создан vhd-файл виртуального диска, введите его имя и нажмите кнопку **Сохранить** (Save).

В поле **Размер виртуального жесткого диска** (Virtual Hard Disk Size) введите размер диска в **МБ** (MB), **ГБ** (GB) или **ТБ** (TB). Укажите, должен ли файл виртуального жесткого диска расширяться до максимального размера по мере записи данных на него или же место для файла виртуального жесткого диска будет выделено в полном объеме независимо от объема данных, сохраненных на нем. После нажатия кнопки **OK** оснастка **Управление дисками** создаст виртуальный жесткий диск.

Виртуальный диск будет присоединен автоматически и добавлен как новый диск. Чтобы инициализировать диск для использования, щелкните по нему правой кнопкой мыши в графическом представлении и выберите команду **Инициализировать диск**.

В окне **Инициализация дисков** выберите диск для инициализации. Укажите стиль разделов — MBR или GPT — и нажмите кнопку **OK**.

После инициализации диска щелкните правой кнопкой мыши по нераспределенному пространству на диске и создайте том нужного типа. После создания тома VHD будет доступен для использования.

Как только VHD будет создан, присоединен, инициализирован и отформатирован, с ним можно будет работать точно так же, как и с другими дисками: записывать и читать данные; даже можно загрузить компьютер с VHD. Виртуальный диск может быть переведен в состояние **В сети** и **Вне сети**, для этого щелкните на диске правой кнопкой мыши в графическом представлении и выберите команду **В сети** и **Вне сети** соответственно. Если VHD больше не нужен, его можно отсоединить. Для этого в графическом представлении щелкните правой кнопкой мыши по диску и выберите команду **Отсоединить виртуальный жесткий диск** (Detach VHD), а затем нажмите кнопку **OK** в окне **Отсоединить виртуальный жесткий диск** (Detach Virtual Hard Disk).

Возможно использование виртуальных дисков, созданных другими программами. Если VHD создан в другой программе или нужно присоединить отключенный VHD, выполните эти действия:

1. В оснастке **Управление дисками** выберите команду **Присоединить виртуальный жесткий диск** (Attach VHD) из меню **Действие**.
2. В окне **Присоединить виртуальный жесткий диск** нажмите кнопку **Обзор**. Используйте окно **Просмотр файлов виртуального диска** для выбора vhd-файла и нажмите кнопку **Открыть** (Open).
3. Если нужно подключить VHD в режиме "только для чтения", выберите опцию **Только для чтения** (Read-Only). Нажмите кнопку **OK** для подключения VHD.

Использование базовых дисков и разделов

При установке нового компьютера или обновлении уже существующего часто нужно создать разделы на дисках компьютера. Для этого используется оснастка **Управление дисками**.

Основы управления разделами

В Windows Server 2012 R2 физический диск, использующий стиль разделов, может иметь до четырех первичных разделов и один расширенный раздел. Это позволяет настраивать MBR-диски одним из двух способов: или использовать четыре первичных раздела, или использовать от одного до трех первичных разделов и один расширенный раздел. Основной раздел может заполнить весь диск или же можно установить подходящий для рабочей станции или сервера размер. В расширенном разделе допускается создание одного или больше логических дисков. *Логический диск* — это просто секция раздела с его собственной файловой системой. Обычно логические диски используются, чтобы разделить большой диск на управляемые разделы. При желании можно разделить расширенный раздел размером 600 Гбайт на три логических диска по 200 Гбайт. У физических дисков со стилем разделов GPT может быть до 128 разделов.

После разделения диска на разделы нужно отформатировать их, чтобы присвоить буквы логическим дискам. Речь идет о высокоуровневом форматировании, создающем структуру файловой системы, а не о низкоуровневом, инициализирующем диск для начального использования. Все мы знакомы с диском C:, используемым Windows Server 2012 R2. Диск C: — это просто указатель раздела диска. Если диск поделен на несколько разделов, у каждого раздела будет своя буква диска. Буквы дисков используются для доступа к файловым системам на разных разделах физического диска. В отличие от MS-DOS, которая присваивает буквы дисков автоматически, начиная с буквы C, Windows Server 2012 R2 позволяет администратору определять буквы дисков. Обычно доступны буквы от C до Z.

> ***Примечание***
>
> Буква диска A назначается системой дисководу для гибких дисков. Если система обнаружит второй дисковод для гибких дисков, она назначит ему букву B. Поэтому администратору доступны только буквы C–Z. Помните, что DVD-диски и другие типы сменных дисков также нуждаются в букве дисков. Общее количество букв дисков, которые можно использовать, — 24. Если необходимы дополнительные тома, используйте пути дисков.

Доступно всего 24 буквы диска. Чтобы преодолеть это ограничение, можно монтировать диск к путям дисков. Путь диска[1] — это каталог, через который осуществляется доступ к другому диску. Например, в системе могут быть дополнительные диски E:\Data1, E:\Data2 и E:\Data3. Пути дисков можно использовать с базовыми и динамическими дисками. Есть только одно ограничение — пути дисков должны быть пустыми папками на NTFS-дисках.

Чтобы было проще различать первичные и расширенные разделы в оснастке **Управление дисками**, используются цветовые коды. Например, темно-синей полосой отмечаются первичные разделы, а логические диски в расширенном разделе отмечаются голубой полосой. Ключ для цветовой схемы показан внизу окна оснастки **Управление дисками**. Изменить цвета можно в диалоговом окне **Параметры** (Settings), которое появится при выборе команды **Параметры** (Settings) в меню **Вид** (View).

Создание разделов и простых томов

ОС Windows Server 2012 R2 упрощает интерфейс пользователя оснастки **Управление дисками**, используя один набор диалоговых окон и мастеров для разделов и томов. Первые три тома на базовом диске создаются автоматически как первичные разделы. При попытке создать четвертый том на базовом диске оставшееся пространство на диске будет автоматически преобразовано в расширенный раздел. Любые последующие тома автоматически создаются в расширенных разделах как логические диски.

В оснастке **Управление дисками** создаются разделы, логические диски и простые тома:

1. В графическом представлении оснастки **Управление дисками** щелкните правой кнопкой мыши на нераспределенной или свободной области, а затем выберите команду **Создать простой том** (New Simple Volume). Будет запущен мастер создания простых томов (New Simple Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку **Далее**.

---

[1] Путь диска — это аналог точки монтирования в UNIX. — *Прим. пер.*

2. Появится страница **Указание размера тома** (Specify Volume Size) (рис. 10.3), показывающая минимальный и максимальный размеры тома в мегабайтах. Введите размер создаваемого тома в пределах ограничений в поле **Размер простого тома (МБ)** (Simple volume size in MB) и нажмите кнопку **Далее**.

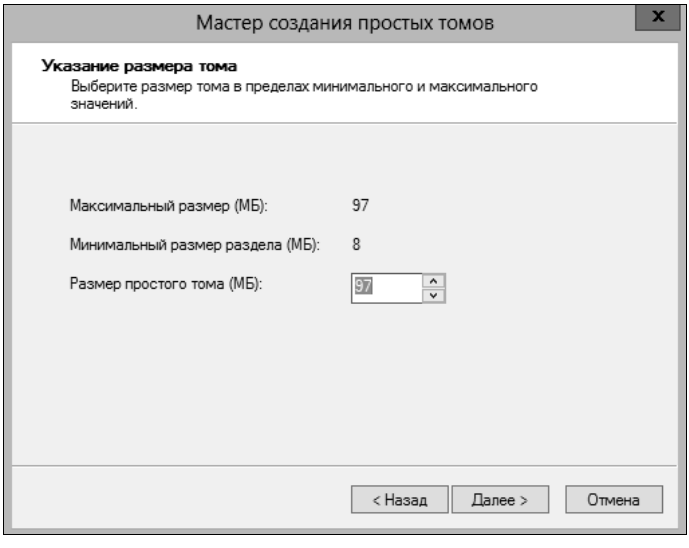


Рис. 1.3. Установите размер тома на странице **Указание размера тома**

3. На странице **Назначение буквы диска или пути** (Assign Drive Letter or Path) (рис. 1.4) укажите, что нужно назначить букву диска или путь, а затем нажмите кнопку **Далее**. Доступны следующие опции.

   - **Назначить букву диска** (Assign the following drive letter) — выберите эту опцию, чтобы назначить букву диска. Затем выберите доступную букву в предоставленном списке. По умолчанию Windows Server 2012 R2 выбирает наименьшую доступную букву диска и исключает зарезервированные буквы, назначенные локальным и сетевым дискам.
   - **Подключить том как пустую NTFS-папку** (Mount in the following empty NTFS folder) — выберите эту опцию для монтирования раздела к пустой NTFS-папке. Затем нужно ввести путь к существующей папке или же нажать кнопку **Обзор** для поиска или создания папки, которая будет использоваться.
   - **Не назначать буквы диска или пути диска** (Do not assign a drive letter or drive path) — выберите эту опцию, если нужно создать раздел без назначения разделу буквы или пути. Если позже нужно назначить разделу букву или диск, это можно сделать в любое время.

Примечание

Допускается не присваивать томам буквы диска или путь. Том без указателей будет размонтирован и по большей части неприменим. Размонтированный том может быть смонтирован с присвоением буквы диска или пути позже *(см. разд. "Назначение буквы диска или путей" главы 2)*.

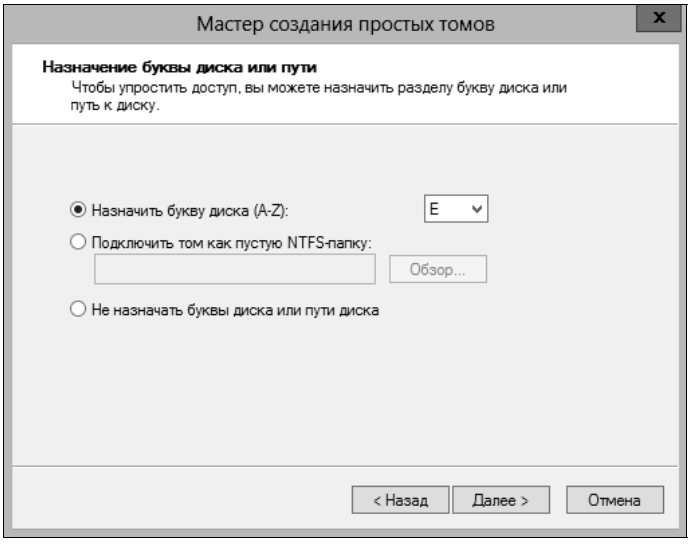


Рис. 1.4. На странице **Назначение буквы диска или пути** можно назначить указатель диска или сделать это позже

4. На странице **Форматирование раздела** (Format Partition) (рис. 1.5) определите, будет ли отформатирован том. Если это необходимо сделать, установите переключатель **Форматировать этот том следующим образом** (Format this volume with the following settings) и укажите следующие параметры.

   - **Файловая система** (File system) — выберите тип файловой системы: FAT, FAT32, exFAT, NTFS или ReFS. Типы файловых систем доступны в зависимости от размера форматируемого тома. При использовании FAT32 можно позже конвертировать том в NTFS утилитой Convert. Однако нельзя конвертировать NTFS-разделы в FAT32.
   - **Размер кластера** (Allocation unit size) — устанавливает размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно задать определенный размер кластера. При наличии большого количества маленьких файлов можно установить наименьший размер кластера, например 512 или 1024 байта. Так маленькие файлы используют меньше дискового пространства. Обратите внимание, что у томов ReFS фиксированный размер кластера, и его нельзя изменить.
   - **Метка тома** (Volume label) — устанавливает текстовую метку раздела. Эта метка — имя тома раздела и по умолчанию используется значение **Новый том** (New Volume). Метку тома можно изменить в любое время, щелкнув по диску правой кнопкой мыши в окне Проводника и выбрав команду **Свойства**. Новую метку можно ввести в поле **Метка** (Label) на вкладке **Общие**.
   - **Быстрое форматирование** (Perform a quick format) — указывает операционной системе Windows Server 2012 R2, что нужно отформатировать раздел без провер-

ки ошибок. На больших разделах эта опция может сэкономить несколько минут. Однако обычно лучше производить проверку на ошибки, в результате которой оснастка **Управление дисками** пометит плохие секторы диска и заблокирует их.

- **Применять сжатие файлов и папок** (Enable file and folder compression) — включает сжатие для диска. Встроенное сжатие доступно только для файловой системы NTFS (и не поддерживается FAT, FAT32, exFAT и ReFS). При использовании NTFS сжатие станет прозрачным для пользователей, и доступ к сжатым файлам ничем не будет отличаться от доступа к обычным файлам. При выборе этой опции файлы и каталоги на этом диске автоматически будут сжиматься. Более подробную информацию о сжатых дисках, файлах *см. в разд. "Сжатие дисков и данных" далее в этой главе*.

5. Нажмите кнопку **Далее**, подтвердите выбранные параметры и нажмите кнопку **Готово**.

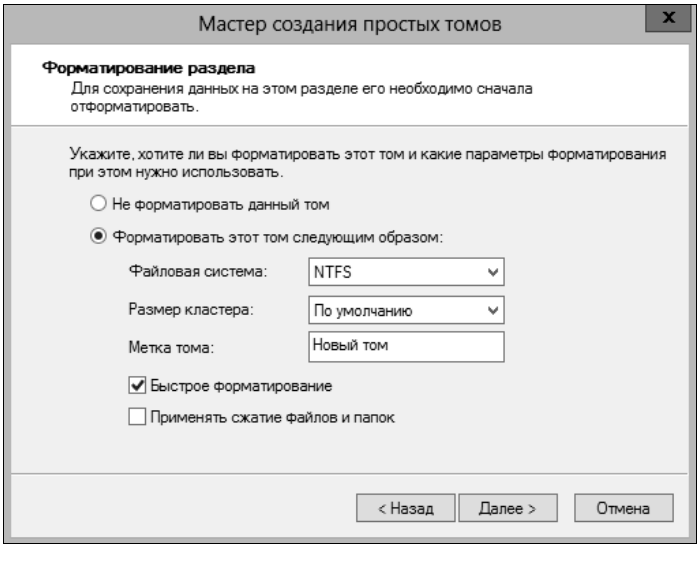


Рис. 1.5. Установите параметры форматирования на странице **Форматирование раздела**

Форматирование разделов

Форматирование делит файловую систему на разделы и удаляет все существующие данные. Здесь идет речь о высокоуровневом форматировании, создающем структуру файловой системы, а не о низкоуровневом, инициализирующем диск для начального использования. Для форматирования раздела щелкните на нем правой кнопкой мыши и выберите команду **Форматировать** (Format). Откроется окно **Форматирование** (Format), показанное на рис. 1.6.

Параметры форматирования:

- **Метка тома** (Volume label) — текстовая метка для раздела. Эта метка — имя тома раздела;

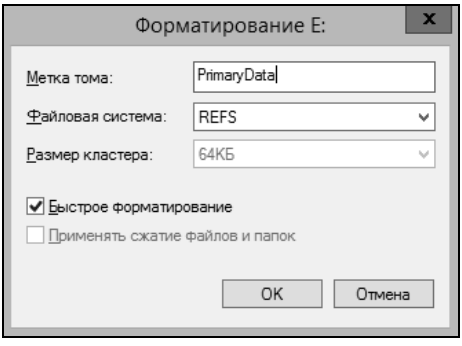


Рис. 1.6. Окно **Форматирование** позволяет выбрать файловую систему и установить метку диска

- **Файловая система** (File system) — тип файловой системы — FAT, FAT32, exFAT, NTFS или ReFS. Доступные типы файловых систем зависят от размера форматируемого тома;
- **Размер кластера** (Allocation unit size) — размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно задать определенный размер кластера. При наличии большого количества маленьких файлов можно установить наименьший размер кластера, например 512 или 1024 байта. Так маленькие файлы используют меньше дискового пространства;
- **Быстрое форматирование** (Perform a quick format) — указывает ОС Windows Server 2012 R2, что нужно отформатировать раздел без проверки ошибок. На больших разделах эта опция может сэкономить несколько минут. Однако обычно лучше производить проверку на ошибки, в результате которой оснастка **Управление дисками** пометит плохие секторы диска и заблокирует их.

Для продолжения нажмите кнопку **OK**. Поскольку форматирование раздела разрушает все существующие данные, оснастка **Управление дисками** предоставляет последний шанс отменить эту процедуру. Нажмите кнопку **OK** для начала форматирования раздела. Оснастка **Управление дисками** изменяет состояние диска и отображает процент завершения форматирования. По завершению форматирования состояние диска будет вновь изменено.

Сжатие дисков и данных

При форматировании диска для файловой системы NTFS Windows Server 2012 R2 позволяет включить встроенную функцию сжатия. При включенном сжатии все файлы и каталоги, хранящиеся на диске, автоматически будут сжиматься при создании. Поскольку сжатие прозрачно для пользователя, то к сжатым данным пользователь получает доступ точно так же, как к обычным файлам. Разница в том, что на сжатый диск можно записать больше данных.

Внимание!

Проводник отмечает имена сжатых ресурсов синим цветом. Также нужно знать, что ReFS не поддерживает сжатия NTFS.

Практический совет

Несмотря на то, что сжатие — конечно, полезная функция, когда нужно сэкономить дисковое пространство, однако нельзя зашифровать сжатые данные. Сжатие и шифрование — это взаимоисключающие функции для NTFS-томов: можно использовать либо сжатие, либо шифрование. Нельзя использовать оба метода. Для получения дополнительной информации о шифровании *см. разд. "Шифрование дисков и данных" далее в этой главе*. При попытке сжать зашифрованные данные Windows Server 2012 R2 автоматически расшифрует их, а затем выполнит сжатие. Аналогично, при попытке зашифровать сжатые данные Windows Server 2012 R2 сначала распакует их, а затем зашифрует.

Сжатие дисков

Для сжатия диска и всего его содержимого выполните следующие действия:

1. В Проводнике или оснастке **Управление дисками** щелкните правой кнопкой мыши по диску, который нужно сжать, и выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** отметьте флажок **Сжать этот диск для экономии места** (Compress drive to save disk space) и нажмите кнопку **OK**.
3. В окне **Подтверждение изменения атрибутов** (Confirm Attribute Changes) выберите применение ко всем подпапкам и файлам и нажмите кнопку **OK**.

Сжатие каталогов и файлов

Если не нужно сжимать весь диск, Windows Server 2012 R2 позволяет сжать каталоги и файлы выборочно. Для сжатия файла или папки выполните такие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или каталоге, который нужно сжать, а затем выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** нажмите кнопку **Другие**. В окне **Дополнительные атрибуты** (Advanced Attributes) установите флажок **Сжимать содержимое для экономии места на диске** (Compress contents to save disk space). Нажмите кнопку **OK** дважды.

В случае с файлом Windows Server помечает файл как сжатый и затем сжимает его. В случае с каталогом Windows Server отмечает его как сжатый и затем сжимает все файлы в нем. Если каталог содержит подпапки, Windows Server выводит на экран диалоговое окно, позволяющее сжать все подпапки в выбранном каталоге. Просто установите переключатель **К данной папке и ко всем вложенным папкам и файлам** (Apply changes to this folder, subfolders, and files) и нажмите кнопку **OK**. После сжатия каталога любые новые файлы, добавленные или скопированные в этот каталог, будут автоматически сжаты.

Примечание

При перемещении несжатого файла с другого диска этот файл будет сжат. Однако если перемещается несжатый файл в сжатую папку на том же NTFS-диске, файл не будет сжат. Заметьте также, что нельзя зашифровать сжатые файлы.

Декомпрессия сжатых дисков

Проводник отмечает имена сжатых файлов и папок синим цветом. Действия по декомпрессии сжатых дисков таковы:

1. В Проводнике или в оснастке **Управление дисками** щелкните правой кнопкой мыши по диску, который нужно развернуть (декомпрессировать), и выберите команду **Свойства**.
2. Снимите флажок **Сжать этот диск для экономии места** и нажмите кнопку **OK**.
3. В окне **Подтверждение изменения атрибутов** выберите применение ко всем подпапкам и файлам и нажмите кнопку **OK**.

> ***Совет***
>
> Windows всегда проверяет доступное дисковое пространство перед разворачиванием сжатых данных. Если доступное свободное пространство меньше, чем нужно, невозможно завершить декомпрессию. Например, если сжатый диск использует 150 Гбайт пространства, но свободного пространства всего 70 Гбайт, то дискового пространства будет недостаточно, чтобы развернуть данные. Обычно нужно в 1,5–2 раза больше свободного пространства, чем сжато данных.

Декомпрессия сжатых каталогов и файлов

Если необходимо развернуть сжатый файл или папку, выполните эти действия:

1. В Проводнике щелкните правой кнопкой мыши по файлу или каталогу и выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** нажмите кнопку **Другие**. В окне **Дополнительные атрибуты** снимите флажок **Сжимать содержимое для экономии места на диске**. Нажмите кнопку **OK** дважды.

В случае с файлами Windows Server удаляет атрибут сжатия и разворачивает файл. В случае с каталогами Windows Server декомпрессирует все файлы в каталоге. Если каталог содержит подпапки, можно также удалить сжатие и с подпапок. Чтобы сделать это, выберите переключатель **К данной папке и ко всем вложенным папкам и файлам** и нажмите кнопку **OK**.

> ***Совет***
>
> Для сжатия и декомпрессии данных в Windows Server можно также использовать утилиты командной строки. Для сжатия используется утилита `compact` (Compact.exe), а для распаковки — утилита `expand` (Expand.exe).

Шифрование дисков и данных

У файловой системы NTFS есть много преимуществ над другими файловыми системами. Одно из основных преимуществ — возможность автоматического шифрования и расшифровки данных с использованием шифрованной файловой системы (Encrypting File System, EFS). При шифровании данных добавляется экстрауровень защиты важных данных, и этот экстрауровень работает как полная защита, блокирующая доступ всех

других пользователей к содержимому зашифрованных файлов. Одно из преимуществ шифрования в том, что только конкретный пользователь может получить доступ к данным. Это преимущество — также и недостаток, ведь пользователь должен расшифровать данные прежде, чем авторизованные пользователи смогут получить к ним доступ.

> ***Примечание***
>
> Как было упомянуто ранее, невозможно зашифровать сжатые файлы. Шифрование и сжатие — взаимоисключающие функции NTFS. Можно использовать одну из этих функций, но не обе одновременно. Заметьте, что ReFS не поддерживает этот тип шифрования.

Шифрование и файловая система EFS

Файловая система EFS позволяет зашифровать как отдельные файлы, так и целые каталоги. Любой файл, помещенный в зашифрованную папку, автоматически будет зашифрован. Зашифрованные файлы могут быть прочитаны только тем лицом, кто их зашифровал. Прежде чем другие пользователи смогут прочитать зашифрованный файл, пользователь должен расшифровать файл или добавить в файл ключ шифрования пользователя.

У каждого зашифрованного файла должен быть уникальный ключ шифрования пользователя, создавшего файл, точнее, того, кто в данный момент является владельцем файла. Зашифрованный файл может быть скопирован, перемещен или переименован, как любой другой файл, и в большинстве случаев эти файлы никак не отражаются на шифровании данных *(более подробно см. разд. "Работа с зашифрованными файлами и папками" далее в этой главе)*. Пользователь, зашифровавший файл, всегда имеет доступ к файлу при условии, что сертификат пользователя с открытым ключом доступен на компьютере, который он использует. Для этого пользователя процесс шифрования и дешифрования обрабатывается автоматически и полностью прозрачно.

EFS — это процесс, выполняющий шифрование и расшифровку. Настройки по умолчанию для EFS позволяют пользователям зашифровывать файлы без специальных полномочий. Файлы шифруются с использованием публичного/частного ключа, которые EFS автоматически генерирует для каждого пользователя.

Сертификаты шифрования хранятся как часть данных в профиле пользователя. Если пользователь работает с несколькими компьютерами и желает использовать шифрование, администратор должен настроить перемещаемый профиль для этого пользователя. Перемещаемый профиль гарантирует, что данные профиля пользователя и сертификаты публичного ключа будут доступны с других компьютеров. Без этого пользователь не сможет получить доступ к своим зашифрованным файлам на другом компьютере.

> ***Внимание!***
>
> Альтернативой перемещаемому профилю может стать копирование сертификата шифрования пользователя на компьютеры, которые он должен использовать. О том, как сделать это, рассказано в *главе 11*. Просто заархивируйте сертификат пользователя на исходном компьютере и восстановите его на каждом компьютере, который использует пользователь.

У EFS есть встроенная система восстановления данных, защищающая от потери данных. Эта система восстановления позволяет убедиться, что зашифрованные данные

могут быть восстановлены, если сертификат публичного ключа пользователя будет потерян или удален. Наиболее вероятный сценарий этого — удаление учетной записи пользователя после его увольнения. У руководителя должна быть возможность войти в учетную запись пользователя, проверить файлы и сохранить важные файлы в другие папки, но если учетная запись пользователя была удалена, зашифрованные файлы будут доступны, только если было отключено шифрование или файлы перемещены в файловые системы exFAT, FAT или FAT32 (где шифрование не поддерживается).

Для доступа к зашифрованным файлам после удаления учетной записи пользователя нужно использовать агент восстановления. Агент восстановления имеет доступ к ключу шифрования файла и при необходимости может разблокировать данные в зашифрованных файлах. Однако для защиты важных данных агент восстановления не имеет доступа к приватному ключу пользователя.

Windows Server не будет расшифровывать файлы без назначенных агентов восстановления EFS. Поэтому агенты восстановления назначаются автоматически, также автоматически генерируются сертификаты, необходимые для восстановления. Это гарантия, что зашифрованные файлы всегда будут восстановлены.

Агенты восстановления EFS настраиваются на двух уровнях.

- **Домен.** Агент восстановления для домена настраивается автоматически при первой установке первого контроллера домена Windows Server. По умолчанию агент восстановления — это администратор домена. С помощью групповой политики администраторы домена могут назначить дополнительных агентов восстановления. Администраторы также могут делегировать привилегии агентов восстановления определенным администраторам безопасности.
- **Локальный компьютер.** Когда компьютер — часть рабочей группы или же полностью автономен, агент восстановления — по умолчанию администратор локального компьютера. Дополнительные агенты восстановления могут быть назначены. В дальнейшем, если нужно в среде домена использовать локальных агентов восстановления, а не агентов восстановления уровня домена, необходимо удалить политику восстановления из групповой политики домена.

Агенты восстановления можно удалить, если в них нет необходимости. Однако, если удалить всех агентов восстановления, EFS больше не сможет шифровать файлы. Для работы функции EFS нужно настроить одного или более агента восстановления.

Шифрование каталогов и файлов

При использовании файловой системы NTFS операционная система Windows Server позволяет выбрать файлы и каталоги для шифрования. Когда файл зашифрован, данные файла конвертируются в зашифрованный формат, который может быть прочитан только лицом, которое зашифровало файл. Пользователи могут зашифровывать файлы, только если у них есть надлежащие права доступа. При шифровании папки она отмечается как зашифрованная, но на самом деле шифруются только файлы внутри нее. Все файлы, которые были созданы или добавлены в зашифрованную папку, шифруются автоматически. Проводник отмечает имена зашифрованных объектов зеленым цветом.

Для шифрования файла или каталога выполните эти действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или каталоге, который нужно зашифровать, и выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** нажмите кнопку **Другие**, а затем установите флажок **Шифровать содержимое для защиты данных** (Encrypt contents to secure data). Нажмите кнопку **OK** дважды.

> ***Примечание***
>
> Невозможно зашифровать сжатые файлы, системные файлы и файлы с атрибутом "только для чтения". При попытке зашифровать сжатые файлы они будут автоматически распакованы, а затем зашифрованы. При попытке зашифровать системные файлы будет отображено сообщение об ошибке.

В случае с отдельными файлами Windows Server помечает файлы как зашифрованные и затем шифрует их. В случае с каталогами Windows Server отмечает каталог как зашифрованный и затем шифрует все файлы в нем. Если каталог содержит подпапки, Windows отобразит окно, позволяющее зашифровать все вложенные подпапки. Просто установите переключатель **К данной папке и ко всем вложенным папкам и файлам** (Apply changes to this folder, subfolders, and files) и нажмите кнопку **OK**.

> ***Примечание***
>
> На NTFS-томах файлы остаются зашифрованными, даже если их переместить, скопировать или переименовать. Если скопировать или переместить зашифрованный файл на exFAT, FAT или FAT32, файл автоматически будет расшифрован перед копированием или перемещением. Для копирования или перемещения файла нужны надлежащие полномочия.

Чтобы предоставить специальный доступ к зашифрованному файлу или каталогу, щелкните правой кнопкой мыши на файле или папке в окне Проводника и выберите команду **Свойства**. На вкладке **Общие** окна **Свойства** нажмите кнопку **Другие**. В окне **Дополнительные атрибуты** нажмите кнопку **Подробно** (Details). В появившемся окне будут перечислены пользователи, обладающие доступом к зашифрованному файлу. Чтобы предоставить другому пользователю доступ к файлу, нажмите кнопку **Добавить**. Если доступен сертификат пользователя, выберите имя пользователя в предоставленном списке и нажмите кнопку **OK**. В противном случае нажмите кнопку **Найти пользователя** (Find user) для выбора сертификата пользователя.

Работа с зашифрованными файлами и папками

Ранее было отмечено, что можно копировать, перемещать и переименовывать зашифрованные файлы и папки подобно любым другим файлам. Это так, но была оговорка — "в большинстве случаев". При работе с зашифрованными файлами, пока они находятся на NTFS-томах того же компьютера, проблем не будет. При работе с другими файловыми системами или компьютерами можно столкнуться с настоящими проблемами. Наиболее вероятны два следующих сценария.

- **Копирование между томами одного и того же компьютера.** При копировании или перемещении зашифрованных файлов или папок с одного NTFS-тома на другой NTFS-том на том же компьютере файлы остаются зашифрованными. Однако, если скопировать или переместить зашифрованные файлы на FAT-том, файлы будут

расшифрованы перед передачей и преобразованы в стандартные файлы, поэтому скопированы будут незашифрованные файлы. Файловая система FAT не поддерживает шифрование.

- **Копирование между томами на разных компьютерах.** При копировании или перемещении зашифрованных файлов или папок с одного NTFS-тома на другой NTFS-том на другом компьютере файлы останутся зашифрованными, пока целевой компьютер позволяет шифровать файлы и удаленному компьютеру доверяют делегирование. В противном случае файлы будут расшифрованы и затем переданы как обычные файлы. То же самое произойдет при копировании или перемещении файлов на FAT-том на другом компьютере. Файловая система FAT не поддерживает шифрование.

После копирования важных зашифрованных файлов нужно убедиться, что шифрование все еще применено. Щелкните на файле правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Общие** окна **Свойства** нажмите кнопку **Другие**. Убедитесь, что параметр **Шифровать содержимое для защиты данных** (Encrypt contents to secure data) включен.

Настройка политики восстановления

Политики восстановления автоматически настраиваются для контроллеров домена и рабочих станций. По умолчанию контроллеры домена назначаются агентами восстановления для доменов, а локальные администраторы — агентами восстановления для автономных рабочих станций.

GPMC (Group Policy Management Console) — это компонент, который вы можете добавить в любую установку Windows Server 2008 и более поздних версий, используя мастер добавления ролей и компонентов (Add Roles And Features Wizard). GPMC также доступна на рабочих столах Windows при установке RSAT (Remote Server Administration Tools). Как только консоль GPMC будет установлена, ее команда будет доступна в меню **Средства** в диспетчере серверов. Используя GMPC, вы можете просматривать, назначать и удалять агенты восстановления, используя следующие шаги:

1. Чтобы в GPMC открыть объект групповой политики (GPO), щелкните по нему правой кнопкой мыши и выберите команду **Изменить** (Edit) из контекстного меню. GPMC откроет редактор управления групповыми политиками, предназначенный для управления настройками политики.
2. Разверните узел **Агент восстановления зашифрованных данных** (Encrypted Data Recovery Agents) в групповой политике. Для этого разверните узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики открытого ключа\Шифрованная файловая система (EFS)** (Computer Configuration\ Windows Settings\Security Settings\Public Key Policies\Encrypting File System).
3. На правой панели отображается список назначенных в данный момент сертификатов восстановления. Для каждого сертификата выводится, кто его выпустил, дата истечения, назначение и т. д.
4. Для назначения дополнительных агентов восстановления щелкните правой кнопкой мыши на узле **Шифрованная файловая система (EFS)** (Encrypting File System) и

выберите команду **Добавить агент восстановления данных** (Add Data Recovery Agent). Будет запущен мастер добавления агента восстановления (Add Recovery Agent Wizard), который используется для выбора ранее сгенерированных сертификатов, назначенных пользователю. Затем можно пометить выбранный сертификат как назначенный сертификат восстановления. Нажмите кнопку **Далее**.

5. На странице **Выбор агентов восстановления** (Select Recovery Agents) можно выбрать сертификаты, опубликованные в Active Directory, или использовать файлы сертификатов. Если нужно применить опубликованный сертификат, нажмите кнопку **Обзор каталога** (Browse Directory), используйте окно **Поиск: Пользов., контакты и группы** (Find Users, Contacts, And Groups), выберите пользователя. Будет предоставлена возможность применять опубликованный сертификат этого пользователя. Если нужно использовать файл сертификата, нажмите кнопку **Обзор папок**. В окне **Открытие** (Open) выберите необходимый файл сертификата.

   Внимание!

   Перед назначением дополнительных агентов восстановления нужно рассмотреть настройку корневого центра сертификации в домене. Затем можно использовать оснастку **Сертификаты** (Certificates) для создания персональных сертификатов, которые используют шаблон EFS Recovery Agent. Корневой центр сертификации должен потом утвердить запрос сертификата, чтобы тот мог использоваться.

6. Для удаления агента восстановления выберите сертификат агента восстановления в правой панели и нажмите кнопку **Удалить**. Затем нажмите кнопку **Да** для удаления сертификата без возможности восстановления. Если политика безопасности пуста (это означает, что не назначено выделенных агентов восстановления), EFS будет выключена так, что файлы больше не будут зашифровываться, а существующие уже зашифрованные ресурсы EFS не будут иметь агента восстановления.

Расшифровка файлов и каталогов

Проводник отмечает зеленым цветом имена зашифрованных файлов. Для расшифровки файла или каталога выполните такие действия:

1. В Проводнике щелкните по файлу или каталогу правой кнопкой мыши и выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** нажмите кнопку **Другие**. Установите флажок **Шифровать содержимое для защиты данных**. Нажмите кнопку **OK** дважды.

В случае с файлами Windows Server расшифрует и восстановит файл в его исходный формат. В случае с папками Windows Server расшифрует все файлы внутри папки. Если каталог содержит подпапки, будет предоставлена возможность снять шифрование и с подпапок. Для этого выберите переключатель **К данной папке и ко всем вложенным папкам и файлам** (Apply Changes To This Folder, Subfolders, And Files) и нажмите кнопку **OK**.

Совет

Windows Server также предоставляет утилиту командной строки `Cipher` (Cipher.exe), которая используется для шифрования и расшифровки данных. Запуск `Cipher` в командной строке без дополнительных параметров выведет состояние шифрования всех папок в текущем каталоге.

ГЛАВА 2

Настройка носителей данных

Управление хранилищем существенно изменилось за прошедшие несколько лет, как и технологии, которые Microsoft Windows Server использует для работы с дисками. Хотя традиционные методы управления хранилищем относятся к физическим дискам, расположенным в сервере, сегодня много серверов использует присоединенные хранилища и виртуальные диски.

Обычно при работе с внутренними жесткими дисками нужно часто выполнять процедуры настройки диска: создание томов или настройку избыточного массива независимых жестких дисков (Redundant Array of Independent Disks, RAID). Администратор создает тома или массивы, которые могут состоять из нескольких дисков, и при этом он знает точное физическое расположение тех дисков.

При работе с присоединенным хранилищем администратор может не знать, на каком физическом диске или дисках находится том, с которым он работает. Вместо этого используется виртуальный диск, называемый также LUN (Logical Unit Number), который является логическим указателем на часть подсистемы хранения. Несмотря на то, что виртуальный диск может находиться на одном или более физических дисках, разметка физических дисков контролируется отдельно от операционной системы (подсистемой хранения).

Когда мне нужно выбрать между двумя методами управления, я сначала обращаюсь к традиционному методу, а затем к методу на основе стандартов. В этой главе сначала будут рассмотрены традиционные методы создания массива томов, а потом стандартизированные методы. Управление томом осуществляется одинаково, независимо от того, используется ли традиционный подход или подход на основе стандартов. Поэтому в заключительном разделе этой главы будут рассмотрены методы работы с существующими томами и дисками.

Практический совет

Способы стандартизированного управления хранилищами могут быть использованы также с внутренними дисками сервера. Когда внутренние диски применяются таким образом (как виртуальные диски, подключенные к хранилищу), выделенные ресурсы будут использовать стандартизированные методы. Это означает, что можно создать тома виртуального диска на физических дисках, добавить физические диски к пулам носителей данных, а также соз-

дать виртуальные диски iSCSI. Также можно включить дедупликацию данных на своих виртуальных дисках. Однако нельзя использовать массив томов и функции RAID операционной системы. Причина заключается в том, что способы стандартизированного управления хранилищем основываются на подсистеме хранения для управления архитектурой физического диска.

Использование томов и массивов томов

Массивы томов и RAID-массивы создаются на динамических дисках. При использовании массива томов можно создать один том, состоящий из нескольких дисков. Пользователи могут получить доступ к этому тому, как будто это единственный диск, независимо от того, сколько дисков входит в состав тома. Том, находящийся на одном диске, называется *простым томом*. Том, охватывающий множество дисков, называется *составным томом*.

С помощью RAID-массивов можно защитить важные деловые данные и в некоторых случаях улучшить производительность дисков. RAID может быть реализован посредством встроенных функций операционной системы (программный RAID) или с помощью аппаратных средств (аппаратный RAID). Windows Server 2012 R2 поддерживает три уровня программного RAID: 0, 1 и 5. RAID-массивы реализуются как зеркальные, чередующиеся и чередующиеся с контролем четности.

Создание и управление томами осуществляется так же, как создание и управление разделами. Том — это часть диска, которую можно использовать для хранения данных непосредственно.

Примечание

При использовании составных и чередующихся томов на базовых дисках можно удалить том, но нельзя создать или расширить том. При использовании зеркальных томов на базовых дисках можно удалять, чинить и синхронизировать зеркало. Также можно разбить зеркало. При использовании чередования с контролем четности (RAID 5) на базовых дисках можно удалить или починить том, но нельзя создать новые тома.

Базовые тома

В оснастке **Управление дисками** тома разных типов помечаются цветом аналогично разделам. На рис. 2.1 показано, что тома имеют следующие свойства:

- **Расположение** (Layout) — может быть: простой, составной, зеркальный чередующийся и чередующийся с контролем четности;
- **Тип** (Type) — тома всегда имеют тип *динамический*;
- **Файловая система** (File System) — подобно разделам, каждый том может иметь собственную файловую систему, например FAT или NTFS. Обратите внимание, что FAT16 доступна только, если размер раздела или тома 2 Гбайт или меньше;
- **Состояние** (Status) — состояние диска. В графическом представлении показано состояние диска как **Исправен** (Healthy), **Отказавшая избыточность** (Failed Redundancy) и т. д. В следующем разделе мы обсудим массивы томов и различные состояния;

- **Емкость** (Capacity) — емкость диска;
- **Свободно** (Free Space) — сколько свободного пространства осталось на томе;
- **Свободно %** (% Free) — процентное соотношение свободного пространства к емкости тома.

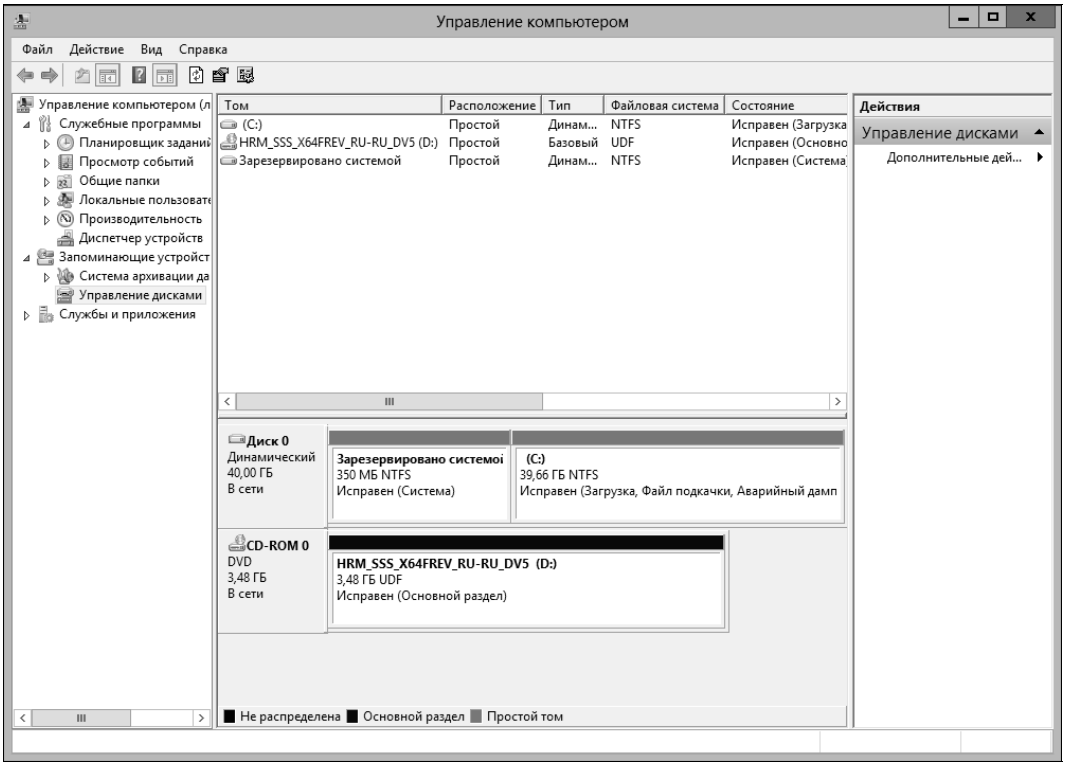


Рис. 2.1. Окно **Управление компьютером** отображает тома как разделы

Важное преимущество динамических томов по сравнению с базовыми томами в том, что они позволяют вносить изменения в тома и диски без необходимости перезапуска системы (в большинстве случаев). Тома также позволяют использовать улучшения отказоустойчивости Windows Server 2012 R2. Можно установить другие операционные системы и использовать двойную загрузку. Чтобы сделать это, нужно создать отдельный том для другой операционной системы. Например, можно установить Windows Server 2012 R2 на томе C, а Windows 8.1 на томе D.

С томами можно сделать следующее:

- назначать буквы и пути дисков, как будет описано в *разд. "Назначение буквы диска или путей" далее в этой главе*;
- создавать любое количество томов на диске — столько, на сколько хватит свободного пространства;
- создавать тома, состоящие из двух или более дисков, при необходимости настроить толерантность отказа;

- расширить тома до полной емкости тома;
- назначить активный, системный и загрузочный тома, как было описано в *главе 1*.

Массивы томов

При работе с массивами томов можно создать тома, состоящие из нескольких дисков. Для этого объедините свободное пространство на разных дисках, чтобы пользователи увидели его как общий том. Файлы хранятся в массиве томов посегментно. Когда первый сегмент свободного пространства заполняется, используется второй сегмент и т. д.

Можно создать массив томов, основанный на свободном пространстве до 32 жестких дисков. Основное преимущество массивов томов заключается в том, что они позволяют использовать свободное пространство и создавать применяемую файловую систему. Основной недостаток — если какой-то жесткий диск в массиве выйдет из строя, массив томов больше нельзя будет использовать, т. е. все данные массива томов будут потеряны.

Полезно разбираться в состояниях тома, особенно при установке новых томов или диагностировании проблем. Оснастка **Управление дисками** показывает состояние диска в графическом представлении и списке томов. В табл. 2.1 приведены значения состояния динамических дисков.

Таблица 2.1. *Состояния диска и решение проблем*

Состояние	Описание	Решение
Неполные данные (Data Incomplete)	Составные тома на чужом диске неполные. Администратор забыл добавить другие диски из составного массива томов	Добавьте диски, содержащие оставшуюся часть составного тома, и затем импортируйте все диски за один раз
Нет избыточности данных (Data Not Redundant)	Была импортирована только часть зеркального тома. Администратор забыл добавить другие диски зеркала или массива RAID 5	Добавьте оставшиеся диски и затем импортируйте все диски сразу
Неисправен (Failed)	Состояние ошибки диска. Диск недоступен или поврежден	Убедитесь, что динамический диск находится в состоянии **В сети**. При необходимости щелкните правой кнопкой мыши на томе и выберите команду **Реактивировать диск**. Для базового диска нужно проверить диск на неправильное подключение
Отказавшая избыточность (Failed Redundancy)	Состояние ошибки. Один из дисков в зеркале или массиве RAID 5 находится в состоянии **Вне сети**	Убедитесь, что динамический диск находится в состоянии **В сети**. При необходимости реактивируйте том. Далее нужно заменить отказавшее зеркало или починить отказавший том RAID 5

Таблица 2.1 *(окончание)*

Состояние	Описание	Решение
Форматирование (Formatting)	Временное состояние, показывающее, что том в данный момент форматируется	Индикатор процесса форматирования показывает процент готовности, за исключением быстрого форматирования
Исправен (Healthy)	Нормальное состояние тома	Нет никаких проблем. Не нужно предпринимать никаких действий
Исправен (Под угрозой) (Healthy (At Risk))	Windows обнаружила проблемы чтения или записи на физическом диске, на котором расположен динамический том. Состояние появляется, когда Windows обнаружит ошибки	Щелкните правой кнопкой мыши на диске и выберите команду **Реактивировать диск**. Если это не поможет (состояние не изменится или состояние отказа диска возвращается), нужно выполнить резервное копирование всех данных диска
Исправен (Неизвестный раздел) (Healthy (Unknown Partition))	Windows не может распознать раздел. Ситуация возникает, если раздел принадлежит другой операционной системе или это раздел, созданный производителем для хранения системных файлов	Не требует корректирующих действий
Инициализация (Initializing)	Временное состояние, диск в данный момент инициализируется	Состояние диска должно измениться через несколько секунд
Регенерация (Regenerating)	Временное состояние, данные и четность для RAID 5 тома регенерируются	Индикатор хода процесса показывает процент выполнения этого процесса. Том должен вернуться в состояние **Исправен**
Ресинхронизация (Resynching)	Временное состояние, показывающее, что зеркало в данный момент ресинхронизируется	Индикатор хода процесса показывает процент выполнения этого процесса. Том должен вернуться в состояние **Исправен** (Healthy)
Устаревшие данные (Stale Data)	Сбой данных на чужих дисках	Пересканируйте диски или перезагрузите компьютер, а затем проверьте состояние. Будет отображено новое состояние, например, **Отказавшая избыточность**
Нет данных (Unknown)	Нет доступа к тому. Скорее всего, поврежден загрузочный сектор	Возможен вирус в загрузочном секторе. Проверьте диск антивирусной программой. Проверьте диск или перезагрузите компьютеры, а затем проверьте состояние

Создание томов и массивов томов

Простые тома можно отформатировать как exFAT, FAT, FAT32 или NTFS. Для упрощения управления составные тома должны быть отформатированы как NTFS. NTFS-

форматирование позволяет расширить тома в случае необходимости. Если понадобится больше пространства на томе, можно расширить простой или составной том. Это можно сделать, выбрав свободное пространство и добавив его в том. Можно расширить простой том в пределах этого же диска. Также можно расширить простой том на другие диски. После этого будет создан расширенный том, который должен быть отформатирован как NTFS.

Создать тома или массивы томов можно с помощью следующих действий:

1. В графическом представлении оснастки **Управление дисками** щелкните правой кнопкой мыши на нераспределенном пространстве и выполните команду **Создать составной том** (New Spanned Volume) или **Создать чередующийся том** (New Striped Volume). Прочтите страницу приветствия и нажмите кнопку **Далее**.
2. На странице **Выбор дисков** (Select Disks) (рис. 2.2) выберите диски, которые должны быть частью тома, а также укажите размер сегментов тома на этих дисках.

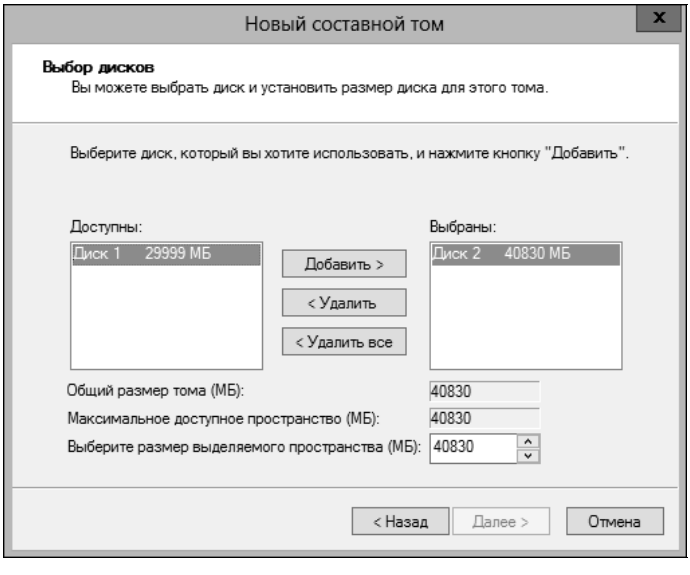


Рис. 2.2. На странице **Выбор дисков** выберите диски, которые должны быть частью тома

3. Доступные диски показаны в списке **Доступны** (Available). Если необходимо, выберите диск в этом списке и нажмите кнопку **Добавить** для добавления диска в список **Выбраны** (Selected). Если будет допущена ошибка, можно удалить диск из списка **Выбраны**: выберите диск и нажмите кнопку **Удалить** (Remove).

> ***Осторожно!***
> Мастера дисков в Windows Server 2012 R2 показывают и базовые, и динамические диски, где есть свободное пространство. Если добавите пространство из базового диска, мастер автоматически конвертирует диск в динамический перед созданием массива томов. Перед нажатием кнопки **Да** для продолжения убедитесь, что действительно это нужно, поскольку это может повлиять на то, как диск используется операционной системой.

4. Выберите диск в списке **Выбраны** (Selected), а затем укажите размер тома на диске в поле **Выберите размер выделяемого пространства (МБ)** (Select the amount of

space in MB). Поле **Максимальное доступное пространство (МБ)** (Maximum available space in MB) показывает наибольшую область свободного пространства, доступного на диске. Поле **Общий размер тома (МБ)** (Total volume size in megabytes) показывает общее дисковое пространство, которое будет использовано для тома. Нажмите кнопку **Далее**.

> ***Совет***
>
> Хотя можно установить размер тома любым способом, примите во внимание, как массивы томов будут использоваться в системе. Простые и составные тома не отказоустойчивы. Вместо создания одного огромного тома на всем доступном свободном пространстве можно создать несколько меньших томов, чтобы отказ одного тома не стал причиной потери всех данных.

5. Укажите, нужно ли назначить букву диска тому или том будет подключен как пустая NTFS-папка, а затем нажмите кнопку **Далее**. Доступны следующие варианты:
   - **Назначить букву диска** (Assign the following drive letter) — позволяет назначить букву диска, отметьте эту опцию и затем выберите доступную букву из предоставленного списка;
   - **Подключить том как пустую NTFS-папку** (Mount in the following empty NTFS folder) — используется для назначения пути диска, выберите эту опцию и затем введите путь к существующей папке на NTFS-диске, нажмите кнопку **Обзор** для поиска или создания папки;
   - **Не назначать буквы диска или пути диска** (Do not assign a drive letter or drive path) — выберите эту опцию для создания тома без назначения буквы диска или пути. Можно назначить букву диска или путь в любое время.
6. Укажите, должен ли том быть отформатированным. Если нужно отформатировать том, установите следующие опции форматирования.
   - **Файловая система** (File system) — укажите тип файловой системы. В оснастке **Управление дисками** доступна только файловая система NTFS.
   - **Размер кластера** (Allocation unit size) — устанавливает размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно установить размер кластера в конкретное значение. Если есть много маленьких файлов, можно задать наименьший размер кластера, например 512 или 1024 байта. Так маленькие файлы используют меньше дискового пространства.
   - **Метка тома** (Volume label) — определяет текстовую метку для раздела. Эта метка — имя тома раздела.
   - **Быстрое форматирование** (Perform a quick format) — указывает Windows Server 2012 R2, что нужно отформатировать раздел без проверки ошибок. На больших разделах эта опция может сэкономить несколько минут. Однако обычно лучше производить проверку на ошибки, в результате которой оснастка **Управление дисками** пометит плохие секторы диска и заблокирует их.

- **Применять сжатие файлов и папок** (Enable file and folder compression) — включает сжатие для диска. Сжатие прозрачно для пользователей, и доступ к сжатым файлам осуществляется подобно доступу к обычным файлам. Если выбрать эту опцию, файлы и каталоги на этом диске будут сжиматься автоматически. Подробная информация относительно сжатия дисков, файлов и каталогов была приведена в *главе 1* (только для NTFS).

7. Нажмите кнопку **Далее**, а затем кнопку **Готово**.

Удаление томов и массивов томов

Тома всех типов (простые, составные, зеркальные, чередующиеся или RAID 5 (чередующиеся с контролем четности)) удаляются одним и тем же способом. Удаление массива томов удаляет связанные файловые системы и все данные на них. Перед удалением массива томов необходимо сделать резервную копию файлов и каталогов, хранящихся на этих массивах томов.

Нельзя удалить том, содержащий системные, загрузочные файлы или файлы подкачки Windows Server 2012 R2.

Для удаления томов выполните действия:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши по тому в массиве и выберите команду **Удалить том** (Delete Volume). Нельзя удалить часть составного тома без удаления всего тома.
2. Нажмите кнопку **Да** для подтверждения удаления тома.

Управление томами

Управление томами происходит аналогично управлению разделами. Следуйте инструкциям, приведенным в *разд. "Управление существующими разделами и дисками" далее в этой главе*.

Повышение производительности и отказоустойчивости с помощью RAID

Часто нужно повысить защиту важных данных от отказов диска. Для этого используется технология RAID. С помощью RAID можно увеличить целостность данных и их доступность, создавая избыточные копии данных. Также можно использовать RAID, чтобы повысить производительность дисков.

Доступны различные реализации технологии RAID. Эти реализации описаны в терминах уровней. На данный момент определены уровни RAID от 0 до 5. Каждый уровень RAID отличается набором функций. Операционная система Windows Server 2012 R2 поддерживает уровни RAID 0, 1 и 5. Можно использовать уровень RAID 0 для повышения производительности дисков. Уровни RAID 1 и RAID 5 применяются для повышения отказоустойчивости данных.

В табл. 2.2 предоставлен краткий обзор поддерживаемых уровней RAID. Поддержка осуществляется полностью программно.

Таблица 2.2. *Уровни RAID, поддерживаемые Windows Server 2012 R2*

Уровень RAID	Тип RAID	Описание	Основные преимущества
0	Чередование дисков	Два или более тома, каждый из которых находится на отдельном диске, настраиваются как чередующийся набор. Данные разбиваются на блоки — страйпы, а затем записываются последовательно на все диски в наборе. Отказ одного диска приводит к неработоспособности массива	Скорость и производительность
1	Зеркалирование дисков	Два тома на двух дисках настраиваются идентично. Данные записываются на оба диска. Если один диск откажет, потерь данных не будет, поскольку другой диск содержит данные (этот уровень не поддерживает чередования)	Отказоустойчивость. Лучшая производительность записи по сравнению с чередованием с контролем четности
5	Чередование диска с контролем четности	Использует три или более тома, каждый на одном из дисков для создания чередования с контролем четности проверки ошибок. В случае сбоя данные могут быть восстановлены	Отказоустойчивость с меньшим количеством издержек, чем зеркалирование. Лучшая скорость чтения по сравнению с зеркалированием

Наиболее часто используемые на Windows-серверах уровни RAID — 1 (зеркалирование) и 5 (чередование с контролем четности). Зеркалирование диска — наименее дорогой способ повысить защиту данных с избыточностью. Здесь для создания избыточного набора данных используются два тома одинакового размера на двух разных дисках. Если один из дисков откажет, можно восстановить данные с другого диска.

С другой стороны, чередование дисков с контролем четности требует большего числа дисков — как минимум три, зато предлагает отказоустойчивость с наименьшим числом издержек, чем зеркалирование дисков. Если произошел сбой диска, можно восстановить данные, комбинируя блоки данных на оставшихся дисках с записью четности. Четность — метод проверки ошибок, которая использует операцию "исключающее ИЛИ" для создания контрольной суммы для каждого блока данных, записанного на диск. Эта контрольная сумма используется для восстановления данных в случае отказа.

Практический совет

Настоящие затраты для зеркалирования должны быть меньше, чем для чередования с четностью, но реальная стоимость гигабайта выше в случае с зеркалированием дисков. В случае с зеркалированием издержки составляют 50%. Например, если зеркалируются два диска по 750 Гбайт (общее пространство составляет 1500 Гбайт), то для хранения данных можно использовать только 750 Гбайт. Для чередования с контролем четности издержки составят примерно 33%. Например, если создается набор RAID 5, использующий три диска по 500 Гбайт (общее пространство — 1500 Гбайт), для хранения данных будет доступно 1000 Гбайт (издержки — одна треть).

Реализация RAID на Windows Server 2012 R2

Операционная система Windows Server 2012 R2 поддерживает зеркалирование диска, чередование дисков и чередование с контролем четности. Реализация этих техник RAID описана в следующем разделе.

> ***Осторожно!***
>
> Некоторые операционные системы, например MS-DOS, не поддерживают RAID. Если нужна двойная загрузка одной из таких операционных систем, RAID-диски будут недоступны.

Реализация RAID 0: чередование дисков

Уровень RAID 0 — это чередование дисков. При чередовании дисков два или более томов каждый на отдельном диске настраиваются как чередующийся набор. Данные, записываемые в чередующийся набор, называются *страйпами*. Эти страйпы записываются последовательно на все диски в наборе. Тома чередующегося набора могут быть размещены на 32 дисках, но более целесообразно использовать наборы из 2–5 томов для лучшей производительности. При большем числе дисков значительно снижается производительность.

Основное преимущество чередования дисков — это скорость. Поскольку данные находятся на нескольких дисках и для доступа к ним используется несколько головок, в результате повышается производительность. Однако этот прирост производительности стоит денег. При работе с наборами томов, если один из дисков откажет, чередующийся набор больше нельзя будет использовать, т. е. все данные в этом наборе будут потеряны. Нужно воссоздать чередующийся набор и восстановить данные из резервной копии. Резервное копирование и восстановление данных обсуждается в *главе 11*.

> ***Осторожно!***
>
> Загрузочный и системный тома не могут быть частью чередующегося набора. Не используйте чередование дисков с этими томами.

При создании чередующихся наборов нужно использовать тома приблизительно одинакового размера. Оснастка **Управление дисками** вычисляет полный размер чередующегося набора по наименьшему размеру тома. Максимальный размер набора — количество дисков, умноженное на размер наименьшего тома. Например, если наименьший размер тома равен 20 Гбайт и нужен набор из трех дисков, максимальный размер набора — 60 Гбайт, даже если два других диска будут размером по 2 Тбайт каждый.

Максимизировать производительность чередующегося набора можно несколькими способами:

- используйте диски, размещенные на разных дисковых контроллерах. Это позволяет системе одновременно получать доступ к дискам;
- не используйте диски, входящие в состав чередующего набора, в других целях. Это позволяет диску выделить все свое время чередующемуся набору.

Создать чередующийся набор можно с помощью следующих действий:

1. В графическом представлении оснастки **Управление дисками** щелкните правой кнопкой мыши по нераспределенной области динамического диска и выберите команду **Создать чередующийся том** (New Striped Volume). Будет запущен мастер создания чередующихся томов (New Striped Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку **Далее**.
2. Создание томов было описано в *разд. "Создание томов и массивов томов" ранее в этой главе*. Основное отличие — нужны как минимум два динамических диска, чтобы создать чередующийся том.

После создания чередующегося тома его можно использовать, как том любого другого типа. Нельзя расширить чередующийся том, как только он будет создан. Поэтому отнеситесь со всей ответственностью к созданию томов.

Реализация RAID 1: зеркалирование диска

RAID 1 — это зеркалирование диска. При зеркалировании используются тома одинакового размера на двух разных дисках для создания избыточного набора данных. На диски записываются идентичные наборы информации, и если один из дисков откажет, информацию все еще можно будет получить со второго диска.

Зеркалирование дисков тоже предлагает отказоустойчивость, как и чередование дисков с четностью. Поскольку диски зеркала не должны записывать контроль четности, они обеспечивают лучшую производительность записи в большинстве случаев. Однако чередование с контролем четности обычно выигрывает в скорости чтения, поскольку операции чтения распределяются по нескольким дискам.

Основной недостаток зеркалирования — неэффективное использование дискового пространства. Например, для зеркалирования диска на 500 Гбайт нужен еще один такой диск на 500 Гбайт. Это означает, что фактически дисковое пространство в 1000 Гбайт будет использоваться для хранения 500 Гбайт информации.

> ***Совет***
>
> Если возможно, нужно зеркально отразить системный и загрузочные тома. Это позволит загрузить сервер в случае выхода одного диска из строя.

Как и с чередованием дисков, зеркально отраженные диски должны быть на отдельных дисковых контроллерах. Это обеспечивает дополнительную защиту в случае отказа одного из дисковых контроллеров. Если один из контроллеров откажет, диск на втором контроллере будет все еще доступен. Технически при использовании двух отдельных контроллеров диска для дедупликации данных на самом деле применяется метод, называемый *дублированием дисков*. На рис. 2.3 показана разница между этими двумя методами. Зеркалирование обычно использует единственный контроллер, дублирование — два контроллера. В противном случае оба метода — по существу, одно и то же.

Если один из дисков набора откажет, операции с диском могут быть продолжены. Здесь при чтении/записи данные будут записаны на работоспособный диск. Перед исправлением зеркала его нужно разбить. Чтобы узнать, как это сделать, *см. разд. "Управление RAID-массивами и восстановление после сбоя" далее в этой главе*.

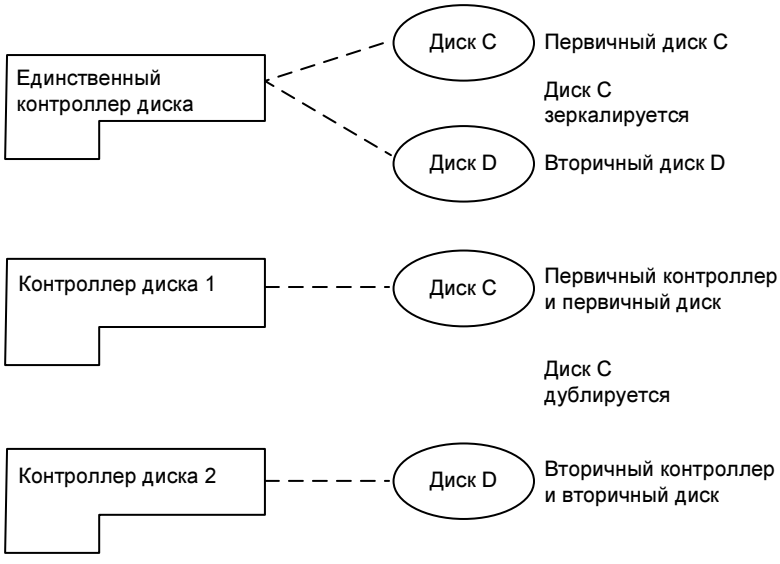


Рис. 2.3. Хотя зеркалирование диска обычно использует единственный контроллер для создания отказоустойчивого набора данных, дедупликация применяет два разных контроллера

Создание зеркального набора в оснастке *Управление дисками*

Создать зеркальный набор можно с помощью следующих действий:

1. В графическом представлении оснастки **Управление дисками** щелкните на нераспределенной области динамического диска и выберите команду **Создать зеркальный том** (New Mirrored Volume). Будет запущен мастер создания образа (New Mirrored Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку **Далее**.
2. Создайте том, как было описано в *разд. "Создание томов и массивов томов" ранее в этой главе*. Основное отличие — нужно создать два тома одинакового размера, и эти тома должны быть расположены на разных динамических дисках. На странице **Выбор диска** (Select Disks) нельзя продолжить, пока не выберете два диска, с которыми будете работать.

Подобно другим техникам RAID, зеркалирование прозрачно для пользователей. Пользователи будут видеть зеркальный набор как единственный диск, доступ к которому может быть получен как к любому другому диску.

> ***Примечание***
>
> Нормальное состояние зеркала — **Исправен**. Во время создания зеркала можно увидеть состояние **Ресинхронизация**, говорящее о том, что оснастка **Управление дисками** создает зеркало.

Зеркалирование существующего тома

Вместо создания нового зеркального тома можно использовать существующий том для создания зеркального набора. Для этого том, который нужно зеркалировать, должен

быть простым томом и на втором диске нужно иметь нераспределенную область равного или большего размера (чем существующий том).

1. Щелкните правой кнопкой мыши по простому тому, который нужно зеркально отразить, а затем выберите команду **Добавить зеркало** (Add Mirror). Появится окно **Добавить зеркальный том** (Add Mirror).
2. В списке **Диски** (Disks) (рис. 2.4) выберите расположение для зеркала, а затем нажмите кнопку **Добавить зеркальный том** (Add Mirror). ОС Windows Server 2012 R2 начнет процесс создания зеркала, а в оснастке **Управление дисками** будет установлено состояние **Ресинхронизация** на обоих томах. У диска, на котором создается зеркальный том, будет значок предупреждения.

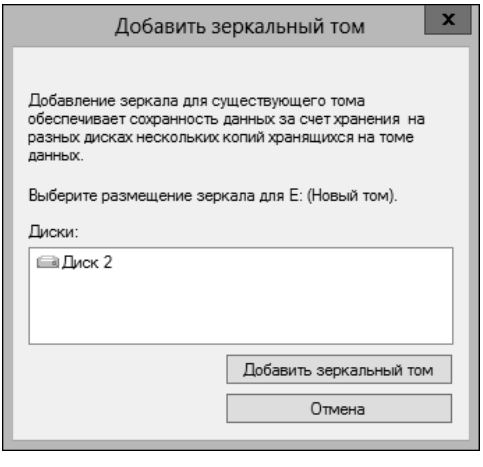


Рис. 2.4. Выберите расположение зеркала

Реализация RAID 5: чередование дисков с контролем четности

Уровень RAID 5 — это чередование дисков с контролем четности. Эта техника требует как минимум трех жестких дисков для настройки отказоустойчивости. Размеры томов на всех трех дисках должны быть одинаковыми.

RAID 5 распределяет данные и данные четности последовательно по всем дискам массива. Отказоустойчивость гарантирует, что отказ одного диска не приведет к отказу всего набора. Вместо отказа набор продолжает функционировать с оставшимися томами в наборе.

Для обеспечения отказоустойчивости RAID 5 записывает контрольные суммы четности с блоками данных. Если любой из дисков набора откажет, можно использовать информацию четности для восстановления данных (этот процесс называется регенерацией чередующегося набора и будет описан в *разд. "Управление RAID-массивами и восстановление после сбоя" далее в этой главе*). Если откажут два диска, информации четности будет недостаточно для восстановления данных и нужно будет восстановить набор из резервной копии.

Создание чередующегося набора с четностью в оснастке *Управление дисками*

В оснастке **Управление дисками** можно создать чередующийся набор с четностью с помощью следующих действий:

1. В графическом представлении оснастки **Управление дисками** щелкните правой кнопкой мыши на нераспределенном пространстве динамического диска и выберите команду **Создать том RAID 5** (New RAID 5 Volume). Будет запущен мастер создания томов RAID 5 (New RAID 5 Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку **Далее**.
2. Создайте том, как было описано в *разд. "Создание томов и массивов томов" ранее в этой главе*. Основное отличие — нужно выбрать три нераспределенных области на трех разных динамических дисках.

После создания чередующегося набора с контролем четности (RAID 5) пользователи могут использовать том, как обычный диск. Помните, что нельзя расширить чередующийся раздел после его создания. Поэтому отнеситесь к созданию набора со всей ответственностью.

Управление RAID-массивами и восстановление после сбоя

Управление зеркальными дисками и чередующимися массивами иногда отличается от управления другими томами, особенно когда речь идет о восстановлении после сбоя. Техники, используемые для управления RAID-массивами и восстановления после сбоя, описаны в этом разделе.

Разделение зеркального набора

Разделить зеркальный набор необходимо по одной из двух причин.

- Если один из зеркальных дисков откажет, дисковые операции могут быть продолжены. Когда пользователи будут читать и записывать данные, эти операции будут произведены с оставшимся диском. Однако нужно исправить зеркало, для этого необходимо сначала разбить зеркало, заменить отказавший диск и затем переустановить зеркало.
- Если больше не нужно зеркально отражать диск, тогда тоже необходимо разбить зеркало. Это позволит использовать дисковое пространство для других целей.

> ***РЕКОМЕНДАЦИИ***
> "Разбить зеркало" не означает удаление всех данных в наборе, однако перед этим лучше всего выполнить резервное копирование данных. Это гарантирует, что в случае сбоя можно восстановить данные.

В оснастке **Управление дисками** можно разбить зеркальный набор с помощью следующих действий:

1. Щелкните по одному из томов зеркального набора и выберите команду **Разделить зеркальный том** (Break Mirrored Volume).

2. Подтвердите действие, нажав кнопку **Да**. Если том используется, будет отображено другое предупреждение. Опять подтвердите свое намерение, нажав кнопку **Да**. Операционная система Windows Server 2012 R2 разобьет зеркало, создав два независимых тома.

Ресинхронизация и восстановление зеркального набора

Операционная система Windows Server 2012 R2 автоматически синхронизирует зеркальные тома на динамических дисках. Однако данные на зеркальных дисках могут оказаться рассинхронизированными. Например, если один из дисков перешел в состояние **Вне сети**, а данные были записаны только на диск, находящийся в состоянии **В сети**.

Можно ресинхронизировать и восстановить зеркальные наборы, но перед этим нужно сначала восстановить набор, используя диски с тем же стилем разделов — либо с главной загрузочной записью (MBR), либо с таблицей GUID (GPT). Необходимо получить оба диска в зеркальном наборе в состоянии **В сети**. Состояние зеркального набора должно быть **Отказавшая избыточность**. Меры по ликвидации последствий, которые можно предпринять, зависят от состояния отказавшего тома.

- Если активно состояние **Отсутствует** или **Вне сети**, убедитесь, что к диску подключено питание и он правильно подключен. Затем запустите оснастку **Управление дисками**, щелкните правой кнопкой мыши по отказавшему тому и выберите команду **Реактивировать том** (Reactivate Volume). Состояние диска должно измениться на **Регенерация**, а затем на **Исправен**. Если том не возвращается в состояние **Исправен**, щелкните по этому тому и выберите действие **Ресинхронизация зеркала** (Resynchronize Mirror).
- Если активно состояние **В сети (Ошибки)**, щелкните правой кнопкой мыши по отказавшему тому и выберите команду **Реактивировать том**. Состояние диска должно измениться на **Регенерация**, а затем на **Исправен**. Если том не возвращается в состояние **Исправен**, щелкните правой кнопкой на томе и выберите команду **Ресинхронизация зеркала**.
- Если один из дисков находится в состоянии **Не читается**, нужно пересканировать диски системы, выбрав команду **Действие | Повторить проверку дисков** (Action | Rescan Disks). Если состояние диска изменится, нужно перезагрузить компьютер.
- Если один из дисков не возвращается в состояние **В сети**, щелкните правой кнопкой мыши на отказавшем томе и выберите команду **Удалить зеркало** (Remove Mirror). Теперь нужно создать зеркало тома на нераспределенной области свободного пространства. Если нет свободного места, его нужно создать, удалив другие тома или заменив отказавший диск.

Восстановление зеркального системного тома для включения загрузки

Отказ зеркально отраженного диска может препятствовать загрузке системы. Как правило, это происходит, когда зеркалируется системный или загрузочный том (или оба) и

основной зеркальный диск отказал. В предыдущих версиях Windows нужно выполнить несколько процедур, чтобы заставить систему снова работать. В Windows Server 2012 R2 отказ зеркала разрешить намного проще.

При зеркалировании системного тома операционная система должна добавить запись в диспетчер начальной загрузки системы, которая позволяет загружаться со вторичного зеркала. Восстановление первичного зеркала с этой записью в файле диспетчера загрузки намного проще, потому что все, что нужно сделать для загрузки со вторичного зеркала — это выбрать данную запись при загрузке. Если зеркалируется загрузочный том и эта запись не была создана, можно отредактировать записи диспетчера загрузки и создать ее с помощью редактора BCD (Bcdedit.exe).

Если не получается загрузиться с основного системного тома, перезагрузите систему и в меню загрузчика выберите пункт **Windows Server 2012 R2 — Secondary Plex** для операционной системы, которую нужно загрузить. Система должна запуститься без проблем. После успешной загрузки со вторичного диска можно приступить к восстановлению зеркала. Нужно выполнить следующие действия:

1. Завершите работу системы и замените отказавший том или добавьте жесткий диск. Затем перезагрузите систему.
2. Разделите зеркало и заново создайте зеркало на диске, который был заменен (обычно это диск 0). Щелкните правой кнопкой мыши на оставшемся от исходного зеркала томе и выберите команду **Добавить зеркало**. Далее следуйте указаниям из *разд. "Зеркалирование существующего тома" ранее в этой главе*.
3. Если нужно, чтобы основное зеркало было на диске, который был добавлен или заменен, используйте оснастку **Управление дисками**, чтобы снова разделить зеркало. Убедитесь, что основному диску в исходном зеркале назначена буква диска, которая была ранее присвоена полному зеркалу. Если это не так, назначьте надлежащую букву диска.
4. Щелкните правой кнопкой мыши по исходному системному тому и выберите команду **Добавить зеркало**. Заново создайте зеркало.
5. Проверьте загрузочные записи в диспетчере загрузки и с помощью редактора BCD убедитесь, что для запуска системы используется исходный системный том.

Удаление зеркального набора

Используя оснастку **Управление дисками**, можно удалить один из томов из зеркального набора. После этого все данные на удаляемом зеркале будут удалены, а используемое пространство будет помечено как нераспределенное.

Чтобы удалить зеркальный набор, выполните следующие действия:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши по одному из томов зеркального набора и выберите команду **Удалить зеркало** (Remove Mirror). Откроется одноименное окно.
2. В окне **Удалить зеркало** выберите диск, с которого нужно удалить зеркало.
3. Подтвердите действие, когда появится соответствующий запрос. Все данные на удаляемом зеркале будут уничтожены.

Восстановление чередующегося массива с контролем четности

Чередующийся массив без контроля четности не отказоустойчивый. Если один из дисков набора откажет, весь массив станет неиспользуемым. Перед попыткой восстановить чередующийся массив нужно восстановить или заменить отказавший диск. Затем необходимо заново создать чередующийся набор и восстановить данные из резервной копии.

Регенерация чередующегося массива с четностью

При использовании RAID 5 можно восстановить чередующийся массив с контролем четности, если один из дисков выйдет из строя. Какой именно из дисков вышел из строя, можно понять по его состоянию: состояние массива будет изменено на **Отказавшая избыточность**, а состояние отдельного тома должно быть изменено на **Отсутствует**, **Вне сети** или **В сети (Ошибки)**.

Можно восстановить диски RAID 5, но нужно перестроить массив с использованием того же стиля разделов — либо MBR, либо GPT. Необходимо, чтобы все диски в наборе RAID 5 были в состоянии **В сети**. Состояние массива должно быть **Отказавшая избыточность**. Предпринимаемые вами меры зависят от состояния отказавшего диска.

- Если активно состояние **Отсутствует** или **Вне сети**, убедитесь, что к диску подключено питание и он правильно подключен. Затем запустите оснастку **Управление дисками**, щелкните правой кнопкой мыши по отказавшему тому и выберите команду **Реактивировать том**. Состояние диска должно измениться на **Регенерация**, а затем на **Исправен**. Если состояние диска не вернулось на **Исправен**, щелкните правой кнопкой мыши по тому и выберите команду **Регенерация четности** (Regenerate Parity).
- Если активно состояние **В сети (Ошибки)**, щелкните правой кнопкой мыши по отказавшему тому и выберите команду **Реактивировать том**. Состояние диска должно быть изменено на **Регенерация**, а затем на **Исправен**. Если состояние диска не вернулось на **Исправен**, щелкните правой кнопкой по тому и выберите команду **Регенерация четности**.
- Если состояние одного из дисков — **Не читается**, нужно пересканировать диски, используя команду **Действие | Повторить проверку дисков** (Action | Rescan Disks). Если состояние диска не изменится, перезагрузите компьютер.
- Если после этого один из дисков все еще **Вне сети**, нужно восстановить отказавшую область массива RAID 5. Щелкните правой кнопкой мыши на отказавшем томе и выберите команду **Удалить том** (Remove Volume). Теперь нужно выбрать нераспределенное пространство на другом динамическом диске для использования в массиве RAID 5. Это пространство должно быть больше, чем область, которую нужно восстановить, и не может быть на диске, который уже используется в массиве RAID 5. Если недостаточно места, команда **Восстановить том** (Repair Volume) будет недоступна и необходимо получить свободное пространство путем удаления других томов или замены отказавшего диска.

Рекомендации

Если возможно, сделайте резервную копию перед выполнением этой процедуры. Это гарантия, что в случае проблем можно будет восстановить данные.

Стандартизированное управление хранилищами

Стандартизированное управление хранилищами фокусируется на самих томах хранилища, а не на физической разметке, полагаясь на аппаратные средства для обработки особенностей архитектуры для избыточности данных и частей диска, которые представлены как используемые диски. Это означает, что расположением физических дисков управляет подсистема внешней памяти, а не операционная система.

Знакомство со стандартизированным управлением хранилищами

При работе со стандартизированным хранилищем физическое расположение дисков абстрагировано. Здесь "диск" может быть логическим указателем на часть подсистемы внешней памяти (виртуальный диск) или физический диск. Это означает, что диск просто становится модулем хранилища, а тома создаются для выделения места на дисках для файловых систем.

Можно поместить в пул все свободное место на дисках так, чтобы модули хранилища (виртуальные диски) могли быть выделены из этого пула по мере необходимости. В свою очередь, эти модули хранилища распределяются на тома для выделения пространства и создания файловых систем, доступных для использования.

Технически, такое хранилище называется *пулом носителей*, а виртуальные диски в пределах пула — *пространствами хранилища*. Этот массив "дисков" можно использовать для создания единственного пула хранения данных, помещая все диски в пул, или же создать несколько пулов, распределив имеющиеся диски между пулами.

Практический совет

Когда мы говорим о подсистеме внешней памяти, на самом деле мы имеем дело с трехуровневой архитектурой. На уровне 1 расположением физических дисков управляет подсистема внешней памяти. Система хранения, вероятно, будет использовать некоторую форму RAID для обеспечения избыточности и отказоустойчивости. На уровне 2 созданные массивами виртуальные диски доступны для серверов. Серверы рассматривают диски как хранилище, которое может быть выделено. ОС Windows Server может применить какой-то из уровней программного RAID или другие способы избыточности для отказоустойчивости. На уровне 3 сервер создает тома на виртуальных дисках, а на них уже создаются файловые системы для хранения файлов и данных.

Работа со стандартизированным хранилищем

При работе с ролью **Файловые службы и службы хранилища** (File Services And Storage) можно сгруппировать доступные диски в пулы хранения так, что можно создать виртуальные диски из доступной емкости. Каждый созданный виртуальный диск — это дисковое пространство (storage space). Дисковые пространства становятся

доступными посредством роли **Службы хранилища**, которая автоматически устанавливается на каждом сервере под управлением Windows Server 2012 R2.

Для интеграции Дисковых пространств (Storage Spaces) со стандартизированным хранилищем вам нужно добавить компонент **Стандартизированное управление хранилищами Windows** (Windows Standards-Based Storage Management) на серверы. Если сервер настроен на работу с ролью **Файловые службы и службы хранилища**, компонент **Стандартизированное управление хранилищами Windows** добавляет компоненты и обновляет диспетчер серверов опциями для работы со стандартизированными томами. Возможно, придется также:

- добавить службу роли **Дедупликация данных** (Data Deduplication), если необходимо включить дедупликацию данных;
- добавить службы ролей **Сервер цели iSCSI** (iSCSI Target Server) и **Поставщик целевого хранилища iSCSI** (iSCSI Target Storage Provider), если нужно размещать виртуальные диски iSCSI.

После настройки сервера надлежащим для производственной среды способом можно выбрать узел **Файловые службы и службы хранилища** (File And Storage Services) в диспетчере серверов для работы с томами хранилища — там находятся дополнительные функции. Подузел **Серверы** (Servers) содержит файловые серверы, которые были настроены для стандартизированного управления хранилищами.

На рис. 2.5 показан подузел **Тома** (Volumes), предоставляющий информацию о выделенном хранилище на каждом сервере. Здесь выводится, как настроены тома и сколько свободного пространства есть на томе. Тома выводятся независимо от того, основаны ли они на физических или виртуальных дисках. Щелкните правой кнопкой мыши на томе для отображения опций управления.

- **Настройка дедупликации данных** (Configure Data Deduplication) — позволяет включить и настроить дедупликацию данных на NTFS-томах. Если эта опция доступна, можно также впоследствии использовать ее для отключения дедупликации.
- **Удалить том** (Delete Volume) — служит для удаления тома. Используемое пространство будет помечено как нераспределенное на соответствующем диске.
- **Расширить том** (Extend Volume) — позволяет расширить том на все нераспределенное пространство на соответствующем диске.
- **Форматировать** (Format) — позволяет создать новую файловую систему на томе, которая перезапишет существующий том.
- **Управление буквой диска или путями доступа** (Manage Drive Letter) — позволяет изменить букву диска или пути доступа, связанные с томом.
- **Создать виртуальный диск iSCSI** (New iSCSI Virtual Disk) — позволяет создать новый виртуальный диск iSCSI, который будет сохранен на томе.
- **Новый общий ресурс** (New Share) — позволяет создать общий ресурс SMB (Server Message Block) или NFS (Network File System) на томе.
- **Свойства** — отображает информацию о типе тома, файловой системе, исправности, емкости, используемом пространстве и свободном пространстве. Можно также использовать окно **Свойства** для установки метки тома.

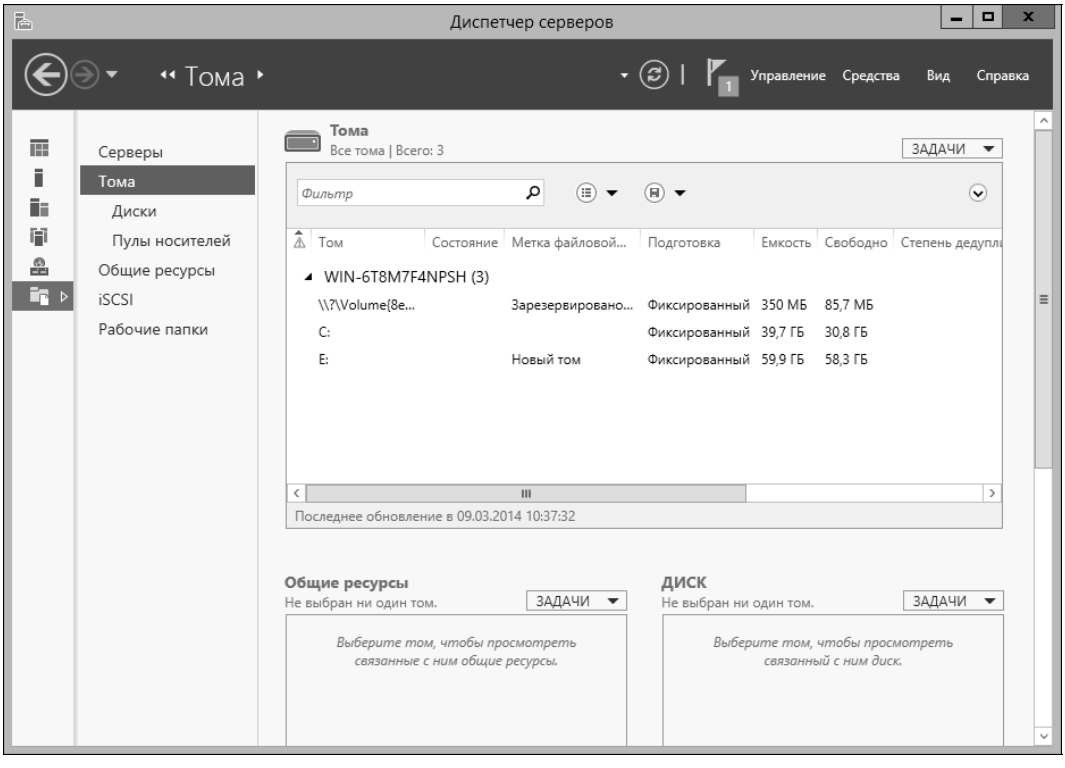


Рис. 2.5. Обратите внимание, как настроены тома

- **Исправить ошибки файловой системы** (Repair File System) — позволяет исправить ошибки, обнаруженные во время оперативного (онлайн) сканирования файловой системы.
- **Проверить файловую систему на наличие ошибок** (Scan File System For Errors) — осуществляет оперативное сканирование файловой системы. Хотя Windows пытается восстановить любые найденные ошибки, некоторые ошибки могут быть исправлены только с помощью этой процедуры.

Как показано на рис. 2.6, подузел **Диски** выводит диски, доступные на каждом сервере, при этом сообщается общая емкость, нераспределенное пространство, стиль раздела, подсистема и тип шины. Диспетчер серверов пытается различать физические и виртуальные диски, показывая метку виртуального диска и исходную подсистему хранения. Щелкните правой кнопкой мыши на диске, чтобы увидеть опции управления:

- **Подключить** (Bring Online) — перевести диск в состояние **В сети**, что сделает его доступным для использования;
- **Отключить** (Take Offline) — перевести диск в состояние **Вне сети**, что сделает его недоступным;
- **Сбросить диск** (Reset Disk) — полностью сбросить диск, что удалит все тома на диске и все доступные данные на нем;
- **Создать том** (New Volume) — создать новый том на диске.

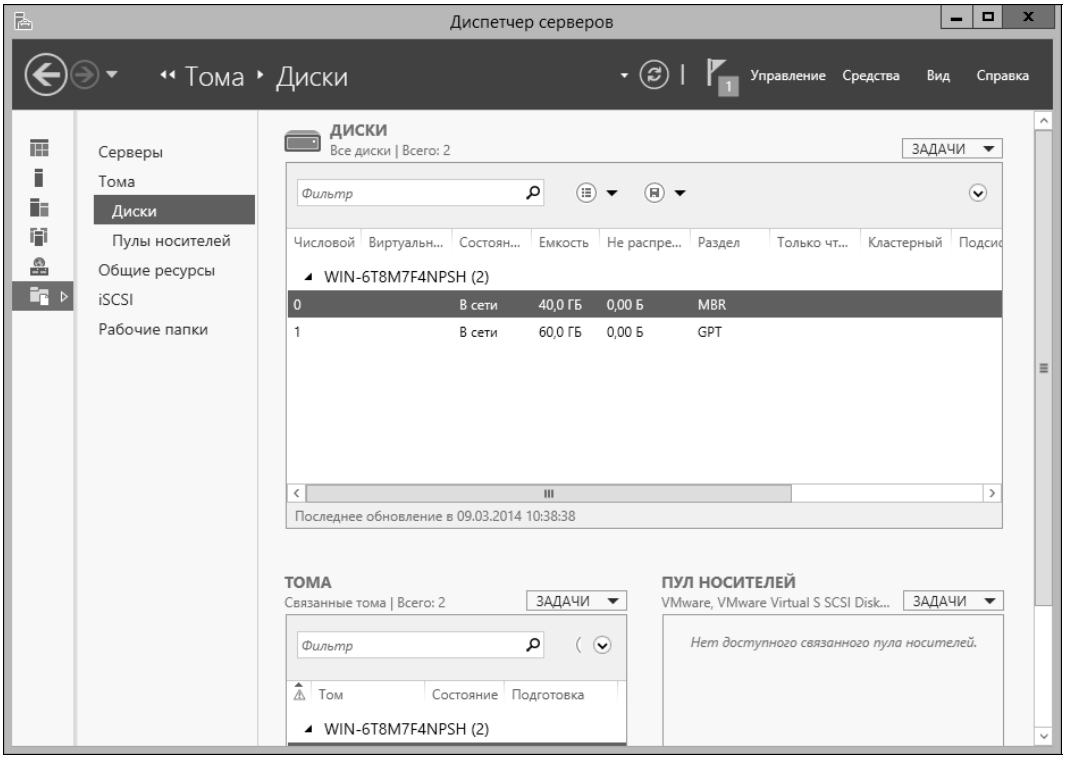


Рис. 2.6. Выводит все доступные диски и сообщает, сколько нераспределенного пространства доступно

Версия Дисковых пространств (Storage Spaces), которая поставляется с Windows Server 2012 R2, отличается от версии, которая поставлялась с Windows Server 2012. Если есть сомнения относительно используемой версии, выполните следующие действия:

1. Щелкните правой кнопкой мыши на пуле носителей, который нужно исследовать, и выберите команду **Свойства** (Properties).
2. В диалоговом окне **Свойства** выберите раздел **Подробности** (Details) на панели слева, а затем выберите свойство **Version** из списка **Свойство** (Property).

Данная техника также может использоваться для проверки емкости, статуса, размера логического сектора, размера физического сервера, используемого пространства и получения другой информации о пуле носителей. По умолчанию Дисковые пространства уведомляют администратора, что дисковое пространство скоро закончится и когда используемое пространство достигает отметки 70% от общего выделенного размера. В случае получения такого уведомления нужно рассмотреть выделение дополнительного пространства.

При желании можно обновить версию Дисковых пространств, используемую пулом носителей, щелкнув на пуле носителей правой кнопкой мыши и выбрав команду **Обновить версию пула носителей** (Upgrade Storage Pool Version). Новая версия дисковых пространств (используемая в Windows Server 2012 R2), помимо исправления

проблем, которые могут привести к состояниям ошибки и предупреждения при создании и управления дисковыми пространствами, делает следующее.

- Поддерживает дисковые пространства с двойной четностью (как просто с четностью, так и двойной четностью) на отказоустойчивых кластерах. Пространства с двойной четностью защищены от одновременного отказа двух дисков.
- Поддерживает автоматическое перестроение дисковых пространств из свободного пространства пула носителей вместо использования горячего резерва для восстановления после отказа диска. Здесь, вместо записи копии данных, которые находились на отказавшем диске, на горячий резерв, зеркально отраженные данные копируются на несколько дисков в пуле для достижения предыдущего уровня отказоустойчивости автоматически. В результате администратору не нужно выделять горячие резервы в пулах носителей при условии, конечно, что пулу присвоено достаточное для автоматического восстановления отказоустойчивости число дисков.
- Поддерживает уровни хранения для автоматического перемещения часто используемых файлов с более медленных физических дисков на более быстрые SSD-диски (Solid State Drive). Эта функция применима только для систем, обладающих как обычными жесткими дисками (HDD), так и SSD-дисками. Также тип хранения должен быть фиксированным, а тома, создаваемые на виртуальных дисках, должны быть того же размера, что и виртуальный диск. Конечно же, на SSD-диске должно быть достаточно свободного пространства, чтобы разместить часто используемые файлы. Для гибкого управления используйте командлет Set-FileStorageTier, позволяющий присвоить файлы или обычному жесткому диску, или более быстрому SSD-диску.
- Поддерживает отложенное (write-back) кэширование, когда пул носителей использует SSD. Отложенное кэширование буферизует случайные операции записи на SSD-носителей перед их дальнейшей записью на обычный жесткий диск (HDD). Буферизация записей таким способом повышает производительность и помогает защитить данные от их потери в случае потери питания. Для корректной работы отложенного кэширования в дисковых пространствах с простыми томами должен быть, по крайней мере, один SSD-диск, в дисковых пространствах с зеркалированием или четностью должно быть, по крайней мере, два SSD-диска, а у дисковых пространств с трехсторонним зеркалированием или двойной четностью должно быть как минимум три SSD-диска. Если эти требования удовлетворены, тома будут автоматически использовать отложенное кэширование на 1 Гбайт по умолчанию. Вы можете назначить SSD-диски, которые будут использоваться для отложенного кэширования, задав их применение в качестве журнала (значение по умолчанию в этой конфигурации). Если в системе недостаточно SSD-дисков, размер отложенного кэша будет установлен 0 (это означает, что отложенное кэширование не используется). Единственное исключение составляют пространства с четностью, для которых назначается размер отложенного кэша 32 Мбайт.

Если вы хотите узнать, какой у вас размер отложенного кэша, выполните следующие действия:

1. Щелкните правой кнопкой мыши по виртуальному диску, который вы хотите исследовать, и выберите команду **Свойства**.

2. В диалоговом окне **Свойства** выберите раздел **Подробности** на панели слева, а затем выберите свойство **WriteCacheSize** из списка **Свойство**.

Также эта техника используется и для получения другой информации, например состояния диска, выделенного размера, типа избыточности и т. д.

Использование пулов носителей и распределение пространства

В диспетчере серверов можно работать с пулами носителей и распределить пространство на них. Для этого перейдите в узел **Файловые службы и службы хранилища | Пулы носителей** (File And Storage Services | Storage Pools). Как показано на рис. 2.7, в подразделе **Пулы носителей** (Storage Pools) выводятся доступные пулы, виртуальные диски, созданные внутри пулов, и доступные физические диски. Помните: диски, представленные как физически, могут оказаться на самом деле виртуальными дисками LUN от подсистемы хранения.

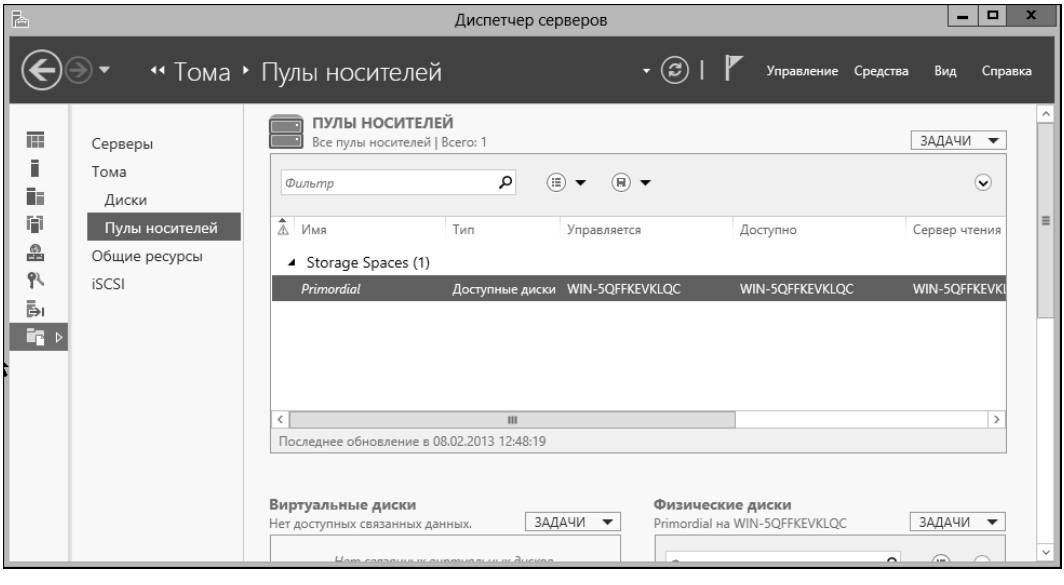


Рис. 2.7. Создание и управление пулами

Работа с пулами носителей — многоэтапный процесс:

1. Администратор создает пулы носителей, чтобы объединить доступное пространство на одном или более дисках.
2. Администратор создает пространство из этого пула для создания одного или более виртуальных дисков.
3. Администратор создает один или более томов на каждом виртуальном диске для распределения хранилища для файловых систем.

Следующие разделы подробно описывают каждый этап.

Создание пула носителей

Пулы носителей позволяют объединять свободное место на дисках так, чтобы модули хранения (виртуальные диски) могли быть распределены из этого пула. Чтобы создать пул носителей, в системе должен быть по крайней мере один неиспользуемый диск, а также подсистема хранилища для его управления. Эта подсистема может включать функцию Дисковое пространство (Storage Spaces) или подсистему, связанную с присоединенным хранилищем.

Когда у компьютера есть дополнительные жесткие диски, кроме диска, на котором установлена Windows, администратор может выделить один или больше из этих дополнительных дисков для использования в виде пула носителей. Однако помните, что если для использования в качестве пула носителей выделяется уже отформатированный диск, Windows удалит все файлы на этом диске. Также важно понимать, что все жесткие диски со стилем разметки MBR, добавляемые в пул, автоматически будут преобразованы в стиль GPT.

Каждый физический диск, выделенный пулу, может использоваться одним из трех способов:

- как хранилище данных, доступное для использования;
- как хранилище данных, которое может быть вручную выделено для использования;
- как горячая замена в случае, если диск в пуле откажет или будет удален из подсистемы.

Можно создать следующие типы томов.

- **Простой** (Simple). Создает простой том, записывая одну копию данных на один или более дисков. Не обеспечивает избыточности, поскольку есть только одна копия данных. В качестве примера, администратор может создать простой том, объединяющий два диска по 2 Тбайт каждый в один диск общим размером 4 Тбайт. Однако, поскольку не обеспечивается избыточность, выход из строя одного диска приведет к краху всего тома.
- **Двухстороннее зеркало** (Two-way mirror). Создает зеркальный набор, записывая две копии данных компьютера, благодаря чему обеспечивается защита от выхода из строя одного диска. Двухстороннее зеркало требует как минимум двух дисков. Половина (50%) доступного пространства используется для обеспечения избыточности. Так, если есть два диска по 2 Тбайт, общий размер зеркалируемого пространства достигнет всего 2 Тбайт.
- **Четность** (Parity). При выборе этого типа тома данные и информация четности чередуются по физическим дискам с использованием метода чередования с контролем четности. Необходимы как минимум три диска. Треть дискового пространства (33,33%) используется для обеспечения избыточности. Так, если есть три диска по 2 Тбайт каждый, для хранения данных будет доступно 4 Тбайт.
- **Тома двойной четности** (Dual parity volumes). Создает том, использующий чередования диска с двумя наборами данных четности, помогая защитить данные от одновременного отказа двух дисков. Такие тома требуют как минимум семь дисков.

- **Трехстороннее зеркало** (Three-way mirrors). Создает набор, записывая три копии данных компьютера и используя чередование диска с зеркалированием. Помогает защитить данные от одновременного отказа двух дисков. Хотя у трехстороннего зеркала нет потерь производительности при чтении, у них действительно есть некоторые потери производительности при записи, связанные с необходимостью записи на три отдельных диска. Эти потери могут быть уменьшены использованием нескольких дисковых контроллеров. В идеале нужны три отдельных дисковых контроллера. Что касается минимального количества дисков, то для трехстороннего зеркала нужно как минимум пять дисков.

Если читатель знаком с RAID 6, он знаком с томами двойной четности. Хотя у таких томов нет издержек при чтении, у них есть огромные потери производительности при записи данных, поскольку вычисление и запись двойных значений четности требует значительных вычислительных ресурсов. Используемое дисковое пространство тома с двойной четностью равно числу дисков минус 2 и умноженному на размер минимального тома в наборе. Например, у нас есть 7 дисков, размер минимального диска — 1 Тбайт, тогда доступное для использования дисковое пространство будет равно 5 Тбайт: $(7 - 2) \times 1$ Тбайт.

Если подумать логически, то, кажется, что нужно, по крайней мере, шесть дисков, чтобы записать три зеркальных копии данных, но необходимы только пять. Почему? Если нужно создать три копии данных, требуется как минимум 15 логических единиц хранения. Разделите 15 на 3, и станет ясно, сколько дисков нужно для хранения трех копий данных. Таким образом, дисковые пространства используют 1/3 каждого диска, чтобы хранить исходные данные, и 2/3 каждого диска, чтобы хранить копии данных. Значит, трехстороннее зеркало с пятью томами использует 2/3 (66,66%) всего пространства для обеспечения избыточности. Говоря другими словами, выделение пяти дисков по 3 Тбайт каждый для трехстороннего зеркала даст вам всего лишь 5 Тбайт для хранения данных (10 Тбайт — это издержки).

При использовании томов с одинарной четностью данные записываются горизонтально с четностью, вычисленной для каждого ряда данных. Двойная четность отличается от одинарной тем, что ряд данных сохраняется не только горизонтально, но и по диагонали. Если произойдет сбой одного диска, данные будут воссозданы с помощью только горизонтального ряда данных четности (как и в случае с одинарной четностью). Если произойдет сбой нескольких дисков, для восстановления будут использованы данные четности, записанные по горизонтали и по диагонали.

Чтобы понять, как работает двойная четность, рассмотрим следующий простой пример. У каждого горизонтального ряда данных есть значение четности, сумма которого сохранена на диске четности для того ряда (и вычислена с помощью операции исключающего ИЛИ — XOR). Каждое горизонтальное чередование четности пропускает один и только один диск. Если значение четности равняется 2, 3, 1 и 4 на дисках 0, 1, 2 и 3 соответственно, сумма четности, сохраненная на диске 4 (диск четности для этого ряда), равна 10 ($2 + 3+ 1 + 4 = 10$). Если произойдет сбой диска 0, значение четности для ряда на этом иске может быть восстановлено путем вычитания оставшихся горизонтальных значений из суммы горизонтальной четности ($10 – 3 – 1 – 4 = 2$).

Второй набор данных четности записывается по диагонали (значение в разных рядах данных на различных дисках). У каждого диагонального ряда данных есть диагональ-

ное значение четности, сумма которого сохранена на диагональном диске четности для того ряда (и вычислена с помощью операции XOR). Каждое диагональное чередование четности пропускает два диска: один диск, в котором сохранена диагональная сумма четности, и один диск, который опускается при диагональном чередовании четности. Кроме того, диагональная сумма четности включает ряд данных из горизонтального ряда четности как часть ее диагональной суммы четности.

Если диагональное значение четности равняется 1, 4, 3 и 7 на дисках 1, 2, 3 и 4 соответственно (с четырьмя связанными горизонтальными рядами), диагональная сумма четности, сохраненная на диске 5 (диагональный диск четности для этого ряда), равна 15 (4 + 1 + 3 + 7 = 15), опущенный диск — диск 0. Если отказали диски 2 и 4, для восстановления данных используется диагональное значение четности для ряда. Сначала из диагональной суммы четности вычитаются остающиеся диагональные значения. Затем восстанавливается недостающее горизонтальное значение, вычитая остающиеся горизонтальные значения для исследуемого ряда из горизонтальной суммы четности для того ряда.

> ***Примечание***
>
> Имейте в виду, что двойная четность, реализованная в дисковых пространствах, использует семь дисков, и предыдущий пример был упрощен. Хотя чередование четности с семью дисками работает несколько иначе, чем было показано в примере, основной подход заключается в использовании горизонтальных и вертикальных страйпов (чередования).

Можно создать пул носителей, выполнив следующие действия:

1. В диспетчере серверов выберите узел **Файловые службы и службы хранилища**, а затем подузел **Пулы носителей**.
2. Выберите меню **Задачи** (Tasks) на панели **Пулы носителей** и затем выберите команду **Создать пул носителей** (New Storage Pool). Будет запущен мастер создания пула хранения (New Storage Pool Wizard). Если мастер отобразит страницу **Перед началом работы** (Before You Begin), просто нажмите кнопку **Далее**.
3. На странице **Укажите имя и подсистему пула носителей** (Specify A Storage Pool Name And Subsystem) введите имя и описание пула носителей. Затем выберите исходный пул, с которым нужно работать. Исходный пул (primordial pool) — это просто группа дисков, управляемая и доступная определенному серверу через подсистему хранения. Нажмите кнопку **Далее**.

   > ***Совет***
   >
   > Выберите исходный пул для сервера, с которым нужно связать пул и для которого нужно распределить хранилище. Например, если настраиваете хранилище для CorpServer38, выберите исходный пул, доступный для CorpServer38.

4. На странице **Выбор физических дисков для пула носителей** (Select Physical Disks For The Storage Pool) выберите неиспользуемые физические диски, которые станут частью пула носителей, а затем укажите тип выделения каждого диска. Пул носителей должен иметь более одного диска для применения функций зеркалирования и четности, которые используются для защиты данных в случае ошибки или сбоя. Когда устанавливаете значение **Выделение** (Allocation), помните о следующем:
   - **Автоматически** (Data Store) — диск выделяется пулу и делается доступным для использования;

- **Вручную** (Manual) — диск выделяется пулу, но он будет недоступным, пока администратор явно этого не разрешит;
- **Горячий резерв** (Hot Spare) — диск будет выделен пулу как горячий резерв, он будет использоваться, если другой диск в пуле откажет или будет удален из подсистемы.

5. Как только будете готовы продолжить, нажмите кнопку **Далее**. После подтверждения установленных параметров нажмите кнопку **Создать** (Create). Мастер покажет ход выполнения создания пула. Когда мастер закончит создавать пул, будет отображена страница **Просмотр результатов** (View Results). Просмотрите ее, чтобы убедиться в успешном завершении всех фаз, а затем нажмите кнопку **Закрыть**.

Если на каком-то этапе конфигурации произошел сбой, определите причину отказа и примите меры по ликвидации последствий, а затем заново повторите эту процедуру.

♦ Если один из физических дисков уже отформатирован и содержит том, вы получите следующую ошибку:

Не возможно создать пул носителей. Один из физических дисков не поддерживает эту операцию. (Could not create storage pool. One of the physical disks specified is not supported by this operation.)

Эта ошибка возникает, потому что физические диски, которые вы хотите добавить в пул носителей, не могут содержать существующие тома. Для решения этой проблемы вам нужно повторить процедуру и выбрать другой физический диск или же удалить все существующие тома на физическом диске, повторить процедуру и выбрать этот диск снова. Помните, что удаление тома стирает все данные на нем.

♦ Если один из выбранных дисков стал недоступен после того, как вы его выбрали, вы получите следующую ошибку:

Не возможно создать пул носителей. Один или более параметров, переданных методу, неправильны. (Could not create storage pool. One or more parameter values passed to the method were invalid.)

Эта ошибка возникает потому, что выбранный физический диск стал недоступен или перешел в состояние оффлайн. Чтобы решить эту проблему, вам нужно: а) повторить процедуру и выбрать другой физический диск; б) перевести физический диск в состояние онлайн (если получится), повторить процедуру и выбрать этот диск снова.

> ***Примечание***
>
> Внешний диск может стать недоступным по самым разным причинам. Например, может быть просто отсоединен кабель или LUN, ранее выделенный серверу, возможно, был перераспределен другим администратором.

Создание виртуального диска в дисковом пространстве

После создания пула носителей можно выделить пространство из пула виртуальным дискам, которые будут доступны серверам. Каждый физический диск в пуле может использоваться одним из трех способов:

- как хранилище данных, доступное для использования;
- как хранилище данных, которое может быть вручную выделено для использования;
- как горячая замена в случае, если диск в пуле откажет или будет удален из подсистемы.

Если в пуле носителей только один диск, будет только одна опция выделения пространства на этом диске — создание виртуальных дисков с простой (simple) разметкой. Простая разметка не защищает от отказа диска. Если в пуле носителей есть несколько дисков, можно использовать следующие опции.

- **Mirror.** При выборе разметки Mirror данные дедуплицируются на дисках с использованием техники зеркалирования, подобной той, которая была ранее рассмотрена в этой главе. Однако техника зеркалирования более сложна тем, что данные зеркалируются на два или три диска за один раз. У этого метода есть свои преимущества и недостатки. Здесь, если в пространстве хранилища есть два или три диска, гарантируется полная защита от сбоя одного диска, а если в пространстве находится пять или более дисков, гарантируется защита от одновременного отказа двух дисков. Недостаток заключается в том, что зеркалирование уменьшает полезную емкость на 50%. Например, если зеркально отражаются два диска по 1 Тбайт каждый, можно использовать только 1 Тбайт для хранения данных.
- **Parity.** При выборе этого типа разметки данные и информация четности чередуются по физическим дискам с использованием метода чередования с контролем четности, подобно тому, который был ранее рассмотрен в этой главе. Подобно стандартному чередованию с контролем четности, у этого метода есть преимущества и недостатки. Нужны как минимум три диска, чтобы полностью защитить свою систему от сбоя одного диска. С чередованием тоже будут потери емкости, но не такие большие, как с зеркалированием.

Можно создать виртуальный диск в пуле носителей, выполнив следующие действия:

1. В диспетчере серверов выберите узел **Файловые службы и службы хранилища**, а затем подузел **Пулы носителей**.
2. На панели **Виртуальные диски** (Virtual Disks) выберите меню **Задачи** (Tasks), а из появившегося списка — команду **Создать виртуальный диск** (New Virtual Disk). Будет запущен мастер создания виртуальных дисков (New Virtual Disk Wizard).
3. На странице **Выбор пула носителей** (Storage Pool) выберите пул носителей, в котором нужно создать виртуальный диск, и нажмите кнопку **Далее**. Для каждого доступного пула выводится сервер, которым он управляется. Убедитесь, что пул содержит достаточно свободного пространства для создания виртуального диска.

   Совет

   Выберите пул носителей для сервера, с которым нужно связать виртуальный диск. Например, если настраиваете хранилище для CorpServer38, нужно выбрать пул носителей, который доступен серверу CorpServer38.

4. На странице **Назначение имени виртуального диска** (Specify The Virtual Disk Name) введите имя и описание виртуального диска. Если применяется комбинация SSD и HDD, используйте предоставленный флажок, чтобы указать, где вы хотите

создать уровни хранилища. Используя уровни хранилища, можно добиться перемещения часто применяемых файлов с более медленного HDD на более быстрый SDD-диск. Данная возможность недоступна для серверов, где используется только HDD-диски или только SSD-диски. Нажмите кнопку **Далее**.

5. На странице **Выбор структуры хранилища** (Select The Storage Layout) выберите разметку хранилища, соответствующую требованиям надежности и избыточности. Для пулов, состоящих из одного диска, доступна только простая разметка (**Simple**). Если есть несколько дисков в пуле, то можно выбрать разметку **Simple**, **Mirror** или **Parity**. Нажмите кнопку **Далее**.

   Практический совет

   Если в системе нет достаточного количества доступных дисков, чтобы реализовать структуру хранилища, администратор получит ошибку: *"Пул носителей содержит недостаточно физических дисков для поддержки выбранной структуры хранилища. Выберите другую структуру"* ("The storage pool does not contain enough physical disks to support the selected storage layout"). Выберите другую структуру или повторите эту процедуру и выберите другой пул носителей.

   Следует иметь в виду, что у пула носителей может быть один или несколько дисков, выделенных как горячий резерв. Горячие резервы создаются автоматически, чтобы была возможность восстановления после отказа диска, если используются зеркалирование или четность — и иначе быть не может. Если нужно, чтобы Windows использовала горячий резерв, администратор может удалить горячий резерв из пула носителей, щелкнув по нему правой кнопкой мыши и выбрать команду **Извлечь диск**[1]. Затем нужно добавить диск назад в пул носителей, щелкнув по пулу правой кнопкой мыши и выбрав команду **Добавить физический диск** (Add Physical Drive). К сожалению, в результате этой операции диск, который раньше использовался для горячего резерва, будет переведен в нездоровое состояние и при попытке добавления диска в пул носителей вы получите ошибку, связанную с тем, что конфигурация пула носителей доступна только для чтения. Но фактически, пул не находится в состоянии только для чтения. Если бы пул хранения был в состоянии только для чтения, то администратор мог бы ввести следующую команду в приглашении Windows PowerShell, чтобы очистить это состояние:

   ```
   Get-Storagepool "PoolName" | Set-Storagepool -IsReadonly $false
   ```

   Однако данная команда не решит проблему. Чтобы избавиться от этой ошибки, нужно сбросить дисковые пространства и связанную подсистему. Для этого проще перезагрузить сервер. После перезагрузки сервера пул носителей данных перейдет из состояния ошибки (красный кружок с белым крестом внутри) в состояние предупреждения (желтый треугольник с восклицательным знаком). Тогда можно удалить физический диск из пула хранения данных, щелкнув по нему правой кнопкой мыши и выбрав команду **Извлечь диск**. Позже можно добавить физический диск, щелкнув по пулу носителей правой кнопкой и выбрав команду **Добавить физический диск** (Add Physical Drive).

6. На странице **Указание типа подготовки** (Specify The Provisioning Type) выберите тип подготовки. Можно выбрать **Тонкая** (Thin) или **Фиксированный** (Fixed). При тонкой подготовке том использует пространство пула по мере необходимости в зависимости от размера тома. Если выбрать тип **Фиксированный**, у тома будет фиксированный размер, и он будет использовать пространство из пула, равное размеру тома. Нажмите кнопку **Далее**.

---

[1] Щелкать нужно по диску в области **Физические диски**. — *Прим. пер.*

7. На странице **Указание размера виртуального диска** (Specify The Size Of The Virtual Disk) используйте предоставленные опции для указания размера виртуального диска. Если выбрать флажок **Создать максимально большой виртуальный диск в пределах указанного размера** (Create The Largest Virtual Disk Possible), то созданный диск захватит все доступное пространство. Например, если создается фиксированный диск размером 2 Тбайт с простой разметкой и только 1,5 Тбайт дискового пространства доступно, будет создан фиксированный диск размером 1,5 Тбайт. Помните, что если диск зеркалируется или чередуется, он может использовать больше свободного пространства, чем будет указано.
8. Когда будете готовы продолжить, нажмите кнопку **Далее**. После подтверждения установленных параметров нажмите кнопку **Создать**. Мастер покажет ход выполнения процесса создания диска. Как только мастер закончит создавать диск, будет отображена страница **Просмотр результатов**. Просмотрите подробности и убедитесь, что все этапы были успешно выполнены. Если на каком-то этапе конфигурации произошел сбой, определите причину отказа и примите меры по ликвидации последствий, а затем заново повторите эту процедуру.
9. Нажмите кнопку **Закрыть**, будет автоматически запущен мастер создания томов (New Volume Wizard). Используйте его для создания тома, как описано в *разд. "Создание стандартного тома" далее в этой главе*.

Создание стандартного тома

Стандартные тома могут быть созданы как на физических, так и на виртуальных дисках. Для создания тома используется один и тот же способ, независимо от того, как диск представлен серверу. Это позволяет создавать стандартные тома на внутренних дисках сервера, на виртуальных дисках в подсистеме хранения, доступной на сервере, и на виртуальных дисках iSCSI, доступных на сервере. Если нужно добавить дедупликацию данных на сервер, можно включить дедупликацию для стандартных томов, созданных для того сервера.

Для создания стандартного тома выполните следующие действия:

1. Запустите мастер создания томов (New Volume Wizard). Этот мастер автоматически запускается после создания пространства хранилища. Запустить его вручную можно одним из двух способов:
   - в подузле **Диски** на панели **диски** выводятся все доступные диски. Выберите диск, с которым нужно работать, а затем из меню **Задачи** выберите команду **Создать том**;
   - в подузле **Пулы носителей** на панели **виртуальные диски** (Virtual disks) выводятся все доступные виртуальные диски. Выберите диск, с которым нужно работать, а затем из списка **Задачи** выберите команду **Создать том**.
2. На странице **Выбор сервера или диска** (Select the server and disk) выберите сервер, на котором находится хранилище, а затем — диск, на котором нужно создать том, и нажмите кнопку **Далее**. Если только что создали пространство хранения, мастер создания томов автоматически выберет нужный сервер и диск, поэтому надо просто нажать кнопку **Далее**.

3. На странице **Выбор размера тома** (Specify the size of the volume) используйте предоставленные параметры для установки размера тома. По умолчанию размер тома равен максимальному доступному пространству на диске. Нажмите кнопку **Далее**.
4. На странице **Назначение букве диска или папке** (Assign to a drive letter or folder) укажите, что нужно назначить — букву диска или папку, и нажмите кнопку **Далее**. Можно использовать следующие параметры:
   - **Буква диска** (Drive letter) — для назначения буквы, выберите этот параметр и укажите доступную букву из предоставленного списка;
   - **Следующая папка** (Following folder) — для назначения пути, выберите этот параметр и введите путь к существующей папке на NTFS-диске или же используйте кнопку **Обзор** для поиска или создания папки;
   - **Не назначать букве диска или папке** (Don't assign to a drive letter or drive path) — том будет создан без назначения букве диска или папке. При необходимости можно назначить том букве диска или папке позже.
5. На странице **Выбор параметров файловой системы** (Select file system settings) укажите, как том должен быть отформатирован:
   - **Файловая система** — тип файловой системы, например NTFS или ReFS;
   - **Размер кластера** — размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно установить размер кластера в определенное значение;
   - **Метка тома** — метка, т. е. название тома.
6. Если выбрана файловая система NTFS и добавлена дедупликация данных на сервер, можно включить и настроить дедупликацию данных. Как только будете готовы продолжить, нажмите кнопку **Далее**.
7. После подтверждения установленных параметров нажмите кнопку **Создать**. Мастер покажет ход выполнения создания тома. Когда мастер закончит создавать том, он отобразит страницу **Просмотр результатов**. Просмотрите ее, чтобы убедиться в успешном завершении всех этапов. Если на каком-то этапе произошел сбой, определите причину сбоя и устраните ее перед повторением этой процедуры.
8. Нажмите кнопку **Закрыть**.

Практический совет

В реестре, в `HKLM\SYSTEM\CurrentControlSet\Control\FileSystem`, параметры `NtfsDisableLastAccessUpdate` и `RefsDisableLastAccessUpdate` определяют, должны ли NTFS и ReFS обновлять последнюю метку времени доступа на каждом каталоге, когда происходит вывод содержимого каталога. Если на загруженном сервере очень много каталогов и сервер не очень быстро реагирует при выводе содержимого каталогов, причина может быть в том, что буфер журнала файловой системы в физической памяти заполнен записями обновления метки времени. Для предотвращения этой проблемы можно установить эти параметры в 1. При этом файловая система не будет обновлять последнюю метку времени доступа, что положительно повлияет на производительность. Иначе, если значение установлено в 0 (по умолчанию), файловая система будет обновлять метку времени на каждом каталоге и это изменение будет записано в журнал файловой системы.

Поиск и устранение неисправностей дисковых пространств

Ранее были рассмотрены типичные проблемы, возникающие при создании дисковых пространств и выделении пространств. Администратор может обнаружить, что физический диск, который должен быть доступен для использования, недоступен. Узел **Пулы носителей**, выбранный в Диспетчере серверов, позволяет добавить физический диск, который был обнаружен, но не указан как доступный. Для этого нужно выбрать элемент **Задачи** (Tasks) на панели **Физические диски** (Physical Disks), а затем выбрать команду **Добавить физический диск** (Add Physical Disk). В окне **Добавление физического диска** (Add Physical Disk) выберите физический диск, а затем нажмите кнопку **OK**. Альтернативно, если физический диск не был обнаружен дисковыми пространствами, выберите **Задачи** на панели **Пулы носителей** (Storage Pools), а затем выберите команду **Повторно сканировать хранилище** (Rescan Storage).

Другие проблемы, с которыми администратор может столкнуться при работе с дисковыми пространствами, имеют отношение отказам диска и потере избыточности. Когда дисковое пространство использует двухстороннее зеркало, трехстороннее зеркало, четность или двойную четность, можно восстановить избыточность, повторно подключив отключенный диск или заменив отказавший диск. Когда дисковое пространство использует простой том и диски были отсоединены, можно восстановить том, переподключив диски.

Выбор значка уведомления в Центре поддержки (Action Center) выведет на экран связанные уведомления. Если проблема связана с дисковыми пространствами, Центр поддержки обновит соответствующую панель уведомления сообщением "Проверьте дисковые пространства на наличие проблем" ("Check Storage Spaces for issues"). Чтобы открыть диспетчер серверов, выберите значок уведомления, а затем предоставленную ссылку. В диспетчере серверов нужно выбрать узел **Файловые службы и службы хранилища** (File And Storage Services), а затем узел **Пулы носителей** (Storage Pools), после чего можно будет ознакомиться с произошедшей ошибкой.

Чтобы просмотреть ошибки и предупреждения для пулов носителей, щелкните правой кнопкой мыши по пулу носителей со значком ошибки или предупреждения, а затем выберите команду **Свойства**. В диалоговом окне **Свойства** выберите пункт **Работоспособность** (Health), чтобы просмотреть состояние работоспособности и рабочее состояние. Например, состояние работоспособности может быть как **Предупреждение** (Warning), а рабочее состояние как **Деградация** (Degraded). Данное рабочее состояние может быть следствием потери избыточности.

Чтобы просмотреть ошибки и предупреждения для виртуальных дисков и связанных с ними физических дисков, щелкните правой кнопкой мыши по виртуальному диску со значком ошибки или предупреждения, а затем выберите команду **Свойства**. В одноименном диалоговом окне выберите пункт **Работоспособность** (Health), чтобы просмотреть состояние работоспособности и рабочее состояние. Обратите внимание на структуру хранилища и используемые физические диски. Если проблема связана с физическим диском, например, потеря связи с ним, тогда это состояние будет отображено. Состояние **Связь потеряна** (Loss of Communication) выводится, когда физический диск отсутствует, отказал или отключен.

Когда дисковые пространства используют внешние диска, отсутствующий диск — типичная проблема, с которой сталкивается администратор. В этом случае пользователи могут продолжить работу, а избыточность будет восстановлена, когда администратор переподключит диск. Однако, если произошел отказ диска, администратору нужно выполнить следующие шаги для восстановления избыточности:

1. Физически отключите отказавший диск. Если диск — внутренний, перед его отключением необходимо завершить работу компьютера и отключить питание. В противном случае просто отключите внешний диск.
2. Физически добавьте или подключите диск замены. Далее добавьте диск в дисковое пространство с помощью следующих действий.
   - На панели **Пулы носителей** (Storage spaces) щелкните правой кнопкой мыши на дисковом пространстве, которое нужно настроить, и выберите команду **Добавить физический диск** (Add Physical Drive).
   - В окне **Добавление физического диска** (Add Physical Disk) выберите диск, который должен быть добавлен в пул носителей.
   - Нажмите кнопку **OK**. При этом Windows Server подготовит диск и выделит его в пул носителей.
3. После этого отказавший диск будет в состоянии **Retired**. Удалите отказавший диск из пула носителей, щелкнув по нему правой кнопкой мыши и выбрав команду **Извлечь диск** (Remove Disk), а затем подтвердите удаление, нажав кнопку **Да** (Yes).

Затем Windows Server восстановит избыточность, скопировав необходимые данные на новый диск. Во время этого процесса состояние дискового пространства будет **Восстановление** (Repairing). Также будет выводиться индикатор прогресса, позволяющий оценить ход процесса восстановления избыточности. Когда его значение достигнет 100%, восстановление будет завершено.

Управление существующими разделами и дисками

Оснастка **Управление дисками** предоставляет множество способов управления существующими разделами и дисками. Можно назначать буквы дискам, удалять разделы, устанавливать активный раздел и т. д. Дополнительно ОС Windows Server 2012 R2 предоставляет другие утилиты для выполнения общих задач, таких как форматирование тома в NTFS, проверка диска на наличие ошибок, очистка неиспользуемого пространства диска.

> ***Примечание***
>
> Windows Vista, как и все последующие версии Windows, поддерживает сменные носители, которые могут использовать NTFS-тома. Эта возможность позволяет форматировать в NTFS флешки (USB-диски) и другие подобные устройства. В результате гарантируется защита от потери данных при извлечении сменного носителя, отформатированного в NTFS.

Назначение буквы диска или путей

Можно назначить диску одну букву или один или более путей диска при условии, что пути диска смонтированы на дисках NTFS. Дискам может быть не назначена ни буква диска, ни путь. Такие диски рассматриваются как размонтированные, и их можно смонтировать позже, присвоив букву диска или путь. Перед перемещением диска на другой компьютер его нужно размонтировать.

ОС Windows не может изменить букву системного, загрузочного томов или тома, на котором находится файл подкачки. Для изменения буквы диска системного или загрузочного тома нужно редактировать реестр, как описано в статье Microsoft Knowledge Base 223188 (**support.microsoft.com/kb/223188/**). Перед изменением буквы диска тома, на котором находится файл подкачки, нужно переместить файл подкачки на другой том.

Для управления буквами дисков и путями щелкните на диске, который нужно настроить в оснастке **Управление дисками**, и выберите команду **Изменить букву диска или путь к диску** (Change Drive Letter And Paths). Откроется окно, изображенное на рис. 2.8. Теперь можно сделать следующее:

- *добавить путь диска* — нажмите кнопку **Добавить**, выберите переключатель **Подключить том как пустую NTFS-папку** (Mount In The Following Empty NTFS Folder) и введите путь к существующей папке или нажмите кнопку **Обзор** для поиска или создания папки;
- *удалить путь диска* — выберите путь диска, который нужно удалить, нажмите кнопку **Удалить**, а затем кнопку **Да**;
- *назначить букву диска* — нажмите кнопку **Добавить**, установите переключатель **Назначить букву диска** (Assign The Following Drive Letter), а затем выберите доступную букву, чтобы назначить ее диску;
- *изменить букву диска* — выберите текущую букву, а затем нажмите кнопку **Изменить** (Change), установите переключатель **Назначить букву диска** и выберите другую букву из списка;
- *удалить букву диска* — выберите текущую букву диска и нажмите кнопку **Удалить**, а затем кнопку **Да**.

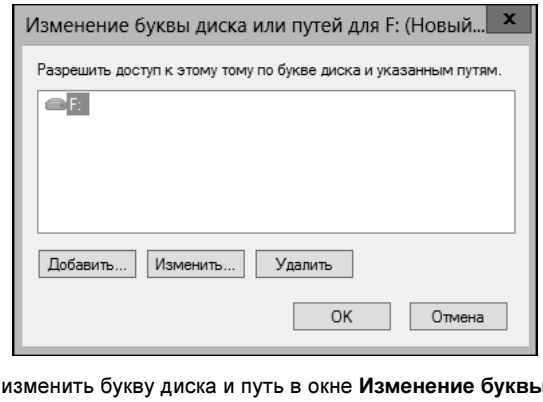


Рис. 2.8. Можете изменить букву диска и путь в окне **Изменение буквы диска или путей**

Примечание

Если попытаетесь изменить букву диска, который в данный момент используется, Windows Server 2012 R2 отобразит предупреждение. Нужно закрыть программы, которые используют диск, и попробовать снова изменить букву диска или же разрешить оснастке **Управление дисками** принудительно изменить букву, нажав кнопку **Да** в предупреждении.

Изменение или удаление метки диска

Метка тома — это текстовый дескриптор диска. При использовании FAT максимальный размер метки — 11 символов, разрешено использовать пробелы. В NTFS максимальный размер метки тома — 32 символа. Хотя FAT не разрешает использовать некоторые специальные символы (* / \ [ ] : ; | = , . + " ? < >), в NTFS не будет никаких проблем с такими символами.

Поскольку метка тома отображается при доступе к диску в разных утилитах Windows Server 2012 R2, в том числе в Проводнике, она может использоваться для предоставления информации о содержимом диска. Можно изменить или удалить метку тома, используя оснастку **Управление дисками** или Проводник.

Используя оснастку **Управление дисками**, можно изменить метку так:

1. Щелкните правой кнопкой мыши на разделе и затем выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** введите новую метку тома в предоставленное текстовое поле или удалите существующую метку. Нажмите кнопку **OK**.

Используя Проводник, можно изменить метку так:

1. Щелкните правой кнопкой мыши на значке диска и выберите команду **Свойства**.
2. На вкладке **Общие** окна **Свойства** введите новую метку тома в предоставленное текстовое поле или удалите существующую метку. Нажмите кнопку **OK**.

Удаление разделов и дисков

Для изменения конфигурации диска, дисковое пространство которого полностью распределено, нужно удалить существующие разделы и логические диски. Удаление раздела или диска удаляет связанную файловую систему, и все данные в файловой системе будут потеряны. Перед удалением раздела или диска нужно сделать резервную копию всех файлов и каталогов, содержащихся на этом разделе или диске.

Примечание

Для защиты целостности системы нельзя удалить системный или загрузочный раздел. Однако Windows Server 2012 R2 позволяет удалить активный раздел или том, если он не назначен как загрузочный или системный. Убедитесь, что удаляемый раздел или том не содержит важных данных или файлов.

Можно удалить первичный раздел, том или диск с помощью следующих действий:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши по разделу, тому или диску, который нужно удалить, а затем выберите команду **Проводник** (Explore). Используя Проводник, переместите все данные на другой том или проверьте существующие резервные копии, чтобы убедиться, что данные сохранены надлежащим образом.

2. В оснастке **Управление дисками** щелкните правой кнопкой мыши по разделу, тому или диску, а затем выберите команду **Удалить раздел** (Delete Partition), **Удалить том** (Delete Volume) или **Удалить логический диск** (Delete Logical Drive) соответственно.
3. Подтвердите удаление, нажав кнопку **Да**.

Действия по удалению расширенного раздела слегка отличаются от удаления первичного раздела или логического диска. Для удаления расширенного раздела выполните такие действия:

1. Удалите все логические диски, как было описано ранее.
2. Выберите область расширенного раздела и удалите ее.

Преобразование тома в NTFS

ОС Windows Server 2012 R2 предоставляет утилиту для преобразования томов FAT в NTFS. Эта утилита называется Convert (Convert.exe) и расположена в папке *%SystemRoot%*. При конвертировании тома с использованием этой утилиты структура файлов и каталогов сохраняется, и данные не будут потеряны. Помните, однако, что в Windows Server 2012 R2 нет утилиты для обратного преобразования из NTFS в FAT. Единственный способ преобразовать раздел с NTFS в FAT — удалить его и создать на его месте FAT-том.

Синтаксис утилиты Convert

Утилита Convert запускается в командной строке. Если нужно конвертировать диск, используйте следующий синтаксис:

```
convert volume /FS:NTFS
```

Здесь *volume* — буква диска с двоеточием, путь диска или имя тома. Например, если нужно преобразовать диск D: в NTFS, используйте команду:

```
convert D: /FS:NTFS
```

Если у тома есть метка, программа попросит ее ввести. Программа не будет просить ввода метки, если та не установлена.

Полный синтаксис программы Convert следующий:

```
convert volume /FS:NTFS [/V] [/X] [/CvtArea:filename] [/NoSecurity]
```

Параметры программы следующие:

- *volume* — задает том, с которым нужно работать;
- /FS:NTFS — преобразование в NTFS;
- /V — включает подробный режим;
- /X — принудительное размонтирование тома перед преобразованием (если необходимо);
- /CvtArea:*filename* — устанавливает имя непрерывного файла в корневом каталоге для резервирования файла для системных файлов NTFS;

- `/NoSecurity` — к преобразуемым файлам будет разрешен доступ для всех пользователей.

Еще один пример вызова Convert:

```
convert C: /FS:NTFS /V
```

Использование утилиты Convert

Перед применением утилиты Convert определите, используется ли раздел в качестве активного загрузочного раздела или системного раздела, содержащего операционную систему. Можно преобразовать активный загрузочный раздел в NTFS. Выполнение этой операции требует, чтобы система получила эксклюзивный доступ к этому разделу, который может быть получен только во время запуска. Таким образом, если попытаетесь преобразовать активный загрузочный раздел в NTFS, ОС Windows Server 2012 R2 отобразит подсказку, позволяющую запланировать преобразование при следующем запуске системы. Если нажать кнопку **Да**, можно перезапустить систему, чтобы начать процесс преобразования.

> ***Совет***
>
> Часто нужно перезагружать систему несколько раз, чтобы полностью завершить преобразование активного загрузочного раздела. Не паникуйте. Позвольте системе завершить преобразование.

Перед тем как утилита Convert преобразует диск в NTFS, она проверит, достаточно ли на диске свободного места для осуществления преобразования. Вообще говоря, Convert требует 25% свободного дискового пространства от общей емкости используемого пространства. Например, если на диске хранится 200 Гбайт данных, утилите Convert нужно около 50 Гбайт свободного пространства. Если на диске не хватает свободного пространства, Convert прервет процесс преобразования и сообщит о том, что нужно освободить дополнительное место на диске. С другой стороны, если на диске достаточно места, Convert начнет процесс преобразования, который занимает несколько минут (или чуть больше для больших дисков). Будьте терпеливы. Не нужно открывать файлы или запускать приложения на диске, пока идет процесс преобразования.

Можно использовать параметр `/CvtArea` для улучшения производительности тома путем резервирования пространства для главной файловой таблицы (Master File Table, MFT). Данная опция помогает предотвратить фрагментацию MFT. Как? Со временем объем MFT может превысить размер дискового пространства, выделенного для нее. В этом случае операционная система должна расширить MFT на другие области диска. Несмотря на то, что утилита оптимизации дисков может дефрагментировать MFT, она не способна переместить первый раздел MFT, и маловероятно, что после MFT будет существовать свободное пространство, поскольку оно будет заполнено данными файла.

Чтобы предотвратить фрагментацию в некоторых случаях, нужно зарезервировать больше свободного пространства, чем резервируется по умолчанию (12,5% размера раздела или тома). Например, можно увеличить размер MFT, если том будет содержать много маленьких файлов (или файлов среднего раздела), а не большие файлы. Чтобы указать резервируемое пространство, можно использовать утилиту FSUtil для создания специального файла-заполнителя, размер которого равен размеру требуемого резерви-

руемого пространства для MFT. Конвертировать том в NTFS и указать имя файла-заполнителя можно опцией `/CvtArea`.

В следующем примере утилита FSUtil используется для создания заполнителя размером около 1,5 Гбайт (1 500 000 000 байтов) с именем temp.txt:

```
fsutil file createnew c:\temp.txt 1500000000
```

Чтобы использовать этот файл-заполнитель для MFT во время преобразования диска C: в NTFS, нужно ввести следующую команду:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Заметьте, что файл-заполнитель создается на разделе или томе, который преобразуется. Во время процесса преобразования файл будет перезаписан метаданными NTFS, и любое незанятое место в файле будет зарезервировано для будущего использования MFT.

Изменение размера раздела и тома

Операционная система Windows Server 2012 R2 не использует загрузчик Ntldr и файл Boot.ini для загрузки операционной системы. Вместо этого у Windows Server 2012 R2 есть предустановочная среда, в которой имеется диспетчер начальной загрузки Windows (Windows Boot Manager) для управления запуском системы, загружающий выбранное загрузочное приложение. Диспетчер начальной загрузки наконец-то освобождает операционную систему от зависимости от MS-DOS, так что можно использовать диски по-новому. В Windows Server 2012 R2 можно сжимать или расширять базовые или динамические диски. Для этого применяется либо оснастка **Управление дисками**, либо утилита DiskPart. Нельзя сжать или расширить чередуемые, зеркальные и чередуемые с контролем четности тома.

При расширении тома конвертируются области нераспределенного пространства и затем добавляются к существующему тому. Для составных томов на динамических дисках пространство можно взять с любого доступного динамического диска, не только с того, где том был создан. Поэтому можно комбинировать области свободного пространства на разных дисках и использовать их для увеличения размера существующего тома.

> ***Внимание!***
>
> Перед расширением тома помните о нескольких ограничениях. Можно расширить простой и составной тома, только если они форматированы в NTFS. Нельзя расширить чередующиеся тома. Также нельзя расширить тома, если они не форматированы или отформатированы как FAT. Нельзя также расширить системный или загрузочный тома независимо от их конфигурации.

Можно сжать простой или составной том так:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши по тому, который нужно сжать, и выберите команду **Сжать том** (Shrink Volume). Эта команда доступна, только если том соответствует описанным ранее критериям.
2. В окне **Сжать** (Shrink) (рис. 2.9) введите размер сжимаемого пространства. Это окно предоставляет следующую информацию:

- **Общий размер до сжатия (МБ)** (Total size before shrink in MB) — общий размер тома в мегабайтах. Это размер форматированного тома;
- **Доступное для сжатия пространство (МБ)** (Size of available shrink space in MB) — размер пространства, доступного для сжатия. Это не общее свободное пространство тома, а общее пространство, которое может быть удалено, исключая данные, зарезервированные для MFT, файлов подкачки, временных файлов и т. д.;
- **Размер сжимаемого пространства (МБ)** (Enter the amount of space to shrink in MB) — пространство, которое может быть удалено из тома. Начальное значение по умолчанию равно предыдущему значению. Для оптимальной производительности нужно убедиться, что на сжимаемом диске останется хотя бы 10% свободного пространства после операции сжатия;
- **Общий размер после сжатия (МБ)** (Total size after shrink in MB) — выводит, какой размер будет у тома после сжатия (в мегабайтах). Это и есть новый размер отформатированного тома.

3. Нажмите кнопку **Сжать** (Shrink) для сжатия тома.

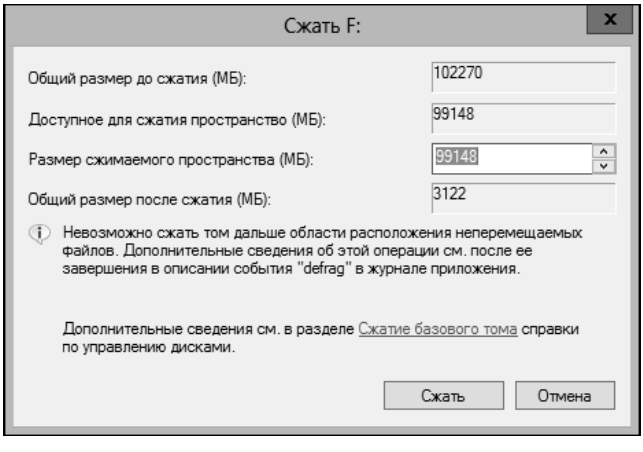


Рис. 2.9. Укажите размер сжимаемого пространства

Расширить простой или составной том можно так:

1. В оснастке **Управление дисками** щелкните правой кнопкой мыши на томе, который нужно расширить, и выберите команду **Расширить том** (Extend Volume). Эта команда будет доступна, только если том соответствует описанным ранее критериям, и на одном или нескольких динамических дисках доступно свободное пространство.
2. В окне приветствия мастера расширения тома (Extend Volume Wizard) нажмите кнопку **Далее**.
3. На странице **Выбор дисков** выберите диск или диски, с которых нужно взять свободное пространство. Будут автоматически выбраны все используемые тома дисков. По умолчанию будет выбрано все используемое пространство на тех дисках.

4. Для динамических дисков можно указать дополнительное пространство, которое нужно использовать на других дисках, так:
   - выберите диск из списка **Доступно** и нажмите кнопку **Добавить** для добавления диска в список **Выбраны**;
   - выберите каждый диск в списке **Выбраны**, а затем в списке **Выберите размер выделяемого пространства (МБ)** (Select The Amount Of Space In MB) укажите размер неиспользуемого пространства, которое нужно добавить к выбранному диску.
5. Нажмите кнопку **Далее**, после чего просмотрите параметры и нажмите кнопку **Готово**.

Автоматическое исправление ошибок диска

Операционная система Windows Server 2012 R2 содержит дополнительные функции, сокращающие число ручных операций по обслуживанию дисков:

- транзакционная NTFS;
- самовосстанавливающаяся NTFS.

Транзакционная NTFS позволяет производить файловые операции на NTFS-томе при помощи транзакций. Это означает, что программы могут использовать транзакцию для группировки операций над файлами и реестром. Пока транзакция активна, изменения не видны вне транзакции. Изменения фиксируются и записываются на диск только, если транзакция успешно завершена. Если произошел сбой транзакции или она была выполнена не полностью, происходит откат работы транзакции для восстановления файловой системы в состояние, предшествующее транзакции.

> ***Практический совет***
>
> Файловая система ReFS (Resilient File System) содержит еще более продвинутые транзакционные и самовосстанавливающиеся функции. В ReFS используется несколько фоновых процессов для автоматического поддержания целостности диска. Процесс scrubber проверяет диск на наличие несогласованности и ошибок. Если обнаружена ошибка, процесс восстановления локализует проблемы и выполняет автоматическое исправление. В редком случае, когда на физическом диске есть поврежденные секторы, ReFS запускает процесс восстановления, чтобы отметить поврежденные секторы и удалить их из файловой системы — и все это без размонтирования тома.

Транзакции, охватывающие несколько томов, координируются диспетчером транзакций ядра (Kernel Transaction Manager, KTM). KTM поддерживает независимое восстановление томов, если произойдет сбой транзакции. Локальный диспетчер ресурсов для тома обслуживает отдельный журнал транзакций и отвечает за поддержку потоков транзакций, отдельных от потоков, осуществляющих работу с файлом.

Традиционно раньше нужно было использовать утилиту Check Disk (ChkDsk) для исправления ошибок и противоречий в NTFS-томах на диске. Поскольку этот процесс может разрушить доступность Windows-систем, ОС Windows Server 2012 R2 применяет самовосстанавливающуюся NTFS, чтобы защитить файловые системы, и не требует использования отдельных инструментов для исправления проблем. Поскольку большая часть процесса самовосстановления выполняется автоматически, нужно обслуживать

том вручную лишь в ситуации, когда будет получено уведомление от операционной системы, что проблема не может быть устранена автоматически. Если произойдет такая ошибка, Windows Server 2012 R2 уведомит о проблеме и предоставит возможные решения.

У самовосстановления NTFS есть много преимуществ по сравнению с Check Disk.

- Check Disk требует эксклюзивный доступ к тому, следовательно, системные и загрузочные тома могут быть проверены только при запуске операционной системы. А с самовосстановлением NTFS файловая система всегда доступна, и в большинстве случаев не нужно переводить ее в автономный режим для коррекции ошибок.
- Самовосстановление NTFS пытается сохранить как можно больше данных с учетом типа обнаруженной проблемы. Также самовосстановление сокращает число отклоненных запросов подключения файловой системы из-за несоответствий во время перезапуска или несоответствий на томе, который работает в оперативном режиме. Во время перезапуска самовосстановление немедленно восстанавливает том так, что он может быть смонтирован.
- Самовосстановление файловой системы NTFS уведомляет об изменениях, внесенных в том в ходе восстановления, с помощью механизмов Chkdsk.exe, уведомлений каталогов и записей журнала USN. Эта функция также позволяет авторизованным пользователям и администраторам контролировать операции восстановления. В число этих возможностей входят инициирование проверки дисков, ожидание завершения восстановления и получение сведений о ходе восстановления.
- Функция самовосстановления NTFS может восстановить том, если загрузочный сектор читаем, но невозможно идентифицировать NTFS-том. В этом случае нужно запустить автономную утилиту, которая восстановит загрузочный сектор, и затем разрешить самовосстановление NTFS для начала восстановления.

Несмотря на то, что функция самовосстановления NTFS — потрясающее улучшение, время от времени придется вручную проверить целостность диска. В этих случаях можно использовать Chkdsk.exe для обнаружения проблем на томах FAT, FAT32, exFAT и NTFS и восстановления (в случае необходимости).

> ***Внимание!***
>
> Поскольку ReFS является самокорректирующейся файловой системой, нет необходимости использовать Check Disk для проверки томов ReFS на наличие ошибок. Однако важно знать, что изначально ReFS не очень эффективно корректирует повреждения на пространствах с четностью. Данный недостаток ReFS был исправен в Windows Server 2012 R2. ReFS автоматически исправляет повреждения на пространствах с четностью, когда потоки целостности обнаруживают поврежденные данные. Когда обнаруживается повреждение, ReFS исследует копии данных и затем использует корректную версию данных, чтобы исправить проблему. Поскольку ReFS теперь поддерживает параллельные запросы I/O к одному и тому же файлу, производительность потоков целостности также улучшена.

Несмотря на то, что Check Disk может проверить и исправить много типов ошибок, утилита прежде всего ищет несогласованности в файловой системе и в ее связанных метаданных. Один из способов, с помощью которых проверка диска обнаруживает ошибки, — это сравнение битового массива тома с секторами диска, назначенными файлам в файловой системе. Вне этого полноценность утилиты проверки диска огра-

ничена. Например, утилита не может восстановить поврежденные данные в файлах, которые, возможно, структурно не повреждены.

Как часть автоматизированного обслуживания, Windows Server 2012 R2 выполняет превентивное сканирование томов NTFS. Как и с другим автоматизированным обслуживанием, Windows сканирует диски, запуская утилиту Check Disk в 2:00, если компьютер работает от сети питания и операционная система неактивна. В противном случае Windows сканирует диски в следующий раз, когда операционная система не активна и компьютер подключен к сети питания. Несмотря на то, что автоматизированное обслуживание инициировало проверку диска, процесс вызова и управления утилитой Check Disk обрабатывается отдельной задачей. В Планировщике заданий находится задача ProactiveScan в библиотеке планировщика (Microsoft\Windows\Chkdsk), и можно получить подробную информацию о выполнении этой задачи на вкладке **Журнал** (History).

Практический совет

Автоматическое обслуживание основано на диагностике Windows. По умолчанию Windows периодически осуществляет регламентное обслуживание в 2:00, если компьютер работает от сети питания и операционная система неактивна. В противном случае обслуживание будет запущено в следующий раз, когда компьютер заработает от сети питания и операционная система будет простаивать. Поскольку обслуживание запускается, только когда операционная система простаивает, обслуживанию разрешено работать в фоновом режиме в течение максимум трех дней. Это позволяет Windows завершать сложные задачи по обслуживанию автоматически. Задачи обслуживания включают обновление программного обеспечения, проверку безопасности, диагностику системы, проверку и оптимизацию дисков. Изменить время запуска автоматического обслуживания можно, открыв Центр поддержки (Action Center), развернув панель **Обслуживание** (Maintenance) и щелкнув по ссылке **Изменить параметры обслуживания** (Change Maintenance Settings). После этого нужно выбрать время запуска автоматического обслуживания.

Проверка дисков вручную

В Windows Server 2012 R2 утилита Check Disk осуществляет расширенное сканирование и восстановление диска автоматически, вместо проверки вручную, как в предыдущих версиях Windows. Здесь, при использовании утилиты Check Disk с NTFS-томами, утилита производит фоновую проверку и анализ ошибок диска. Утилита записывает любую информацию о каждом обнаруженном повреждении в системный файл $corrupt. Если том используется, обнаруженные повреждения могут быть восстановлены путем временного отключения тома. Однако размонтирование тома закрывает все открытые дескрипторы файлов. Восстановление загрузочного/системного тома происходит при следующем запуске компьютера.

Сохранение информации о повреждении и последующее восстановление тома после его размонтирования позволяют Windows быстро восстанавливать тома, а также использовать диск, пока выполняется сканирование. Как правило, оффлайн-восстановление занимает несколько секунд (сравните с устаревшими методами сканирования и восстановления, когда сканирование и восстановление больших томов длилось часами).

Примечание

FAT, FAT32 и exFAT не поддерживают расширенные функции. При использовании Check Disk с FAT, FAT32 или exFAT Windows Server 2012 R2 применяет процесс традиционного

сканирования и восстановления. Это означает, что для сканирования и восстановления нужно размонтировать том, из-за этого он не может быть использован во время сканирования. Использовать Check Disk для проверки ReFS-томов невозможно.

Можно запустить утилиту Check Disk из командной строки или из других утилит. В командной строке для проверки целостности диска E: можно ввести следующую команду:

```
chkdsk /scan E:
```

Утилита выполнит анализ диска и выведет результат проверки. Если дополнительные опции не указаны, Check Disk не будет исправлять ошибки. Для исправления ошибок на диске E: нужно ввести эту команду:

```
chkdsk /spotfix E:
```

Исправление ошибок требует эксклюзивного доступа к тому. Как он будет осуществляться, зависит от типа тома.

- Для несистемных томов будет отображен запрос: можно ли размонтировать том для восстановления? В этом случае введите Y для продолжения или N, чтобы отменить размонтирование. Если отменить размонтирование, то будет отображен другой запрос: нужно ли запланировать восстановление тома при следующем запуске компьютера? Введите Y, чтобы запланировать восстановление, или N для отмены восстановления.
- Для системных томов программа спросит, нужно ли запланировать восстановление тома при следующем запуске компьютера. Введите Y, чтобы запланировать восстановление, или N для отмены восстановления.

Нельзя запустить Check Disk с обоими параметрами — `/scan` и `/spotfix`. Причина в том, что сканирование и восстановление — независимые друг от друга задачи.

Полный синтаксис команды ChkDsk выглядит так:

```
chkdsk [volume[[path]filename]] [/F] [/V] [/R] [/X] [/I] [/C] [/B] [/L[:size]] [/scan]
[/forceofflinefix] [/perf] [/spotfix] [/sdcleanup] [/offlinescanandfix]
```

Описание параметров:

- *volume* — задает том, который нужно проверить или восстановить;
- [*path*]*filename* — только для FAT. Указывает файлы для проверки на предмет фрагментации;
- `/B` — переоценивает поврежденные кластеры тома (только для NTFS; подразумевает `/R`);
- `/C` — только для NTFS. Пропускает проверку циклов в структуре папок;
- `/F` — исправляет ошибки на диске, используя устаревшие методы;
- `/I` — только для NTFS. Менее строгая проверка элементов индекса;
- `/L:`*size* — только для NTFS. Изменяет размер файла журнала;
- `/R` — определяет поврежденные секторы и восстанавливает читаемую информацию (требует `/F`);
- `/V` — в FAT отображает полное имя (путь и имя) каждого файла на диске. В NTFS выводит сообщения об очистке (если они имеются);

- `/X` — предварительное отключение (размонтирование) тома, если необходимо (подразумевает параметр `/F`).

Для NTFS-томов утилита поддерживает расширенные параметры:

- `/forceofflinefix` — должен использоваться со `/scan`. Все найденные неполадки добавляются в очередь для восстановления в автономном режиме;
- `/offlinescanandfix` — запускает автономную проверку и исправление тома;
- `/perf` — использует больше системных ресурсов для скорейшего выполнения сканирования;
- `/scan` — выполняет упреждающее сканирование тома (по умолчанию). Обнаруженные во время сканирования ошибки будут записаны в системный файл $corrupt;
- `/sdcleanup` — очищает ненужные данные дескриптора, применяется с `/F`;
- `/spotfix` — позволяет исправить некоторые типы ошибок онлайн.

Можно запустить утилиту Check Disk интерактивно, используя Проводник или оснастку **Управление дисками**. Следуйте этим действиям:

1. Щелкните на диске и выберите команду **Свойства**.
2. На вкладке **Сервис** (Tools) нажмите кнопку **Проверить** (Check). Откроется окно **Проверка ошибок** (Check Disk), показанное на рис. 2.10.
3. Нажмите кнопку **Проверить диск** (Scan Drive) для начала сканирования. Если ошибки не будут найдены, Windows сообщит об этом. Если ошибки будут обнаружены, появятся дополнительные опции, а какие именно, зависит от типа тома, с которым производится работа — с системным или несистемным томом.

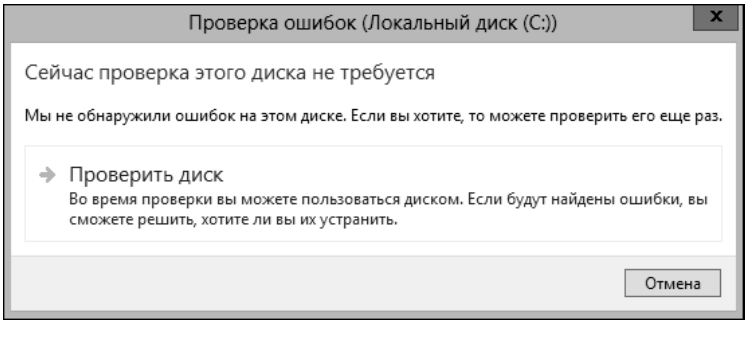


Рис. 2.10. Используйте утилиту Check Disk для проверки диска на наличие ошибок и их устранения, если они будут найдены

Примечание

Для томов FAT, FAT32 и exFAT Windows использует традиционную проверку. Для начала сканирования нужно нажать кнопку **Проверить и восстановить диск** (Scan And Repair Drive). Если при сканировании будут найдены ошибки, нужно перезапустить компьютер для их исправления.

Анализ и оптимизация дисков

При добавлении или удалении файлов данные на диске становятся фрагментированными. Когда диск фрагментирован, большие файлы не могут быть записаны в последовательную область на диске. В результате операционная система должна записать файл на несколько меньших областей диска, и значит, для чтения файла понадобится больше времени. Для сокращения фрагментации ОС Windows Server 2012 R2 может вручную или автоматически анализировать и оптимизировать диски посредством утилиты **Оптимизация дисков** (Optimize Drives).

При ручной оптимизации утилита **Оптимизация дисков** проводит анализ тома и затем сообщает процент фрагментации. Если необходима дефрагментация, можно ее осуществить. Системные и загрузочные тома могут быть дефрагментированы в оперативном режиме (без размонтирования диска), а также утилита **Оптимизация дисков** может использоваться с томами FAT, FAT32, exFAT, NTFS и ReFS.

Запустить анализ и оптимизацию диска вручную можно с помощью следующих действий:

1. В оснастке **Управление компьютером** выберите узел **Запоминающие устройства** (Storage), а затем узел **Управление дисками**. Щелкните правой кнопкой мыши на диске и выберите команду **Свойства**.
2. Перейдите на вкладку **Сервис** и нажмите кнопку **Оптимизировать** (Optimize). В окне **Оптимизация дисков** (Optimize Drives) выберите диск и нажмите кнопку **Анализировать** (Analyze). Утилита **Оптимизация дисков** (рис. 2.11) проанализи-

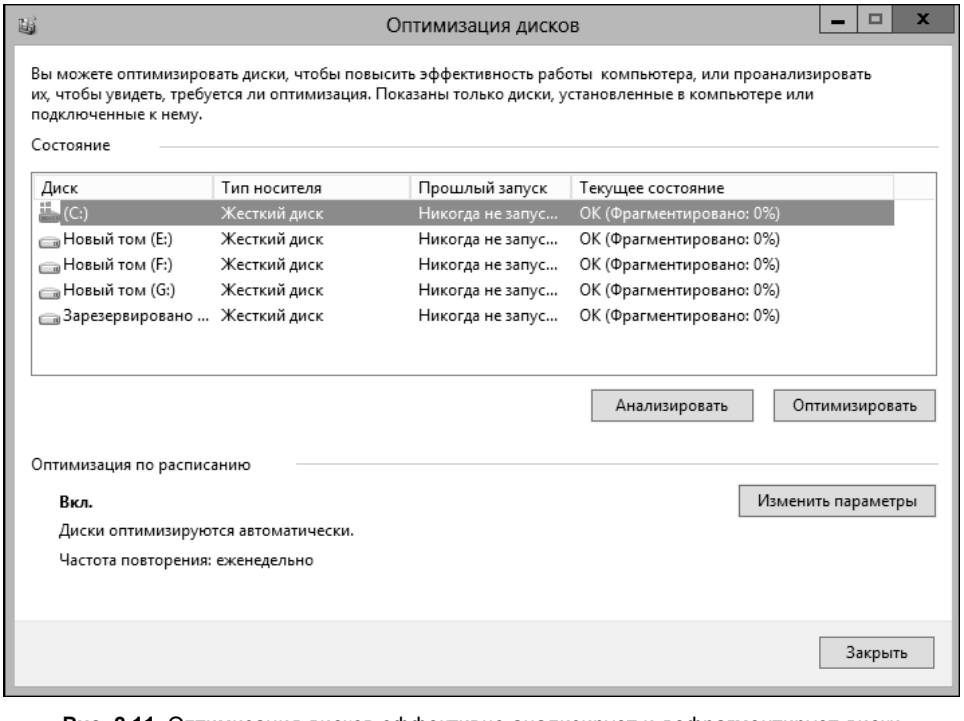


Рис. 2.11. Оптимизация дисков эффективно анализирует и дефрагментирует диски

рует диск, чтобы определить, нуждается ли он в дефрагментации. Если это так, программа порекомендует дефрагментировать диск.

3. Если диск нуждается в дефрагментации, выберите диск и нажмите кнопку **Оптимизировать**.

> ***Примечание***
>
> В зависимости от размера диска дефрагментация может занять несколько часов. Можно прервать дефрагментацию в любой момент, нажав кнопку **Стоп** (Stop).

Анализ и оптимизация дисков может происходить автоматически — когда компьютер подключен к сети питания (а не работает от аккумулятора — для ноутбуков) и когда операционная система запущена, но находится в состоянии простоя. По умолчанию оптимизация диска — это еженедельное задание, а не ежедневное, и для этого есть серьезное основание. Обычно оптимизировать диски нужно только периодически, и оптимизация раз в неделю в большинстве случаев вполне достаточна. Отметьте, однако, что хотя несистемные диски могут быть быстро проанализированы и оптимизированы, оптимизация системных дисков занимает намного больше времени.

Можно управлять приблизительным временем начала анализа и оптимизации дисков, изменяя автоматизированное время начала обслуживания. Операционная Windows Server также уведомляет, если пропущены три последовательных попытки оптимизации. Все внутренние диски и определенные внешние диски оптимизируются автоматически как часть регулярного расписания.

> ***Примечание***
>
> ОС Windows Server 2012 R2 автоматически осуществляет циклическую дефрагментацию. Благодаря этой функции, когда запланированная дефрагментация остановлена и запущена заново, компьютер автоматически продолжает дефрагментацию с места, на котором она была прервана.

Автоматической дефрагментацией можно управлять с помощью следующих действий:

1. В оснастке **Управление компьютером** выберите узел **Запоминающие устройства** (Storage), а затем узел **Управление дисками**. Щелкните правой кнопкой мыши на диске и выберите команду **Свойства**.
2. На вкладке **Сервис** нажмите кнопку **Оптимизировать**. Откроется окно **Оптимизация дисков**.
3. Если нужно изменить параметры оптимизации, нажмите кнопку **Изменить параметры** (Change Settings). Откроется окно, изображенное на рис. 2.12. Для отмены автоматической дефрагментации сбросьте флажок **Выполнять по расписанию (рекомендуется)** (Run on a schedule). Для включения автоматической дефрагментации, наоборот, установите этот флажок.
4. Частота дефрагментации по умолчанию установлена так, как показано на рис. 2.12. В раскрывающемся списке **Частота** (Frequency) можно выбрать значения **ежедневно** (Daily), **еженедельно** (Weekly) и **ежемесячно** (Monthly). Если не нужно получать уведомления о пропущенных выполнениях по расписанию, установите флажок **Уведомлять в случае пропуска трех выполнений по расписанию подряд** (Notify me if three consecutive scheduled runs are missed).

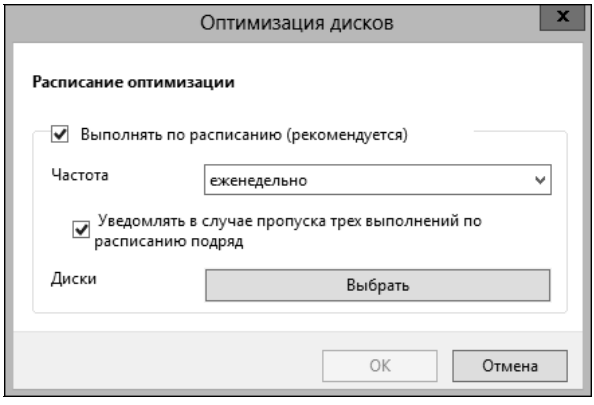


Рис. 2.12. Установите расписание для автоматической дефрагментации

5. Если нужно указать, какие диски должны быть дефрагментированы, нажмите кнопку **Выбрать** (Choose) и укажите тома, которые следует дефрагментировать. По умолчанию все диски, установленные внутри компьютера или подключенные к компьютеру, дефрагментируются. Также автоматически дефрагментируется каждый новый диск, подключенный к компьютеру. Установите флажки дисков, которые должны быть дефрагментированы, а также флажки для дисков, которые не нужно автоматически дефрагментировать. Нажмите кнопку **OK** для сохранения параметров.
6. Нажмите кнопку **OK**, а затем кнопку **Закрыть**.

ГЛАВА 3

Общий доступ к данным и избыточность

Протокол SMB (Server Message Block) — основной протокол предоставления общего доступа к файлам, используемый компьютерами под управлением Microsoft Windows. Когда к папкам предоставляется общий доступ по сети, клиент SMB применяется для чтения/записи файлов и для запроса служб с компьютеров, на которых находятся общие папки. При использовании SMB Windows Server 2012 R2 поддерживает две модели предоставления общего доступа к файлам: *стандартный общий доступ* и *папка* ***Общие*** *(Public)*. Стандартный общий доступ позволяет удаленным пользователям получить доступ к сетевым ресурсам — файлам, папкам и дискам. При предоставлении общего доступа к папке или диску все их файлы и подпапки также станут доступными определенным пользователям. Не нужно перемещать файлы из их текущего местоположения для предоставления общего доступа к ним.

Включить стандартный общий доступ к файлам можно на дисках, отформатированных как FAT, FAT32, exFAT, NTFS и ReFS. К дискам exFAT, FAT или FAT32 применяется один набор разрешений — *разрешения общего доступа*. К дискам NTFS и ReFS применяются два набора разрешений — *NTFS-разрешения* (также называются *разрешениями доступа*) и *разрешения общего доступа*. Наличие двух наборов разрешений позволяет точно определять, кто получит доступ к общим файлам, а также уровень назначенного доступа. С NTFS-разрешениями или разрешениями общего доступа не нужно перемещать файлы, к которым предоставляется общий доступ.

При использовании папки **Общие** (Public) нужно просто скопировать или переместить файлы в папку **Общие** компьютера. Общие файлы доступны любому, кто входит в компьютер локально, независимо от того, есть ли у него стандартная учетная запись или учетная запись администратора. Также можно предоставить сетевой доступ к папке **Общие**. Если сделать это, возможности как-либо ограничить доступ не будет. Папка **Общие** и все ее содержимое открыты для всех, кто может получить доступ к компьютеру по локальной сети.

Использование и включение общего доступа к файлам

Параметры общего доступа на компьютере определяют способ предоставления общего доступа к файлам. Операционная система Windows Server 2012 R2 поддерживает две модели предоставления общего доступа к файлам.

- **Стандартный общий доступ к файлам** позволяет удаленным пользователям получать доступ к файлам, папкам и дискам по сети. При предоставлении общего доступа к папке или диску все файлы и подпапки в этой папке (на диске) станут доступными определенным пользователям. Разрешения общего доступа и разрешения доступа используются для определения, кто получит доступ к общим файлам и каким будет уровень этого доступа. Не нужно перемещать файлы, к которым предоставляется общий доступ.
- Папка **Общие** предоставляет локальным и удаленным (если установлено) пользователям доступ к любым файлам, помещенным в папку *%SystemDrive%*\Пользователи\Общие (*%SystemDrive%*\Users\Public) компьютера. Разрешения доступа на папке **Общие** определяют, какие пользователи и группы могут получить доступ к общим файлам, и задают уровень этого доступа. При копировании или перемещении файлов в папку **Общие** разрешения доступа файлов изменяются так, чтобы они совпадали с разрешениями папки **Общие**. Также добавляются некоторые дополнительные разрешения. Когда компьютер — часть рабочей группы, можно добавить защиту паролем для папки **Общие**. Отдельная защита паролем не нужна в домене. В домене только пользователи домена (группа **Domain Users**) имеют доступ к папке **Общие**.

Со стандартным общим доступом к файлам локальные пользователи автоматически не получают доступ к любым данным, сохраненным на компьютере. Администратор контролирует локальный доступ к файлам и папкам, используя параметры безопасности на локальном диске. При использовании папки **Общие** файлы, скопированные или перемещенные в эту папку, доступны любому пользователю, зарегистрировавшемуся локально. Также можно предоставить сетевой доступ к папке **Общие**. В результате, однако, папка **Общие** и все ее содержимое будет открыто каждому, кто может получить доступ к компьютеру по сети.

Операционная система Windows Server 2012 R2 добавляет новые уровни безопасности с помощью комплексной проверки подлинности, технологии идентификации на основе требований и политик централизованного доступа. В Windows 8.1 и Windows Server 2012 R2 можно назначить идентификацию на основе требований к ресурсам файла и папки на томах NTFS и ReFS. В Windows Server 2012 R2 пользователям доступ к ресурсам файла и папки предоставляется непосредственно с помощью разрешений доступа и разрешений общего доступа или косвенно посредством идентификации на основе требований и политик централизованного доступа.

SMB 3.0 позволяет шифровать данные, передающиеся по сети. Можно включить SMB-шифрование для общих ресурсов на NTFS- и ReFS-томах. SMB-шифрование работает только тогда, когда компьютер, запрашивающий данные из SMB-ресурса (либо стандартный общий ресурс, либо DFS-ресурс), и сервер поддерживают SMB 3.0. Операци-

онные системы Windows 8.1 и Windows Server 2012 R2 поддерживают SMB 3.0 (они используют клиента SMB 3.0).

Папка **Общие** разработана для предоставления пользователям общего доступа к файлам и каталогам из одного расположения. В этом случае следует скопировать или переместить файлы, к которым нужно предоставить общий доступ, в папку *%SystemDrive%*\Пользователи\Общие (*%SystemDrive%*\Users\Public) компьютера. Доступ к общим файлам можно получить из Проводника. Дважды щелкните по системному диску, а затем перейдите в папку Пользователи\Общие (Users\Public).

В папке **Общие** есть несколько подпапок, которые можно использовать для организации общих файлов.

- **Общий рабочий стол** (Public Desktop) — используется для предоставления общего доступа к элементам рабочего стола. Любые файлы и ярлыки программ, помещенные в эту папку, появятся на рабочем столе всех пользователей, которые зайдут на этот компьютер (и всех сетевых пользователей, если к папке **Общие** был предоставлен сетевой доступ).
- **Общие документы** (Public Documents), **Общая музыка** (Public Music), **Общие изображения** (Public Pictures), **Общие видео** (Public Videos) — используются для предоставления общего доступа к документам и файлам мультимедиа. Все файлы, помещенные в одну из этих папок, доступны всем пользователям, которые зашли на этот компьютер (и всем сетевым пользователям, если к папке **Общие** был предоставлен сетевой доступ).
- **Общие загруженные файлы** (Public Downloads) — используются для предоставления общего доступа к загруженным файлам. Любые загрузки, помещенные в подпапку **Общие загруженные файлы**, станут доступны всем пользователям, которые зашли на этот компьютер (и всем сетевым пользователям, если к папке **Общие** был предоставлен сетевой доступ).

> ***Примечание***
>
> По умолчанию папка **Общий рабочий стол** скрыта. Для отображения скрытых папок в Проводнике выберите вкладку **Вид**, а затем нажмите кнопку **Показать или скрыть**, после — включите флажок **Скрытые элементы**.

По умолчанию доступ к папке **Общие** есть у любого пользователя с учетной записью и паролем. При копировании или перемещении файлов в папку **Общие** разрешения доступа изменяются так, чтобы соответствовать папке **Общие**, а также добавляются некоторые дополнительные разрешения.

Можно изменить настройки общего доступа папки **Общие** двумя основными способами.

- Разрешить пользователям, которые зарегистрировались на компьютере, просматривать и управлять общими файлами, но запретить сетевым пользователям доступ к этим файлам. После настройки этой опции неявные группы **Интерактивные** (Interactive), **Пакетные файлы** (Batch) и **Служба** (Service) получат особые разрешения для публичных файлов и папок.
- Разрешить пользователям с сетевым доступом просматривать и управлять общими файлами. Это позволит сетевым пользователям открывать, изменять, создавать и

удалять публичные файлы. Неявной группе **Все** (Everyone) будут предоставлены полные права к публичным файлам и папкам.

Операционная система Windows Server 2012 R2 может применять одну или обе модели совместного использования в любое время. Однако стандартный общий доступ к файлам более безопасен и предоставляет лучшую защиту, чем использование папки **Общие**, а улучшение безопасности очень важно для защиты данных организации. Со стандартным общим доступом к файлам разрешения общего доступа используются только тогда, когда пользователь пытается получить доступ к файлу или папке с другого компьютера по сети. Права доступа (разрешения доступа) используются всегда, независимо от того, зарегистрировался ли пользователь локально или удаленно для получения доступа к файлу или папке по сети. Если доступ к данным осуществляется удаленно, сначала применяются разрешения общего доступа, а затем — обычные разрешения доступа.

Как показано на рис. 3.1, можно настроить параметры базового общего доступа, используя опцию **Дополнительные параметры общего доступа** (Advanced Sharing Settings) в Центре управления сетями и общим доступом (Network and Sharing Center). Отдельные параметры предусмотрены для сетевого обнаружения, общего доступа к файлам и принтерам.

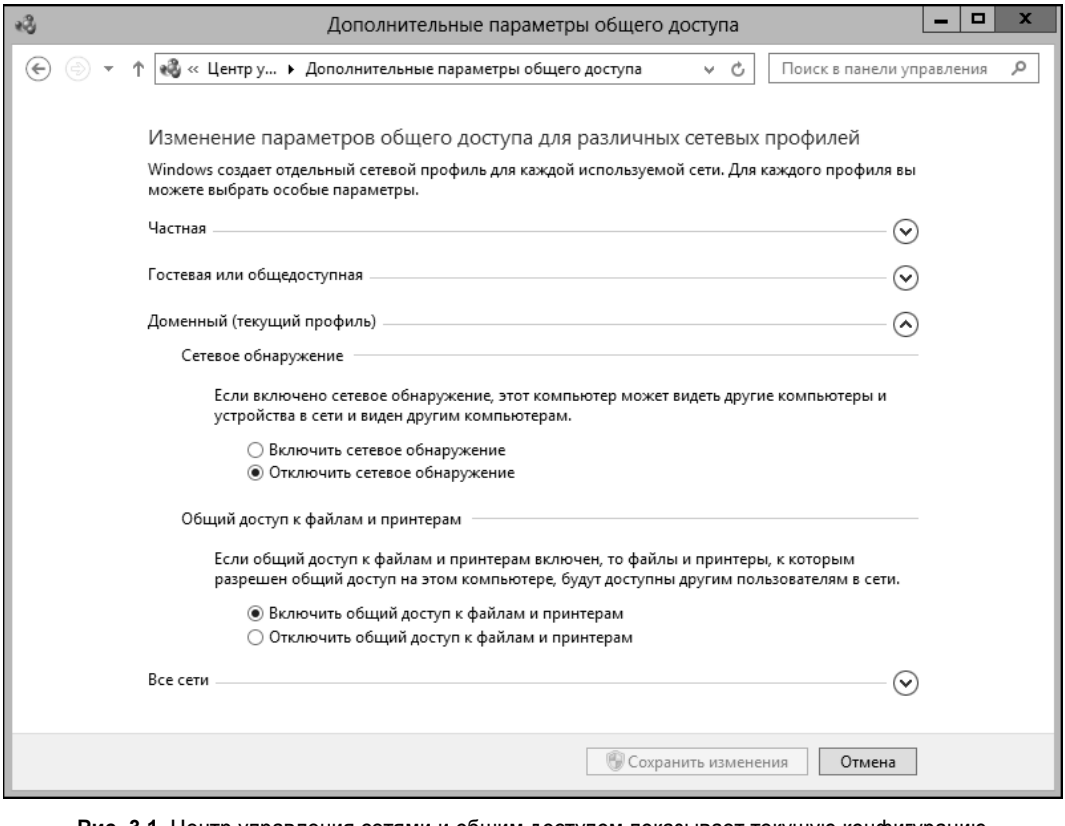


Рис. 3.1. Центр управления сетями и общим доступом показывает текущую конфигурацию

Можно управлять конфигурацией общего доступа компьютера так:

1. В Панели управления щелкните по ссылке **Просмотр состояния сети и задач** в (View network status and tasks) категории **Сеть и Интернет** (Network and Internet). В результате будет открыт Центр управления сетями и общим доступом.
2. В Центре управления сетями и общим доступом щелкните по ссылке **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) на панели слева. Выберите профиль сети, для которой нужно включить общий доступ к файлам и принтерам. Обычно это профиль **Доменный** (Domain).
3. Стандартный общий доступ к файлам и принтерам управляет сетевым доступом к общим ресурсам. Для настройки стандартного общего доступа к файлам выберите одну из опций:
   - **Включить общий доступ к файлам и принтерам** (Turn on file and printer sharing) для включения общего доступа;
   - **Отключить общий доступ к файлам и принтерам** для отключения общего доступа (Turn off file and printer sharing).
4. Доступ к общедоступным папкам контролирует доступ к папке **Общие** компьютера. Для настройки этого доступа разверните панель **Все сети** (All Networks Public Folder Sharing), нажав соответствующую кнопку. Выберите одну из опций:
   - **Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках** (Turn on sharing so anyone with network access can read and write files in the public folders) — включает доступ к папке **Общие** и ко всем общим данным для всех, кто может получить доступ к компьютеру по сети. Настройки Брандмауэра Windows (Windows Firewall) могут блокировать внешний доступ;
   - **Отключить общий доступ** (Turn off public folder sharing) — отключает общий доступ, запрещая доступ локальной сети к папке **Общие**. Любой пользователь, который зарегистрировался локально на компьютере, все еще сможет получить доступ к папке **Общие** и к ее файлам.
5. Нажмите кнопку **Сохранить изменения** (Save Changes).

Настройка стандартного общего доступа к файлам

Общие ресурсы используются для контроля доступа удаленных пользователей. Разрешения на общих папках не имеют никакого эффекта для пользователей, зарегистрировавшихся локально на сервере или рабочей станции, на которой размещены общие папки.

Понимание изменений SMB

SMB — основной протокол совместного доступа к файлам, используемый операционными системами Windows. Поскольку сама Windows изменилась за эти годы, изменил-

ся и SMB. Протокол SMB был разработан так, чтобы клиент и сервер могли согласовать между собой номер версии и использовать самую высокую версию, поддерживаемую как клиентом, который пытается подключиться к SMB-ресурсу, так и сервером, предоставляющим доступ к этому ресурсу.

Текущая версия SMB — 3.02. Она поддерживается операционными системами Windows 8.1 и Windows Server 2012 R2. Поэтому, когда компьютер под управлением Windows 8.1 подключается к SMB-ресурсу, размещенному на сервере под управлением Windows Server 2012 R2, используется версия 3.02 протокола SMB.

Самая ранняя реализация SMB называлась CIFS. Данная реализация использовалась операционной системой Windows NT 4.0. После нее появился SMB 1.0, который использовался всеми версиями Windows — от Windows 2000 до Windows Server 2003 R2. Начиная с Windows 8.1 и Windows Server 2012 R2, поддержка CIFS и SMB 1.0 — дополнительная опция, которая должна быть активирована вручную. Поскольку CIFS и SMB 1.0 устарели, не обеспечивают должного уровня функциональности и безопасности, компонент **Поддержка протокола общего доступа к файлам SMB 1.0/CIFS и протокола браузера компьютеров** (SMB 1.0/CIFS File Sharing Support) включать не нужно за исключением случаев крайней необходимости. А такая необходимость может возникнуть только в случае, если компьютеру, работающему под управлением устаревшей версии Windows, нужно соединиться с сервером, работающем под управлением Windows Server 2012 R2.

Таблица 3.1 предоставляет сводку версий протокола SMB, использующихся в актуальных версиях Windows, а также краткое описание функций, предоставляемых той или иной версией SMB. Определить версию SMB можно с помощью команды `Get-SmbConnection`, введенной в командной строке Windows PowerShell, запущенной с правами администратора. В выводе команды версия SMB выводится в колонке `Dialect`, что и показано в следующем демонстрационном выводе:

```
ServerName ShareName   UserName        Credential      Dialect NumOpens
---------- ---------   --------        ----------      ------- --------
Server36   IPC$        CPANDL\williams CPANDL\williams 3.02    0
Server36   PrimaryData CPANDL\williams CPANDL\williams 3.02    14
```

Таблица 3.1. *Обзор текущих версий SMB*

Версия SMB	Версия Windows	Функции
SMB 2.0	Windows Vista SP1, Windows Server 2008	Улучшена масштабируемость и безопасность, асинхронные операции, больше операций чтения/записи, компоновка запроса
SMB 2.1	Windows 7, Windows Server 2008 R2	Поддержка больших MTU, поддержка BranchCache
SMB 3.0	Windows 8, Windows Server 2012	Улучшения для кластеров сервера, поддержка BranchCache v2, SMB по RDMA, улучшенная безопасность
SMB 3.02	Windows 8.1, Windows Server 2012 R2	Улучшенная производительность SMB по RDMA, дополнительные возможности масштабирования, поддержка "живой" миграции Hyper-V

ВНИМАНИЕ!

В SMB 3.0 и SMB 3.02 появилось много улучшений, касающихся производительности, особенно при использовании кластерных файловых серверов. Другим ключевым улучшением является сквозное шифрование данных SMB, что избавляет от необходимости использовать протокол IPSec, специализированные аппаратные средства или акселераторы глобальной сети (WAN) для защиты данных от прослушки. SMB-шифрование можно включить отдельно для каждого общего ресурса.

Просмотр существующих общих ресурсов

Для работы с общими ресурсами можно использовать и оснастку **Управление компьютером** и консоль **Диспетчер серверов** (Server Manager). Также можно просмотреть текущие общие ресурсы на компьютере с помощью команды `net share`, введенной в командной строке, или команды `get-smbshare`, введенной в приглашении PowerShell.

СОВЕТ

Командлет get-smbshare — один из многих командлетов, связанных с модулем smbshare. Чтобы получить список других доступных для работы с SMB-ресурсами командлетов, введите команду `get-command -module smbshare` в приглашении Windows PowerShell.

ПРИМЕЧАНИЕ

Управление компьютером, `net share` и `get-smbshare` отображают информацию о SMB-ресурсах, включая стандартные SMB-папки, скрытые SMB-папки (которые заканчиваются суффиксом $) и SMB-папки, предоставленные в общий доступ с использованием DFS (Distributed File System). **Диспетчер серверов** отображает информацию о стандартных SMB-папках, DFS-ресурсах и папках, предоставленных в общий доступ с использованием NFS. **Диспетчер серверов** не отображает скрытые SMB-папки.

В оснастке **Управление компьютером** можно просмотреть общие папки на локальном или удаленном компьютере так:

1. По умолчанию оснастка подключена к локальному компьютеру. Если нужно подключиться к удаленному компьютеру, щелкните по узлу **Управление компьютером** правой кнопкой мыши и выберите команду **Подключиться к другому компьютеру** (Connect to another computer). В появившемся окне выберите переключатель **другим компьютером** (Another Computer) и введите имя или IP-адрес компьютера, к которому нужно подключиться, а затем нажмите кнопку **OK**.
2. В дереве консоли перейдите к узлу **Служебные программы\Общие папки** (System Tools\Shared Folders), а затем выберите узел **Общие ресурсы** (Shares). Будет отображена информация о текущих общих ресурсах в системе (рис. 3.2).
3. Колонки узла **Общие ресурсы** (Shares) предоставляют следующую информацию:
   - **Общий ресурс** (Share name) — имя общей папки;
   - **Путь к папке** (Folder path complete) — полный путь к папке на локальной системе;
   - **Тип** (Type) — тип компьютеров, которые могут использовать этот ресурс. Обычно здесь выводится **Windows**, поскольку SMB-ресурсы предназначены для Windows-компьютеров;

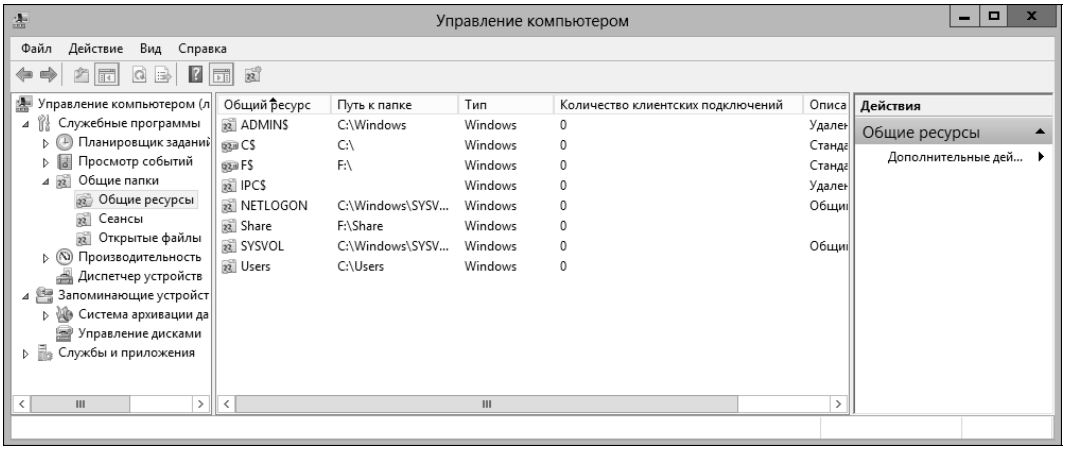


Рис. 3.2. Доступные общие ресурсы выводятся в узле **Общие ресурсы**

- **Количество клиентских подключений** (# Client Connections) — число клиентов, подключенных в данный момент к ресурсу;
- **Описание** (Description) — описание общего ресурса.

В диспетчере серверов можно просмотреть общие папки на локальном или удаленном компьютере с помощью следующих действий:

1. Выберите опцию **Файловые службы и службы хранилища** (File and Storage Services), а затем подузел **Общие ресурсы**.
2. Подузел **Общие ресурсы** предоставляет информацию о каждом ресурсе на каждом сервере, который был добавлен для управления (рис. 3.3).

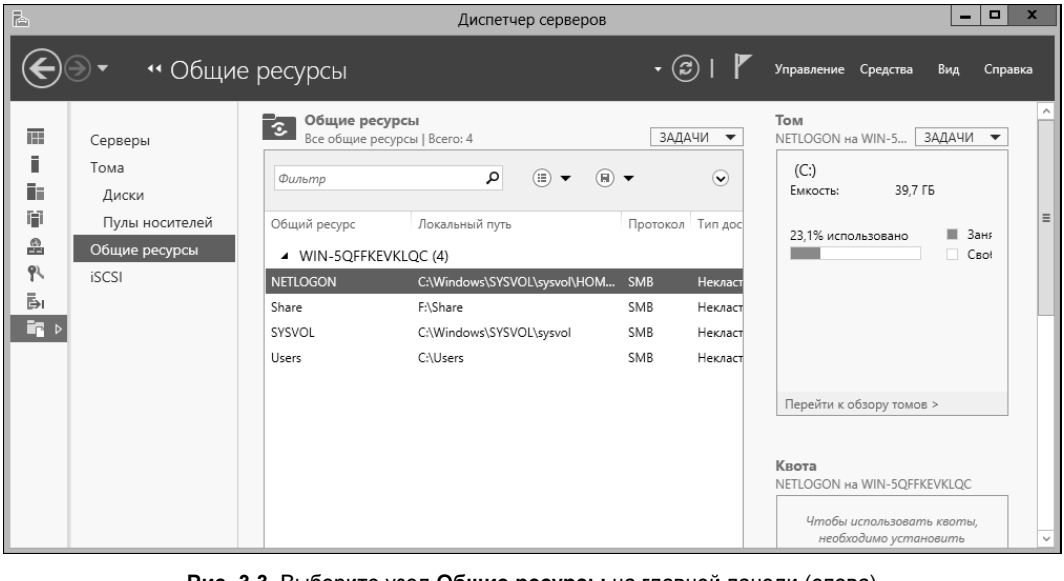


Рис. 3.3. Выберите узел **Общие ресурсы** на главной панели (слева) для просмотра всех доступных общих ресурсов

Колонки узла **Общие ресурсы** предоставляют следующую информацию:

- **Общий ресурс** (Share) — имя общей папки;
- **Локальный путь** (Local Path) — полный путь к папке на локальной системе;
- **Протокол** (Protocol) — используемый протокол, SMB или NFS;
- **Тип доступности** (Cluster Role) — если сервер, предоставляющий общий доступ к папке, часть кластера, здесь показан тип кластера. В противном случае, тип кластера — **Некластерный** (None).

3. Если щелкнуть по общему ресурсу на панели **Общие ресурсы**, на панели **Том** (Volume) (справа) будет отображена информация о соответствующем томе.

> ***Практический совет***
>
> Сетевая файловая система (NFS, Network File System) — протокол общего доступа к файлам, используемый в UNIX-системах, в том числе и на компьютерах под управлением Mac OS X. Как будет сказано в *разд. "Настройка общих ресурсов NFS" далее в этой главе*, можно включить поддержку NFS, установив роль **Сервер для NFS** (Server For NFS), как часть настройки файлового сервера.

Создание общих папок в оснастке *Управление компьютером*

Операционная система Windows Server 2012 R2 предлагает несколько способов предоставления общего доступа к папкам. Можно предоставить общий доступ к локальным папкам, используя Проводник, а общий доступ к локальным и удаленным папкам — в оснастке **Управление компьютером** или консоли **Диспетчер серверов**.

При создании общего ресурса в оснастке **Управление компьютером** можно настроить его разрешения общего доступа и автономные параметры. При создании общего ресурса в диспетчере серверов можно настроить все аспекты общего доступа, включая разрешения NTFS, шифрование данных, автономные параметры для кэширования и разрешения общего доступа. Обычно нужно создавать общие ресурсы на NTFS-тома, поскольку NTFS предлагает самое устойчивое решение.

В оснастке **Управление компьютером** для предоставления общего доступа к папке выполните следующие действия:

1. Если необходимо, подключитесь к удаленному компьютеру. В дереве консоли перейдите в узел **Служебные программы\Общие папки\Общие ресурсы**. Будут отображены текущие общие ресурсы в системе.
2. Щелкните правой кнопкой мыши по подузлу **Общие ресурсы** и выберите команду **Новый общий ресурс** (New Share). Будет запущен мастер создания общих ресурсов (Create A Shared Folder Wizard). Нажмите кнопку **Далее**.
3. В поле **Путь к папке** (Folder Path) введите локальный путь к папке, к которой предоставляется общий доступ. Путь должен быть точным, например, C:\EntData\Documents. Если не знаете точный полный путь, нажмите кнопку **Обзор** и используйте окно **Обзор папок** для поиска папки, к которой нужно предоставить совместный доступ. Затем нажмите кнопку **OK**, потом кнопку **Далее**.

Совет

Если путь, указанный в поле **Путь к папке**, не существует, мастер создаст эту папку автоматически. Нажмите кнопку **Да**, когда появится запрос на создание папки.

4. В поле **Общий ресурс** (Share Name) введите имя общего ресурса (рис. 3.4). Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальны для каждой системы.

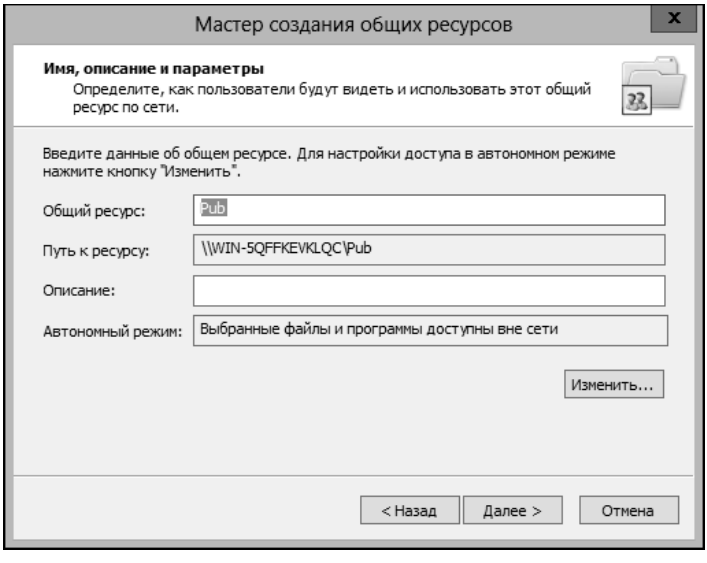


Рис. 3.4. Используйте мастер создания общих ресурсов для настройки параметров общего ресурса, включая имя, описание и параметры автономного режима

Совет

Если нужно скрыть общий ресурс от пользователей (это означает, что они не увидят ресурс, когда попытаются просмотреть список общих ресурсов в Проводнике или командной строке), введите знак доллара ($) в качестве последнего знака имени ресурса. Например, можно создать ресурс с именем PrivEngData$, который будет скрыт в Проводнике, в утилите `net view` и других подобных утилитах. Пользователи все еще могут подключиться к общему ресурсу и получить доступ к его данным, если им были предоставлены надлежащие разрешения доступа и они знают имя ресурса. Заметьте, что $ должен быть введен как часть имени общего ресурса, когда осуществляется подключение.

5. Можно ввести описание общего ресурса в поле **Описание** (Description). При просмотре общих ресурсов на определенном компьютере в оснастке **Управление компьютером** будет отображено описание ресурса.
6. По умолчанию общий ресурс настраивается так, что только файлы и программы, которые определяют пользователи, доступны в автономном режиме. Обычно эту опцию удобно использовать, поскольку она также позволяет пользователям получить преимущества новой функции **Всегда вне сети** (Always Offline). Если нужно использовать другие настройки автономного режима, нажмите кнопку **Изменить** и в окне **Настройка автономного режима** (Offline Settings) установите надлежащие параметры.

Можно установить следующие параметры.

- **Вне сети доступны только указанные пользователем файлы и программы** (Only the files and programs that users specify are available offline) — выберите эту опцию, если нужно, чтобы клиентские компьютеры кэшировали только файлы и программы, которые укажут пользователи для автономного использования. Дополнительно, если служба роли **BranchCache для сетевых файлов** (BranchCache For Network Files) установлена на файловом сервере, установите флажок **Включить BranchCache** (Enable BranchCache), чтобы включить кэширование файлов компьютерами филиалов, которые были загружены из общего ресурса. Эти файлы также будут безопасно предоставлены в общий доступ другим компьютерам филиала.
- **Файлы и программы в этой общей папке недоступны вне сети** (No files or programs from the shared folder are available offline) — выберите эту опцию, если не нужно, чтобы кэшированные копии файлов и программ из общего ресурса были доступны на клиентских компьютерах в автономном режиме.
- **Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы** (All files and programs that users open from the share are automatically available offline) — выберите эту опцию, если нужно, чтобы клиентские компьютеры автоматически кэшировали все файлы и программы, которые пользователи открывали из общего ресурса. Дополнительно можно установить флажок **Оптимизировать производительность** (Optimize for performance) для запуска программных файлов из локального кэша, а не с общего ресурса на сервере.

7. Нажмите кнопку **Далее** и установите основные разрешения для общего ресурса. Доступны следующие параметры.
   - **У всех пользователей доступ только для чтения** (All users have read-only access) — предоставляет пользователям право просмотра файлов и чтения данных. Пользователи не могут создавать, изменять или удалять файлы и папки.
   - **Администраторы имеют полный доступ, остальные — доступ только для чтения** (Administrators have full access; other users have read-only access) — предоставляет администраторам полный доступ к общему ресурсу. Полный доступ позволяет администраторам создавать, изменять и удалять файлы и папки. На NTFS-томе или разделе администраторы также могут изменять разрешения доступа и владельцев файлов и папок. Другие пользователи могут только просматривать файлы и читать данные. Они не могут создавать, изменять или удалять файлы и папки.
   - **Администраторы имеют полный доступ, остальные не имеют доступа** (Administrators have full access; other users have no access) — предоставляет администраторам полный доступ к ресурсу, остальным пользователям доступ запрещен.
   - **Настройка разрешений доступа** (Customize permissions) — позволяет настроить доступ определенным пользователям и группам, обычно это лучший способ. Установка разрешений доступа подробно рассматривается в *разд. "Управление разрешениями общих ресурсов" далее в этой главе*.

8. После нажатия кнопки **Готово** мастер создаст общий ресурс и отобразит состояние "Работа мастера создания общих ресурсов успешно завершена" (Sharing was successful). Если вместо этого будет отображена ошибка, запомните ее, примите меры по ее ликвидации и повторите попытку создания общего ресурса. Нажмите кнопку **Готово**.

Отдельные папки могут иметь несколько общих ресурсов. У каждого ресурса собственное имя и собственный набор прав доступа. Для создания дополнительных общих ресурсов на уже существующем общем ресурсе просто следуйте предыдущей процедуре с этими изменениями:

- на этапе 4 при вводе имени общего ресурса убедитесь, что используете отличающееся имя;
- на этапе 5 при добавлении описания для общего ресурса используйте описание, объясняющее, какой это ресурс, для чего он используется и чем отличается от других ресурсов в этой же папке.

Создание общих папок в диспетчере серверов

В диспетчере серверов можно предоставить общий доступ к папке так:

1. Подузел **Общие ресурсы** в узле **Файловые службы и службы хранилища** показывает существующие общие ресурсы на всех файловых серверах, добавленных для управления.
2. На панели **Общие ресурсы** выберите меню **Задачи**, а затем команду **Новый общий ресурс** (New share wizard). Будет запущен мастер создания общих ресурсов (New share). Выберите один из профилей общего ресурса и нажмите кнопку **Далее**. Мастер предлагает несколько профилей:
   - **Общий ресурс SMB — быстрый профиль** (SMB share — quick) — основной профиль для создания общего ресурса SMB, который позволяет настраивать свои параметры и разрешения;
   - **Общий ресурс SMB — дополнительные** (SMB share — advanced) — дополнительный профиль для создания SMB-ресурса, позволяющий настроить параметры, разрешения, свойства управления и NTFS-квоты (если применимо);
   - **Общий ресурс SMB — профиль приложений** (SMB share —applications) — пользовательский профиль для создания SMB-ресурсов с параметрами, подходящими для Hyper-V, определенных СУБД и других серверных приложений. Это почти то же самое, что и быстрый профиль, но не позволяет включать перечисление на основе доступа — ABE (Access-based Enumeration) и автономное кэширование.

Примечание

Если используется служба роли **Сервер для NFS** (Server For NFS), также будут доступны профили для создания NFS-ресурсов.

Практический совет

SMB 3.0 содержит расширения для серверных приложений. Эти расширения повышают производительность небольших случайных чтений и записей, которые характерны для сер-

верных приложений, например Microsoft SQL Server OLTP. В SMB 3.0 пакеты используют наибольший размер передаваемых данных (Maximum Transmission Unit, MTU), что повышает производительность больших передач данных, которые характерны для развертывания и копирования виртуальных жестких дисков по сети, резервного копирования базы данных и восстановления по сети, транзакций хранилища данных SQL-сервера по сети.

3. На странице **Укажите сервер и путь к этой общей папке** (Select the server and path for this share) выберите сервер и том, на которых нужно создать общую папку. Доступны только файловые серверы, добавленные для управления. Как только будете готовы продолжить, нажмите кнопку **Далее**. По умолчанию консоль **Диспетчер серверов** создает общий ресурс как новую папку в каталоге \Shares на выбранном томе. Чтобы переопределить это, выберите опцию **Ввести пользовательский путь** (Type a custom path) и затем введите нужный путь общего ресурса, например C:\Data, или нажмите кнопку **Обзор** и используйте окно **Обзор папок** для выбора пути общего ресурса.
4. На странице **Выбор имени общего ресурса** (Specify share name) введите имя общего ресурса (рис. 3.5). Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальными для каждой системы.
5. При необходимости введите описание общего ресурса в поле **Описание общего ресурса**. При просмотре списка общих ресурсов на определенном компьютере описание будет показано в оснастке **Управление компьютером**.

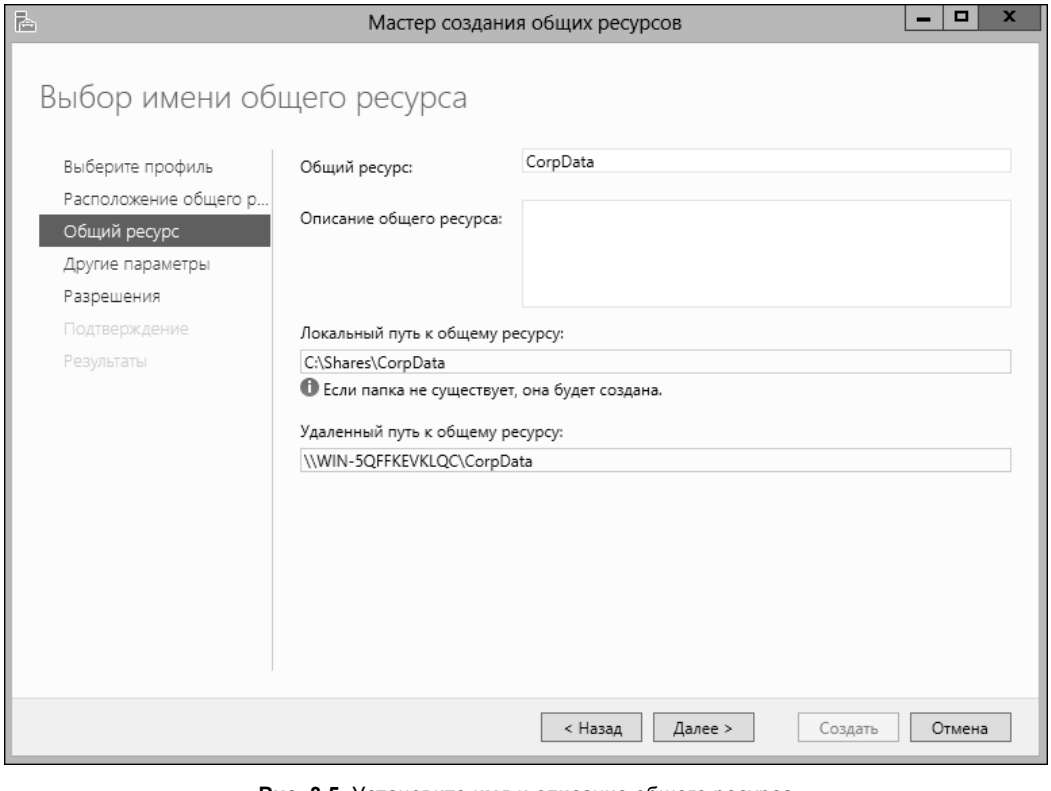


Рис. 3.5. Установите имя и описание общего ресурса

6. Запишите локальный и удаленный пути доступа к общему ресурсу. Эти пути установлены на основании расположения папки и указанного имени. Нажмите кнопку **Далее** для продолжения.
7. На странице **Настройка параметров общего ресурса** (Configure share settings) можно задать способ использования общего ресурса.
   - **Включить перечисление на основе доступа** (Enable access-based enumeration) — настраивает разрешения так, что при просмотре папки пользователями будут отображены только файлы и папки, которым как минимум предоставлено право чтения. Если у пользователя нет права чтения (или эквивалентного) для файла или папки внутри общей папки, этот файл или папка будут скрыты. (Эта опция недоступна, если создается SMB-ресурс, оптимизированный для приложений.)
   - **Разрешить кэширование общего ресурса** (Allow caching of share) — настраивает общий доступ для кэширования только файлов и программ, которые пользователи выберут для автономного использования. Хотя можно позже отредактировать свойства общего ресурса и изменить настройки автономного режима, обычно нужно выбрать эту опцию, поскольку она позволяет пользователям использовать преимущества новой функции **Всегда не в сети** (Always offline). Дополнительно, если служба роли **BranchCache для сетевых файлов** (BranchCache for network files) установлена на файловом сервере, отметьте флажок **Включить BranchCache** (Enable BranchCache) для общего файлового ресурса, чтобы включить кэширование файлов компьютерами филиалов, которые были загружены из общего ресурса. Эти файлы также будут безопасно предоставлены в общий доступ другим компьютерам филиала. (Эта опция недоступна при создании SMB-ресурса, оптимизированного для приложений.)
   - **Зашифровать доступ к данным** (Encrypt data access) — включает SMB-шифрование, которое защищает данные файла от прослушивания при их передаче по сети. Опция полезна в ненадежных сетях.
8. На странице **Определение разрешений для управления доступом** (Specify permissions to control access) назначены разрешения по умолчанию. По умолчанию специальной группе **Все** предоставляется полный доступ, также перечислены разрешения папки. Для изменения разрешений ресурса, папки (или обоих типов разрешений) нажмите кнопку **Настройка разрешений** (Customize permissions) и затем используйте окно **Дополнительные параметры безопасности** (Advanced security settings) для настройки требуемых полномочий. Установка разрешений общего доступа полностью описана в *разд. "Управление разрешениями общих ресурсов" далее в этой главе*. Установка разрешений папки полностью описана в *разд. "Разрешения файла и папки" главы 4*.
9. Если используется дополнительный профиль, можно установить свойства управления папки и затем нажать кнопку **Далее**. Эти свойства определяют назначение папки и тип данных, сохраненных в ней так, что политики управления данными, такие как правила классификации, могут использовать эти свойства.
10. Если используется расширенный профиль, дополнительно можно установить квоты папки по шаблону и затем нажать кнопку **Далее**. Можно выбрать только шаб-

лон квоты, который уже создан. Подробно этот процесс будет описан в *разд. "Управление шаблонами дисковых квот" главы 4*.

11. На странице **Подтверждение выбора** (Confirm Selections) просмотрите установленные параметры. После нажатия кнопки **Создать** мастер создаст общий ресурс, настроит его и установит разрешения. В случае успешного создания ресурса будет установлено состояние "Общий ресурс успешно создан" (The share was successfully created). Если вместо этого будет отображено сообщение об ошибке, запишите его и примите меры по исправлению ошибки перед повторением этой процедуры. Нажмите кнопку **Закрыть**.

Примечание

Если общий ресурс будет использоваться для Hyper-V, нужно включить ограниченное делегирование для удаленного управления Hyper-V.

Изменение параметров общей папки

После создания общего ресурса можно настроить множество базовых и расширенных параметров, включая перечисление на основе доступа, зашифрованный доступ к данным, автономное кэширование и свойства управления.

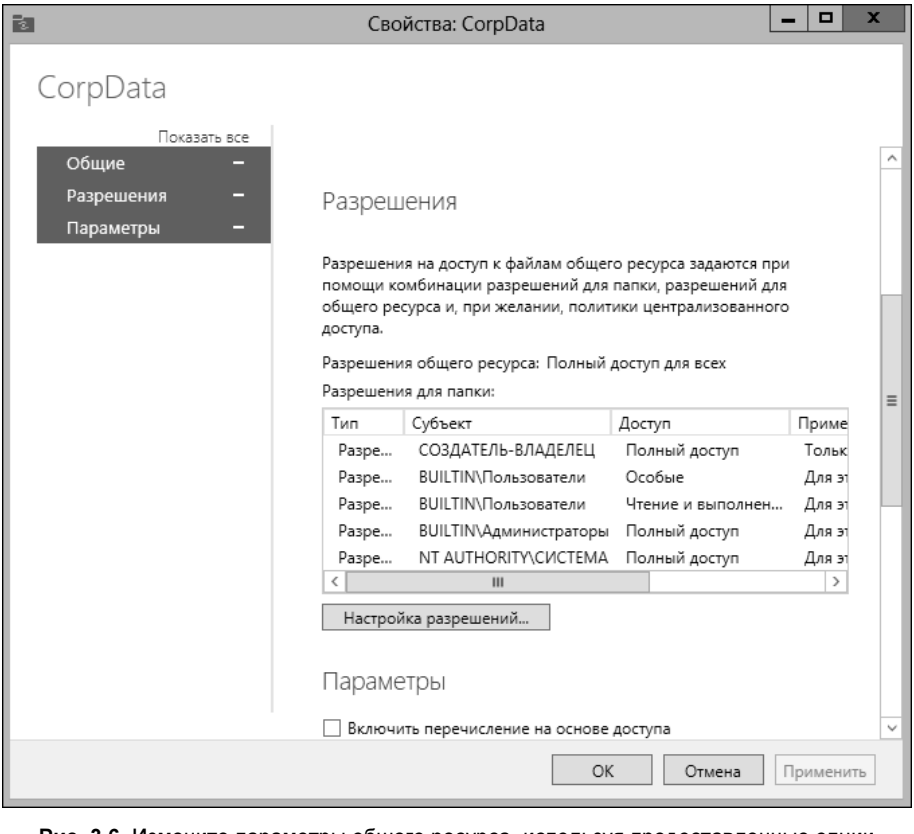


Рис. 3.6. Измените параметры общего ресурса, используя предоставленные опции

В диспетчере серверов можно модифицировать эти свойства так:

1. Подузел **Общие ресурсы** узла **Файловые службы и службы хранилища** (File And Storage Services) показывает существующие общие ресурсы для всех файловых серверов, добавленных для управления. Щелкните правой кнопкой мыши на общем ресурсе, с которым нужно работать, и выберите команду **Свойства**.
2. В окне **Свойства** (рис. 3.6) есть несколько панелей с параметрами. Можно развернуть панели по одной или выбрать опцию **Показать все** (Show All), чтобы просмотреть все панели за один раз.
3. Используйте предоставленные параметры для изменения настроек (при необходимости), а затем нажмите кнопку **OK**. Доступны те же параметры, что и при создании ресурса, они зависят от используемого профиля.

> ***Совет***
>
> Если создается ресурс для общего использования и общего доступа, можно опубликовать общий ресурс в Active Directory. Публикация ресурса в Active Directory делает доступ к нему проще для других пользователей. Однако эта опция не доступна в диспетчере серверов. Для публикации общего ресурса в Active Directory щелкните на ресурсе в оснастке **Управление компьютером** и выберите команду **Свойства**. На вкладке **Публикация** (Publish) установите флажок **Опубликовать этот общий ресурс в Active Directory** (Publish this share in Active Directory), добавьте описание и информацию о владельце, а затем нажмите кнопку **OK**.

Управление разрешениями общих ресурсов

Разрешения доступа устанавливают максимальные допустимые действия с общим ресурсом. По умолчанию при создании общего ресурса каждый пользователь с доступом к сети имеет право чтения содержимого общего ресурса. Это очень важное изменение с точки зрения безопасности — в предыдущих версиях Windows Server разрешением по умолчанию было **Полный доступ**.

Для томов NTFS и ReFS можно использовать разрешения файла и папки, а также разрешения общего доступа для ограничения доступа к ресурсу. Для томов FAT можно устанавливать только разрешения общего доступа.

Различные разрешения общего ресурса

Список разрешений от самого строгого до наименее строгого таков:

- **Нет доступа** (No Access) — ресурсу не предоставлены какие-либо разрешения;
- **Чтение** (Read) — с этим разрешением пользователи могут:
  - просматривать имена файлов и подпапок;
  - получать доступ к подпапкам общей папки;
  - читать данные и атрибуты файла;
  - запускать программы;

- **Изменение** (Change) — у пользователей есть разрешение **Чтение** и возможность выполнять следующие операции:
  - создавать файлы и подпапки;
  - изменять файлы;
  - изменять атрибуты файлов и подпапок;
  - удалять файлы и подпапки;
- **Полный доступ** (Full Control) — у пользователей есть разрешения **Чтение** и **Изменение**, а также дополнительные возможности на NTFS-томах:
  - изменение разрешений файлов и папок;
  - изменение владельца файлов и папок.

Можно назначить разрешения доступа пользователям и группам, в том числе даже неявным группам. Для более подробной информации о неявных группах см. главу 9 книги "Windows Server 2012 R2 Pocket Consultant: Essentials & Configuration".

Просмотр и настройка разрешений общего доступа

Просмотреть и настроить разрешения общего доступа можно в оснастке **Управление компьютером** или в консоли **Диспетчер серверов**. Для просмотра и настройки разрешений общего доступа в оснастке **Управление компьютером** выполните следующие действия:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс. В дереве консоли разверните узел **Служебные программы\Общие папки\Общие ресурсы**.
2. Щелкните правой кнопкой мыши на ресурсе, настройки которого нужно изменить, и выберите команду **Свойства**.
3. В окне **Свойства** перейдите на вкладку **Разрешения для общего ресурса** (Share Permissions), как показано на рис. 3.7. Теперь можно просмотреть список пользователей и групп, у которых есть доступ к этому ресурсу, а также тип предоставленного им доступа.
4. Пользователи или группы, которым уже предоставлен доступ к общему ресурсу, отображаются в списке **Группы или пользователи** (Group or user names). Можно удалить разрешения для этих пользователей и групп, выбрав учетную запись пользователя или группу, разрешения для которых нужно удалить, и затем нажав кнопку **Удалить** (Remove). Изменить разрешения для этих пользователей и групп можно так:
   - выберите пользователя или группу;
   - измените разрешения в списке **Разрешения** (Permissions).
5. Для добавления разрешений для другой учетной записи пользователя или группы нажмите кнопку **Добавить**. Будет открыто окно **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"** (рис. 3.8).

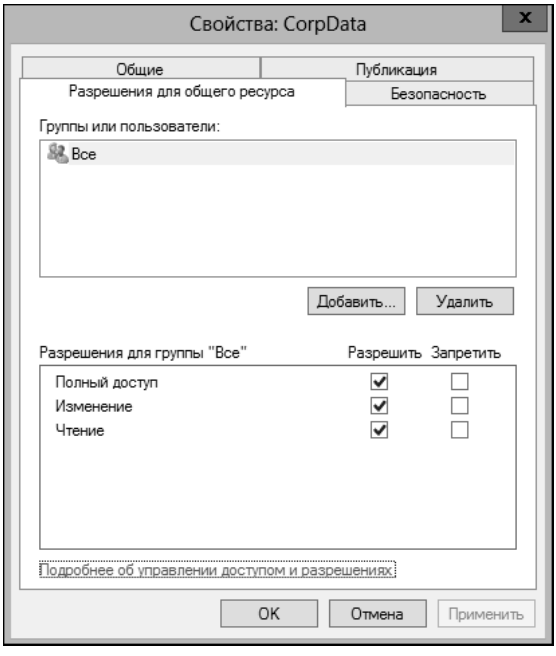


Рис. 3.7. Вкладка **Разрешения для общего ресурса** показывает, какие пользователи и группы обладают доступом к общему ресурсу и какой тип доступа им предоставлен

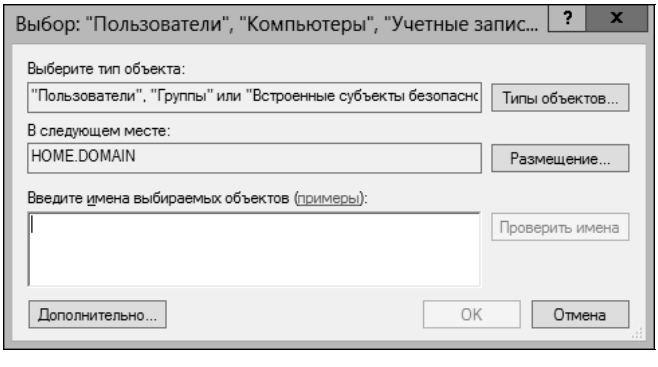


Рис. 3.8. Добавьте пользователей и группы в общий ресурс

6. Введите имя пользователя, компьютера или группы в текущем домене, а затем нажмите кнопку **Проверить имена** (Check Names). У этой процедуры может быть один из следующих результатов:
   - если найдено одно совпадение, диалоговое окно будет автоматически обновлено и эта запись будет подчеркнута;
   - если совпадения не найдены, введено неправильное имя или выбрано неправильное место (домен), измените имя и попробуйте еще раз или же нажмите кнопку **Размещение** (Locations) и выберите другое место;
   - если найдено несколько совпадений, выберите имя или имена, которые должны использоваться, и затем нажмите кнопку **OK**. Чтобы присвоить полномочия дру-

гим пользователям, компьютерам или группам, вводят точку с запятой (;) и затем повторяют этот процесс.

Примечание

Кнопка **Размещение** позволяет получить доступ к именам в других доменах. Нажмите эту кнопку, чтобы увидеть список доменов, к которым есть доступ. Благодаря транзитивным доверительным отношениям в Windows Server обычно можно получить доступ ко всем доменам в дереве доменов или лесу.

7. Нажмите кнопку **OK**. Пользователи и группы будут добавлены в список **Группы или пользователи** для ресурса.
8. Настройте разрешения доступа для каждого пользователя, компьютера и группы, выбрав имя учетной записи и затем разрешив или запретив разрешения доступа. Помните, что устанавливаются максимально допустимые разрешения для определенной учетной записи.
9. Нажмите кнопку **OK**. Как назначить дополнительные разрешения безопасности для NTFS, *см. в разд. "Разрешения файла и папки" главы 4*.

Внимание!

Имейте в виду, что можно выбрать противоположное разрешение, чтобы переопределить наследованное разрешение. Отметьте также, что обычно запрещающие разрешения перезаписывают разрешающие.

Для просмотра и настройки разрешений общего доступа в диспетчере серверов выполните следующие действия:

1. Подузел **Общие ресурсы** узла **Файловые службы и службы хранилища** показывает существующие общие ресурсы для всех файловых серверов, добавленных для управления.
2. Щелкните правой кнопкой мыши на общем ресурсе, с которым нужно работать, и выберите команду **Свойства**.
3. В окне **Свойства** выберите опцию **Разрешения** (Permissions) на панели слева. Теперь можно просмотреть, кому и какие разрешения предоставлены.
4. Для изменения разрешений общего доступа или папки (или обоих типов разрешений) нажмите кнопку **Настройка разрешений** (Customize Permissions). Далее выберите вкладку **Общая папка** (Share) в окне **Дополнительные параметры безопасности** (Advanced Security Settings), как показано на рис. 3.9.
5. Пользователи и группы, которым предоставлен доступ к ресурсу, выводятся в списке **Элементы разрешений** (Permission entries). Можно удалить разрешения для пользователей и групп, выделив пользователя или группу и нажав кнопку **Удалить**. Изменить разрешения для пользователя или группы можно так:
   - выберите пользователя или группу и щелкните по ссылке **Изменить**;
   - разрешите или запретите разрешения доступа в списке **Элементы разрешений** и нажмите кнопку **OK**.
6. Чтобы добавить разрешения для другого пользователя или группы, нажмите кнопку **Добавить**. Откроется окно **Элемент разрешения** (рис. 3.10).

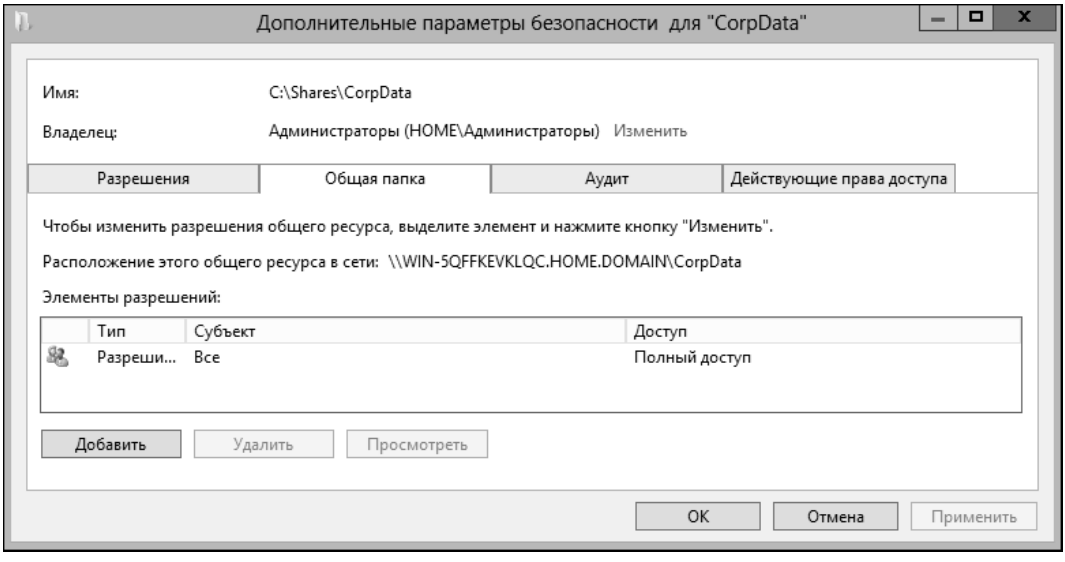


Рис. 3.9. Вкладка **Общая папка** показывает, какие пользователи и группы имеют доступ к ресурсу и какой тип доступа им назначен

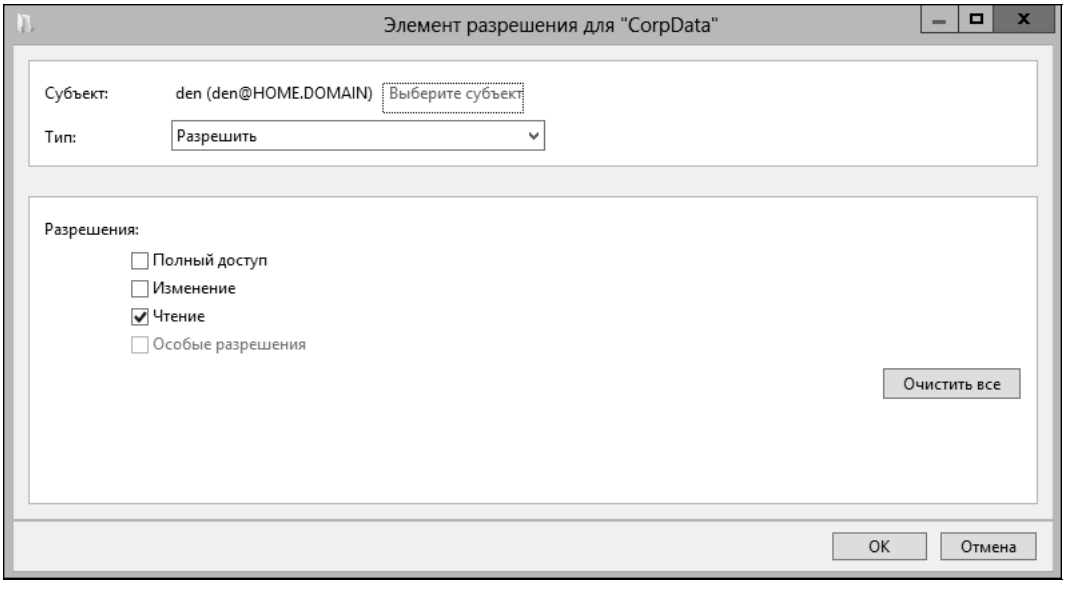


Рис. 3.10. Добавление разрешений для определенной учетной записи пользователя или группы

7. Щелкните по ссылке **Выберите субъект** (Select a principal) для отображения окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**. Введите имя пользователя или группы. Убедитесь, что ссылаетесь на учетное имя пользователя, а не на полное имя пользователя. За один раз можно ввести только одно имя.

8. Нажмите кнопку **Проверить имена**. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова либо нажмите кнопку **Размещение** для выбора нового размещения. Если будет найдено несколько совпадений, в окне **Найдено несколько имен** (Multiple Names Found) выберите имя, которое нужно использовать, и нажмите кнопку **OK**.
9. Нажмите кнопку **OK**. Пользователь или группа будут добавлены как **Субъект** (Principal), а окно **Элемент разрешения** будет обновлено, чтобы отобразить это.
10. Используйте список **Тип** (Type) для указания, что нужно сделать: разрешить или запретить разрешения. А затем выберите разрешения, которые нужно разрешить или запретить.
11. Нажмите кнопку **OK**, чтобы вернуться в окно **Дополнительные параметры безопасности** (Advanced Security Settings). Как назначить дополнительные разрешения безопасности для NTFS, *см. в разд. "Разрешения файла и папки" главы 4*.

Управление существующими общими ресурсами

Администратору часто приходится управлять общими папками. В этом разделе мы рассмотрим общие административные задачи по управлению общими ресурсами.

Особые общие ресурсы

При установке Windows Server операционная система автоматически создает особые общие ресурсы, которые так же известны, как *административные общие ресурсы* (administrative shares) или *скрытые общие ресурсы* (hidden shares). Эти ресурсы разработаны с целью сделать системное администрирование проще. Нельзя установить разрешения доступа на автоматически созданных особых общих ресурсах. ОС Windows Server назначает разрешения доступом (можно создать собственные скрытые ресурсы, добавив символ $ в качестве последнего символа общего ресурса).

Можно временно удалить особые общие ресурсы, если какие-то из них не нужны. Однако общие ресурсы будут созданы вновь при следующем запуске операционной системы. Для постоянного отключения административных общих ресурсов установите следующие значения реестра в 0:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer`;
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks`.

Какие особые ресурсы будут доступны, зависит от конфигурации системы. В табл. 3.2 перечислены специальные ресурсы и указано их использование.

Таблица 3.2. *Особые общие ресурсы, используемые в Windows Server 2012 R2*

Имя ресурса	Описание	Использование
ADMIN$	Общий ресурс используется во время удаленного администрирования системы. Предоставляет доступ к папке *%SystemRoot%* операционной системы	На рабочих станциях и серверах администраторы и операторы архива могут получить доступ к этому ресурсу. На контроллерах домена доступ к этому ресурсу могут получить также операторы сервера
FAX$	Поддерживает сетевой факс	Используется факс-клиентами при отправке факсов
IPC$	Поддерживает именованные каналы во время межпроцессного взаимодействия	Используется программами при осуществлении удаленного администрирования и при просмотре общих ресурсов
NETLOGON	Поддерживает службу Net Logon	Используется службой Net Logon при обработке запросов входа в домен. Каждый пользователь имеет доступ **Чтение** к этому ресурсу
PRINT$	Поддерживает общие ресурсы принтера, предоставляя доступ к драйверам принтеров	Используется общими принтерами. У каждого пользователя есть доступ **Чтение**. Полный доступ к этому ресурсу имеют администраторы, операторы сервера и операторы печати
SYSVOL	Поддерживает Active Directory	Используется для хранения данных и объектов для Active Directory
Буква_диска$	Общий ресурс, позволяющий администраторам подключаться к корневой папке диска. Эти общие ресурсы показаны как C$, D$, E$ и т. д.	К этим ресурсам на рабочих станциях и серверах имеют доступ администраторы, операторы архива. На контроллерах домена также доступ к ресурсам есть и у операторов сервера

Подключение к особым ресурсам

Имена особых ресурсов заканчиваются символом $. Хотя эти ресурсы не отображаются в Проводнике, администраторы и определенные операторы могут подключаться к ним (за исключением NETLOGON и SYSVOL). Если у текущей учетной записи есть надлежащие полномочия, можно подключиться непосредственно к особому ресурсу или к любому обычному ресурсу, указав UNC-путь в поле адреса Проводника. Базовый синтаксис следующий:

```
\\ИмяСервера\ИмяРесурса
```

Здесь *ИмяСервера* — DNS-имя или IP-адрес сервера, а *ИмяРесурса* — имя общего ресурса. В следующем примере производится подключение к ресурсу D$ на сервере CorpServer25:

```
\\CorpServer25\D$
```

Если есть необходимость, чтобы данный ресурс был представлен на этом компьютере как сетевой диск, или же нужно определить учетные данные, выполните следующие действия:

1. Откройте Проводник, по умолчанию будет открыт узел **Этот компьютер** (This PC). Если окно Проводника уже открыто и узел **Этот компьютер** не выбран на панели слева, выберите его.

2. Нажмите кнопку **Подключить сетевой диск** (Map Network Drive) на панели **Компьютер**. Откроется окно **Подключение сетевого диска** (Map Network Drive) (рис. 3.11).

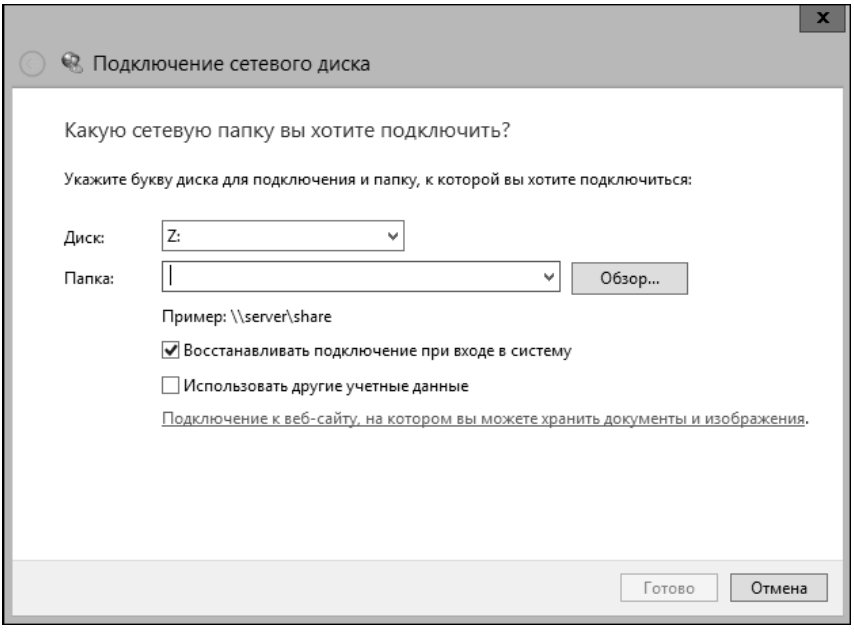


Рис. 3.11. Подключитесь к особым ресурсам, используя окно **Подключение сетевого диска**

3. В раскрывающемся списке **Диск** (Drive) выберите свободную букву диска. Она будет использоваться для доступа к особому ресурсу.
4. В поле **Папка** (Folder) введите UNC-путь к общему ресурсу. Например, для получения доступа к ресурсу C$ на сервере Twiddle введите \\TWIDDLE\C$.
5. Флажок **Восстанавливать подключение при входе в систему** (Reconnect At Sign-In) установлен автоматически, обеспечивая подключение сетевого диска при каждом входе пользователя в систему. Если нужно получить доступ к общему ресурсу только на время текущего сеанса, сбросьте этот флажок.
6. Если нужно подключиться к ресурсу с помощью других учетных данных, установите флажок **Использовать другие учетные данные** (Connect Using Different Credentials).
7. Нажмите кнопку **Готово**. При попытке подключения посредством других учетных данных введите имя пользователя и пароль. Введите имя пользователя в формате *домен\пользователь*, например Cpandl\Williams. Перед нажатием кнопки **OK** установите флажок **Запомнить учетные данные** (Remember My Credentials), если нужно сохранить учетные данные. В противном случае в будущем снова придется предоставить учетные данные.

После подключения к особому ресурсу с ним можно работать как с любым другим диском. Поскольку специальные ресурсы защищены, не нужно волноваться о доступе

обычных пользователей к этим ресурсам. При первом подключении к ресурсу система может попросить ввести имя пользователя и пароль. Предоставьте эту информацию.

Просмотр сессий пользователя и компьютера

Оснастку **Управление компьютером** можно использовать для отслеживания всех соединений к общим ресурсам на системе Windows Server 2012 R2. Независимо от того, кто подключился к ресурсу — пользователь или компьютер, Windows Server 2012 R2 выводит соединение в узле **Сеансы** (Sessions).

Для просмотра соединений к общим ресурсам введите команду `net session` в командной строке или команду `Get-SMBSession` в приглашении Windows PowerShell. Также можно выполнить следующие действия:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором был создан общий ресурс.
2. В дереве консоли разверните узел **Служебные программы\Общие папки**, а затем выберите узел **Сеансы** (Sessions). Теперь можно просмотреть соединения к общим ресурсам для пользователей и компьютеров.

Колонки в узле **Сессии** предоставляют следующую важную информацию о соединениях пользователей и компьютеров:

- **Пользователь** (User) — имя пользователя или компьютера, подключенного к общему ресурсу. Чтобы различать имена пользователей и компьютеров, к имени компьютера добавляется суффикс $;
- **Компьютер** (Computer) — имя используемого компьютера;
- **Тип** (Type) — тип используемого соединения;
- **Количество открытых файлов** (# Open Files) — число файлов, с которыми работает пользователь. Для более подробной информации (какие именно файлы открыты) перейдите в узел **Открытые файлы** (Open Files);
- **Время подсоединения** (Connected Time) — время, которое прошло с момента установки соединения;
- **Время простоя** (Idle Time) — время, прошедшее с момента последнего использования ресурса;
- **Гость** (Guest) — зарегистрирован ли пользователь как гость.

Как показано в следующем примере, вывод команды `Get-SMBSession` содержит идентификатор сессии, имя клиентского компьютера, имя пользователя клиента, число открытых файлов для каждого сеанса:

```
SessionId     ClientComputerName   ClientUserName   NumOpens
---------     ------------------   --------------   --------
601295421497  10.0.0.60            CPANDL\williams  2
```

Управление сеансами и общими ресурсами

Управление сеансами и общими ресурсами — общая административная задача. Перед завершением работы сервера или приложения, запущенного на сервере, нужно отклю-

чить пользователей от общих ресурсов. Также следует отключить пользователей, если планируется изменение прав доступа или удаление общего ресурса. Другая причина отключения пользователей — это избавление от блокировок файлов. Отключить пользователей от общего ресурса можно путем завершения соответствующих сеансов пользователя.

Завершение отдельных сеансов

Для отключения отдельных пользователей от общего ресурса введите команду `net session \\`*`ИмяКомпьютера`* `/delete` в командной строке или команду `Close-SMBSession -ComputerName` *`ИмяКомпьютера`* в приглашении Windows PowerShell. В обоих случаях, *`ИмяКомпьютера`* — это DNS-имя или IP-адрес компьютера, из которого исходит сеанс.

Также можно отключить пользователей, выполнив эти действия:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел **Служебные программы\Общие папки\Сеансы**.
3. Щелкните правой кнопкой мыши на сеансе пользователя и выберите команду **Закрыть сеанс** (Close Session).
4. Нажмите кнопку **Да** для подтверждения действия.

Закрытие всех сеансов

Для отключения всех пользователей от общих ресурсов выполните эти действия:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел **Служебные программы\Общие папки\Сеансы**.
3. Выберите команду **Отключить все сеансы** (Disconnect All Sessions), а затем нажмите кнопку **Да**, чтобы подтвердить действие.

> ***Примечание***
>
> Помните, что пользователи отключаются от общих ресурсов, но не от домена. Чтобы заставить пользователей выйти из домена, можно использовать только часы входа и групповую политику. Отключение пользователей не означает отключение их от сети. Они просто отключаются от общего ресурса.

Для отключения отдельных пользователей от общих ресурсов введите команду `net session \\`*`ИмяКомпьютера`* `/delete` в командной строке или команду `Close-SMBSession -ComputerName` *`ИмяКомпьютера`* в приглашении Windows PowerShell. В обоих случаях, *`ИмяКомпьютера`* — это DNS-имя или IP-адрес компьютера, из которого исходит сеанс.

Также можно использовать Windows PowerShell для отключения всех пользователей от общего ресурса. Основной момент здесь — убедиться, что вы закрываете только те сеансы, которые нужно закрыть. Рассмотрим следующий пример:

```
ForEach-Object ($Session in (Get-SMBSession)) {
Close-SMBSession -force}
```

В этом примере цикл `ForEach` получает все активные SMB-сеансы, а затем поочередно закрывает каждый открытый сеанс. Таким образом, если ввести этот пример в пригла-

шении Windows PowerShell, то будут отключены все пользователи от всех общих ресурсов.

Чтобы закрыть соединения только с определенным ресурсом, нужно создать такой цикл ForEach, который исследует только соединения для этого ресурса:

```
ForEach-Object ($Session in (Get-SMBShare CorpData |
Get-SMBSession)) {Close-SMBSession –force}
```

Этот пример использует цикл ForEach, получающий все активные SMB-сеансы для ресурса CorpData, и затем закрывает поочередно каждый сеанс. Если ввести этот пример в приглашении Windows PowerShell, будут отключены все пользователи от ресурса CorpDate.

Управление открытыми ресурсами

Каждый раз, когда пользователи соединяются с общими ресурсами, открытые ими файлы и объекты ресурсов отображаются в узле **Открытые файлы** (Open Files). Узел **Открытые файлы** показывает файлы, открытые пользователем, но в данный момент не редактируемые.

Получить доступ к узлу **Открытые файлы** (Open Files) можно так:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел **Служебные программы\Общие папки**, а затем — **Открытые файлы**. Узел **Открытые файлы** предоставляет следующую информацию об использовании ресурса:
   - **Открытый файл** (Open File) — путь к файлу (или папке), который пользователь открыл на локальной системе. Путь также может быть именованным каналом, например \PIPE\spools, который используется для спула принтера;
   - **Пользователь** (Accessed By) — имя пользователя, получающего доступ к файлу;
   - **Тип** (Type) — тип используемого сетевого соединения;
   - **Блокир.** (# Locks) — число блокировок ресурса;
   - **Режим открытия** (Open Mode) — режим доступа, используемый при открытии ресурса, например, **Чтение** (read), **Запись** (write) или **Чтение + Запись** (read + write).

Также можно использовать команду Get-SMBOpenFile для вывода списка открытых файлов. Для каждого файла данная команда выводит идентификатор файла, идентификатор сеанса, путь, относительный путь общего ресурса, имя клиентского компьютера, имя пользователя клиента:

```
FileId SessionId Path ShareRelativePath ClientComputerName ClientUserN
------ --------- ---- ----------------- ------------------ ------------
601295424973 601295421497 C:\PrimaryData\ 10.0.0.60 CPANDL\williams
601295425045 601295421577 C:\Windows\SYSVOL cpan... 10.0.0.60 CPANDL\CORPPC29$
```

Закрытие открытого файла

Чтобы закрыть открытый на общем ресурсе файл, выполните следующие действия:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел **Служебные программы\Общие папки\ Открытые файлы**.
3. Щелкните правой кнопкой мыши на файле, который нужно закрыть, а затем выберите команду **Закрыть открытый файл** (Close Open File).
4. Нажмите кнопку **Да** для подтверждения действия.

Также можно использовать команду `Close-SMBOpenFile` для закрытия открытого файла. При закрытии файла параметр `-FileID` используется для указания идентификатора файла, который нужно закрыть, например:

```
Close-SMBOpenFile –FileID 601295424973
```

Параметр `-Force` используется для принудительного закрытия файла. Однако, если файл был изменен пользователей, любые изменения в файле будут потеряны.

Закрытие всех открытых файлов

Для закрытия всех открытых файлов на общем ресурсе выполните эти действия:

1. В оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел **Служебные программы\Общие папки\ Открытые файлы**. Щелкните правой кнопкой мыши по узлу **Открытые файлы**.
3. Выберите команду **Отключить все открытые файлы** (Disconnect All Open Files) и нажмите кнопку **Да** для подтверждения действия.

Снова можно использовать Windows PowerShell для закрытия всех открытых на общем ресурсе файлов. Очень важно убедиться, что закрываются только необходимые файлы. Рассмотрим следующий пример:

```
ForEach-Object ($Session in (Get-SMBOpenFile)) {
Close-SMBOpenFile –force}
```

В этом примере цикл `ForEach` используется для получения всех открытых SMB-файлов, а затем закрывает каждый файл. При вводе этого примера в приглашение Windows PowerShell все открытые файлы на всех общих ресурсах будут закрыты.

Чтобы закрыть все файлы на определенном ресурсе, нужно создать цикл `ForEach`, который получает список открытых только на том ресурсе файлов, например:

```
ForEach-Object ($Session in (Get-SMBShare CorpData |
Get-SMBOpenFile)) {Close-SMBOpenFile –force}
```

Этот пример использует цикл `ForEach` для получения всех открытых SMB-файлов для ресурса CorpData и затем закрывает каждый открытый на этом ресурсе файл. Если ввести этот пример в приглашении Windows PowerShell, будут закрыты все открытые на CorpData файлы.

Прекращение общего доступа

Для прекращения доступа к папке:

1. Выполните одно из следующих действий:
   - в диспетчере серверов выберите общий ресурс в узле **Файловые службы и службы хранилища\Общие ресурсы**;
   - в оснастке **Управление компьютером** подключитесь к компьютеру, на котором создан общий ресурс, и перейдите в раздел **Общие ресурсы**.
2. Щелкните правой кнопкой мыши на ресурсе, который нужно удалить, и выберите команду **Прекратить общий доступ** (Stop Sharing), а затем нажмите кнопку **Да** для подтверждения действия.

> ***Осторожно!***
>
> Никогда не удаляйте папку, содержащую общие ресурсы без предварительного прекращения общего доступа к ресурсам. Если не получилось прекратить общий доступ, ОС Windows Server 2012 R2 попытается переустановить общие ресурсы при следующем запуске компьютера, и в результате вы получите ошибку, записанную в системный журнал событий.

Настройка общих ресурсов NFS

Как было упомянуто в *главе 1*, можно установить службу роли **Сервер для NFS** (Server for NFS) на файловый сервер. Служба предоставляет решение для совместного доступа к файлам на предприятии, где используются компьютеры под управлением Windows, Mac OS X и UNIX, позволяя пользователям передавать файлы между операционными системами Windows Server 2012 R2, Mac OS X и UNIX с использованием протокола NFS (Network File System).

Можно настроить совместный доступ по протоколу NFS к локальным папкам на NTFS-томах, используя Проводник. Также можно настроить общий NFS-доступ для локальных и удаленных папок на NTFS-томах посредством диспетчера серверов. В Проводнике для включения и настройки общего NFS-доступа выполните следующие действия:

1. Щелкните правой кнопкой мыши на общей папке и выберите команду **Свойства**. Будет показано окно **Свойства** для этой общей папки.
2. На вкладке **Совместный доступ NFS** (NFS Sharing) нажмите кнопку **Управление доступом NFS** (Manage NFS Sharing).
3. В окне **Дополнительные параметры общего доступа NFS** (NFS Advanced Sharing) установите флажок **Открыть общий доступ к этой папке** (Share this folder), как показано на рис. 3.12.
4. В поле **Общий ресурс** (Share name) введите имя общего ресурса. Это имя папки, к которой будут подключаться UNIX-пользователи. Имена NFS-ресурсов должны быть уникальными для каждой системы и могут быть такими же, как и для стандартного общего доступа к файлам.
5. По умолчанию используется кодировка ANSI для отображения информации каталога и имен файлов. Если UNIX-компьютеры используют другую кодировку, можно выбрать ее из раскрывающегося списка **Кодировка** (Encoding).

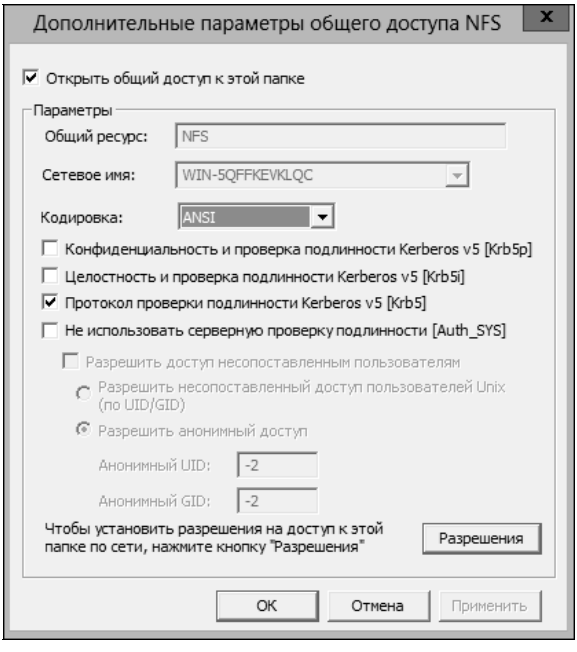


Рис. 3.12. Можно использовать общий доступ NFS для обмена файлами между Windows и UNIX-компьютерами

6. UNIX-компьютеры по умолчанию используют аутентификацию Kerberos v5. Обычно также нужно разрешить целостность Kerberos и стандартную аутентификацию Kerberos. Установите флажки напротив механизмов аутентификации, которые нужно использовать. Снимите флажки тех методов, которые не планируется использовать.
7. Общий ресурс может быть настроен без проверки аутентификации серверов. Если не нужна аутентификация сервера, установите флажок **Не использовать серверную проверку подлинности** (No server authentication) и затем выберите дополнительные параметры. Доступ несопоставленным пользователям может быть разрешен и включен. Если нужно разрешить анонимным пользователям доступ к NFS-ресурсам, установите переключатель **Разрешить анонимный доступ** (Allow anonymous access) и укажите UID анонимного пользователя и GID анонимной группы.
8. Для UNIX-компьютеров доступ настраивается на основе имен компьютеров (они также называются *именами хостов*). По умолчанию ни один из UNIX-компьютеров не имеет доступ к NFS-ресурсу. Если нужно предоставить права чтения или чтения/записи, нажмите кнопку **Разрешения**, установите разрешения в окне **Разрешения для общей папки NFS** (NFS Share Permissions) и нажмите кнопку **OK**. Можно настроить типы доступа **Нет доступа** (No Access), **Только для чтения** (Read-Only Access), **Чтение и запись** (Read/Write Access).
9. Нажмите кнопку **OK** дважды для закрытия открытых диалоговых окон и сохранения настроек.

В Проводнике можно отключить NFS-доступ так:

1. Щелкните правой кнопкой мыши на общей папке и выберите команду **Свойства**. Будет открыто одноименное окно для этой общей папки.
2. На вкладке **Совместный доступ NFS** нажмите кнопку **Управление доступом NFS**.
3. Сбросьте флажок **Открыть общий доступ к этой папке** и дважды нажмите кнопку **OK**.

В диспетчере серверов можно настроить NFS-разрешения как часть начальной конфигурации общего ресурса при его настройке. В подузле **Общие ресурсы** узла **Файловые службы и службы хранилища** можно создать NFS-ресурс так:

1. На панели **Общие ресурсы** выберите меню **Задачи**, а затем — **Новый общий ресурс** (New Share). Будет запущен мастер создания общих ресурсов (New Share Wizard). Выберите профиль **Общий ресурс NFS — быстрый профиль** или **Общий ресурс NFS — дополнительные** и нажмите кнопку **Далее**.
2. Укажите имя общего ресурса и расположение, как и в случае с SMB-ресурсом.
3. На странице **Задайте способы проверки подлинности** (Specify Authentication Methods) настройте аутентификацию Kerberos и аутентификацию без проверки подлинности сервера. Предоставленные опции подобны описанным ранее в этом разделе.
4. На странице **Назначение разрешений для общей папки** (Specify Share Permissions) настройте доступ для UNIX-узлов. Узлам (хостам) может быть предоставлен доступ на чтение или чтение/запись.
5. На странице **Определение разрешений для управления доступом** (Specify Permissions To Control Access) задайте NTFS-разрешения для общего ресурса.
6. На странице **Подтверждение выбора** (Confirm Selections) просмотрите все настройки. После нажатия кнопки **Создать** мастер создаст общий ресурс, настроит его и установит разрешения. В случае успешного создания ресурса будет отображено состояние "Общий ресурс успешно создан" (The share was successfully created). Если вместо этого появится ошибка, запишите ее и примите меры по ее исправлению перед повторением этой процедуры. Однако типичные ошибки касаются конфигурирования доступа хоста, и вероятно, не нужно повторять эту процедуру. Вместо этого следует изменить разрешения общего ресурса. Нажмите кнопку **Закрыть**.

Использование теневых копий

Если пользователи работают с общими папками, нужно рассмотреть создание теневых копий этих общих папок. *Теневые копии* (shadow copies) — резервные копии файлов данных, к которым пользователи могут получить доступ непосредственно в общих папках. Эти резервные копии могут сэкономить администраторам организации много времени, особенно если нужно получить потерянный, перезаписанный или поврежденный файл данных из резервной копии. Обычная процедура получения теневых копий — это использование Предыдущих версий (Previous Versions) или клиента Теневой копии. В Windows Server 2012 R2, благодаря дополнительной функции, можно вернуть весь несистемный том в предыдущее состояние.

Что такое теневые копии

Теневые копии можно создать только на NTFS-томах и использовать для автоматического создания резервных копий файлов. Функция настраивается отдельно для каждого тома. Например, на файловом сервере есть три NTFS-тома, на каждом из них существуют общие папки, и нужно настроить эту функцию отдельно для каждого тома.

Если включить эту функцию в ее конфигурации по умолчанию, теневые копии будут создаваться дважды в неделю (в понедельник и пятницу) в 7 часов утра и в 12 часов ночи. Необходимо как минимум 100 Мбайт свободного пространства для создания первой теневой копии на томе. Общий объем дискового пространства зависит от объема данных, хранящихся в общих папках тома. Можно ограничить общий размер дискового пространства, используемый для хранения теневых копий, установив максимальный размер резервных копий.

Просмотреть и установить параметры теневых копий можно на вкладке **Теневые копии** (Shadow Copies) окна **Свойства** диска. В Проводнике или оснастке **Управление компьютером** щелкните правой кнопкой мыши на значке диска и выберите команду **Свойства**, а затем перейдите на вкладку **Теневые копии**[1]. Панель **Выберите том** (Select A Volume) показывает следующее:

- **Том** (Volume) — метка NTFS-тома на выбранном диске;
- **Время следующего запуска** (Next Run Time) — состояние теневой копии. Может быть указано либо значение **Отключено** (Disabled), либо время следующего создания теневой копии;
- **Общие ресурсы** — число общих папок на томе;
- **Использовано** (Used) — сколько дискового пространства заняла теневая копия.

Отдельные теневые копии выбранного в данный момент тома отображаются на панели **Теневые копии выбранного тома** (Shadow Copies Of Selected Volume) с сортировкой по дате и времени.

Создание теневых копий

Чтобы создать теневую копию на NTFS-томе с общими папками, выполните следующие действия:

1. Откройте оснастку **Управление компьютером**. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства** (Storage), а затем — **Управление дисками**. Будут показаны тома, сконфигурированные на выбранном компьютере.

---

[1] Если данная вкладка не отображается, запустите оснастку **Управление компьютером**, щелкните правой кнопкой на узле **Общие папки**, выберите команду **Все задачи | Настроить теневые копии**. В появившемся окне выберите диск, для которого нужно включить теневые копии, и нажмите кнопку **Включить**. Повторите эту процедуру для каждого диска, где необходимо создать теневые копии. — *Прим. пер.*

3. Щелкните правой кнопкой мыши на узле **Управление дисками** и выберите команду меню **Все задачи | Настроить теневые копии** (All tasks | Configure shadow copies).
4. На вкладке **Теневые копии** (Shadow Copies) в списке **Выберите том** (Select a volume) выберите том, который нужно настроить.
5. Нажмите кнопку **Параметры** (Settings) для настройки максимального размера всех теневых копий для этого тома и изменения расписания по умолчанию. Нажмите кнопку **OK**.
6. После настройки параметров теневых копий тома нажмите кнопку **Включить** (Enable), если необходимо. Для подтверждения действия нажмите кнопку **Да**. Включение теневых копий создает первую теневую копию и устанавливает расписание для следующих теневых копий.

> ***Примечание***
>
> Если создается расписание путем настройки параметров теневой копии, теневое копирование будет автоматически включено после нажатия кнопки **OK** в окне **Параметры**. Однако первая теневая копия не будет создана до следующего запланированного раза. Если нужно создать теневую копию тома прямо сейчас, выберите том и нажмите кнопку **Создать** (Create).

Восстановление теневой копии

Пользователи, работающие на клиентских компьютерах, получают доступ к теневым копиям отдельных общих папок, используя функцию Предыдущие версии (Previous Versions) или Клиент теневых копий (Shadow Copy client). Лучший способ получить доступ к теневым копиям клиентского компьютера — следовать этим рекомендациям:

1. В Проводнике щелкните правой кнопкой мыши по общему ресурсу, доступ к предыдущим версиям файлов которого нужно получить, и выберите команду **Свойства**, а затем перейдите на вкладку **Предыдущие версии** (Previous Versions).
2. Выберите папку, с которой нужно работать. Для каждой папки выводится дата изменения. Нажмите кнопку, соответствующую действию, которое необходимо выполнить:
   - нажмите кнопку **Открыть** (Open), чтобы открыть теневую копию в Проводнике;
   - нажмите кнопку **Копировать** (Copy) для отображения окна **Копирование элементов** (Copy Items), которое используется для копирования теневой копии папки в выбранное расположение;
   - нажмите кнопку **Восстановить** (Restore), чтобы сделать откат общей папки в ее состояние на момент создания выбранной версии.

Восстановление предыдущего состояния всего тома

Операционная система Windows Server 2012 R2 содержит улучшение функции теневых копий, позволяющее возвращать целый том к состоянию, в котором он был на момент создания определенной теневой копии. Поскольку тома, содержащие файлы операци-

онной системы, не могут быть восстановлены, восстанавливаемый том не должен быть системным. Это же касается и томов на общем кластерном диске.

Чтобы восстановить предыдущее состояние тома, выполните эти действия:

1. Откройте оснастку **Управление компьютером**. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства** (Storage), а затем выберите узел **Управление дисками**, щелкните на нем правой кнопкой мыши и выберите команду меню **Все задачи | Настроить теневые копии** (All tasks | Configure shadow copies).
3. На вкладке **Теневые копии** (Shadow copies) выберите том из списка **Выберите том** (Select a volume).
4. Отдельные теневые копии выбранного в данный момент тома отображаются на панели **Теневые копии выбранного тома** (Shadow copies of selected volume) с сортировкой по дате и времени. Выберите нужную теневую копию и нажмите кнопку **Восстановить** (Revert).
5. Чтобы подтвердить это действие, установите флажок **Выполнить откат состояния этого тома** (Check here if you want to revert this volume) и нажмите кнопку **Откатить** (Revert now). Нажмите кнопку **OK**, чтобы закрыть окно **Теневые копии**.

Удаление теневых копий

Каждая контрольная точка может обслуживаться отдельно. Можно удалить отдельные теневые копии тома при необходимости. Эта операция восстановит дисковое пространство, занятое теневыми копиями.

Для удаления теневой копии действия:

1. Откройте оснастку **Управление компьютером**. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства**, а затем щелкните правой кнопкой мыши по узлу **Управление дисками**. Выберите команду меню **Все задачи | Настроить теневые копии**.
3. На вкладке **Теневые копии** выберите том из списка **Выберите том**.
4. Отдельные теневые копии выбранного в данный момент тома отображаются на панели **Теневые копии выбранного тома** с сортировкой по дате и времени. Выберите нужную теневую копию, которую следует удалить, и нажмите кнопку **Удалить**. Нажмите кнопку **Да** для подтверждения действия.

Отключение теневых копий

Если больше не планируется использование теневых копий тома, можно отключить функцию теневых копий. Отключение этой функции выключает расписание автоматических резервных копий и удаляет существующие теневые копии.

Для отключения теневых копий тома выполните следующие действия:

1. Откройте оснастку **Управление компьютером**. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства**, а затем щелкните правой кнопкой мыши по узлу **Управление дисками**. Выберите команду меню **Все задачи | Настроить теневые копии**.
3. На вкладке **Теневые копии** выберите том из списка **Выберите том**, а затем нажмите кнопку **Отключить** (Disable).
4. Для подтверждения действия нажмите кнопку **Да**. Нажмите кнопку **OK** для закрытия окна **Теневые копии**.

Подключение к сетевым дискам

Пользователи могут подключаться к сетевым дискам и к общим ресурсам, доступным в сети. Это соединение будет показано значком сетевого диска, к которому пользователи могут получить доступ как к любому другому диску в своих системах.

> ***Примечание***
>
> Когда пользователи подключаются к сетевым дискам, проверяются не только разрешения общих ресурсов, но и разрешения файлов и папок Windows Server 2012 R2. Различие в этих наборах разрешений — обычная причина отказа в доступе к определенному файлу или подпапке на сетевом диске.

Сопоставление сетевого диска

В ОС Windows Server 2012 R2 подключение к сетевому диску осуществляется путем его сопоставления буквы диска общему ресурсу с использованием команд `net use` и `New-PsDrive`. Синтаксис команды `net use` таков:

```
net use DeviceName \\ComputerName\ShareName
```

Здесь *`DeviceName`* определяет букву диска, можно указать символ `*` для использования следующей доступной буквы диска, а *`\\ComputerName\ShareName`* — UNC-путь к общему ресурсу, например:

```
net use g: \\ROMEO\DOCS
```

или

```
net use * \\ROMEO\DOCS
```

> ***Примечание***
>
> Чтобы убедиться, что сопоставленный диск будет доступен при следующем входе в систему, сделайте его постоянным, добавив опцию `/Persistent:Yes`.

Синтаксис для `New-PsDrive` следующий:

```
New-PsDrive -Name DriveLetter -Root \\ServerName\ShareName
-PsProvider FileSystem
```

Здесь *DriveLetter* — буква диска, а *ServerName* — DNS-имя или IP-адрес сервера, размещающего ресурс, *ShareName* — имя ресурса, например:

```
New-PsDrive –Name g –Root \\CorpServer21\CorpData
–PsProvider FileSystem
```

> ***Примечание***
>
> Чтобы убедиться, что сопоставленный диск доступен при каждом входе пользователя в систему, добавьте параметр `–Persist`.

Если клиентский компьютер работает под управлением Windows 8.1, можно сопоставить сетевые диски, выполнив следующие действия:

1. В Проводнике щелкните по крайнему левому переключателю в списке адресов, а затем выберите элемент **Компьютер** (Computer).
2. На панели **Компьютер** нажмите кнопку **Подключить сетевой диск** (Map Network Drive), а затем выберите команду **Подключить сетевой диск** (сначала нужно нажать на кнопку, а потом выбрать такую же команду из появившегося меню).
3. Используйте список **Диск** (Drive) для выбора свободной буквы диска, а затем нажмите кнопку **Обзор** справа от поля **Папка** (Folder). В окне **Обзор папок** разверните сетевые папки, чтобы можно выбрать имя рабочей группы или домена, с которым нужно работать.
4. Если развернуть имя компьютера в рабочей группе или домене, будет отображен список общих папок. Выберите необходимую общую папку и нажмите кнопку **OK**.
5. Установите флажок **Восстанавливать подключение при входе в систему** (Reconnect At Logon), если нужно, чтобы Windows автоматически подключалась к общей папке в начале каждого сеанса.
6. Нажмите кнопку **Готово**. Если у текущего пользователя нет надлежащих разрешений доступа для общего ресурса, выберите **Использовать другие учетные данные** (Connect Using Different Credentials) и затем нажмите кнопку **Готово**. После нажатия кнопки **Готово** можно будет ввести имя пользователя и пароль, которые будут использоваться для подключения к общей папке. Введите имя пользователя в формате *домен\пользователь*, например Cpandl\Williams. Перед нажатием кнопки **OK** отметьте флажок **Запомнить учетные данные** (Remember My Credentials), если нужно сохранить учетные данные. В противном случае в будущем вновь придется предоставить учетные данные.

Отключение сетевого диска

В Windows Sever 2012 R2 отключить сетевой диск можно с использованием команд `net use` и `Remove-PsDrive`. Синтаксис команды `net use` следующий:

```
net use DeviceName /delete
```

Здесь *DeviceName* указывает сетевой диск, который будет удален, например:

```
net use g: /delete
```

Синтаксис `Remove-PsDrive` таков:

```
Remove-PsDrive –Name DriveLetter
```

Здесь *DriveLetter* — буква диска, который будет удален, например:

```
Remove-PsDrive -Name g
```

> ***Примечание***
>
> Если с сетевым диском установлены соединения, вы можете принудительно удалить сетевой диск, используя параметр `-Force`.

Для отключения сетевого диска в Проводнике выполните следующие действия:

1. В Проводнике щелкните по крайнему левому переключателю в списке адресов, а затем выберите элемент **Компьютер**.
2. В группе **Сетевое расположение** (Network location) щелкните правой кнопкой мыши по значку сетевого диска и выберите команду **Отключить** (Disconnect).

Настройка общего ресурса синхронизации

Стандартный подход к совместному использованию файлов не подразумевает синхронизации общего доступа. Благодаря общим ресурсам синхронизации пользователи могут использовать Интернет или корпоративную сеть для синхронизации данных на их устройствах с папками, расположенных на корпоративных серверах. Синхронизированный общий доступ можно реализовать с помощью *рабочих папок* (Work Folders).

Рабочие папки — это функция, добавленная в серверы под управлением Windows Server 2012 R2. Рабочие папки используют клиент-серверную архитектуру. Клиент рабочих папок встроен по умолчанию в Windows 8.1, а также доступны клиенты для Windows 7, Apple iPad и других устройств.

Начинаем работать с рабочими папками

Разместить рабочие папки можно с помощью следующих процедур:

1. Добавьте роль **Рабочие папки** на серверы, на которых должны быть размещены синхронизируемые общие ресурсы.
2. Используйте групповую политику для включения обнаружения рабочих папок.
3. Создайте синхронизируемые общие ресурсы и, если необходимо, включите SMB-доступ к ним.
4. Настройте клиенты для доступа к рабочим папкам.

> ***Примечание***
>
> Групповая политика детально обсуждается в *главе 6*. Подробное описание включения обнаружения рабочих папок приводится в *разд. "Автоматическая настройка рабочих папок" главы 6*.

Рабочие папки используют удаленный веб-шлюз, сконфигурированный в качестве части внутрипроцессного веб-ядра IIS (IIS hostable web core). Когда пользователи получают доступ к общему ресурсу синхронизации (sync share) посредством URL, который предоставлен администратором и сконфигурирован в групповой политике, пользовательская папка создается как подпапка синхронизируемого общего ресурса и в ней

хранятся данные пользователя. Формат имени пользовательской папки устанавливается при создании общего ресурса синхронизации. Обычно папка называется с использованием только логина пользователя или же используется полное имя входа в формате *псевдоним@домен*. Выбор формата, прежде всего, зависит от требуемой совместимости. Использование полного имени устраняет потенциальные конфликты, когда у пользователей разных доменов есть одинаковые псевдонимы (логины), но зато такой формат несовместим с перенаправленными папками.

Для обеспечения совместимости с перенаправленными папками необходимо настроить рабочие папки так, чтобы использовались только псевдонимы (логины) пользователей. Однако у этого подхода есть огромный недостаток, с которым столкнутся администраторы корпоративных сетей с несколькими доменами. Ведь может возникнуть конфликт имен между одинаковыми именами пользователей в разных доменах. Несмотря на то, что автоматически настроенные полномочия предотвратят доступ пользователя amyh из домена cpandl.com к папке, созданной для пользователя amyh из домена pocket-consultant.com, конфликт имен приведет к тому, что если уже существует папка для пользователя amyh из домена cpandl.com, невозможно будет создать пользовательскую папку для пользователя amyh из домена pocket-consultant.com.

При использовании рабочих папок есть несколько важных параметров. Можно зашифровать файлы в рабочих папках на клиентских устройствах и гарантировать, что экраны на пользовательских устройствах будут блокироваться автоматически и потребуют ввода пароля для доступа. Шифрование реализовано посредством файловой системы EFS. EFS шифрует файлы ключом шифрования предприятия, а не ключом шифрования, сгенерированным клиентским устройством. Ключ шифрования предприятия определяется для идентификатора пользователя предприятия (который по умолчанию является SMTP-адресом пользователя). Наличие отдельного ключа шифрования предприятия, который отличается от стандартного клиентского ключа шифрования, позволяет гарантировать, что зашифрованные персональные файлы и зашифрованные рабочие файлы управляются отдельно.

Когда файлы зашифрованы, администраторы могут использовать выборочное стирание, чтобы удалить файлы предприятия с клиентского устройства. Выборочное стирание удаляет ключ шифрования предприятия и делает недоступными рабочие файлы. Выборочное стирание не затрагивает персональные файлы. Поскольку рабочие файлы остаются зашифрованными, нет никакой потребности удалять рабочие файлы с клиентского устройства. Однако можно запустить оптимизацию дисков для диска, на котором хранятся рабочие файлы. Во время этого процесса оптимизатор диска перезапишет секторы, в которых были сохранены рабочие файлы. Выборочное стирание работает только, если включена опция шифрования на рабочих папках.

Хотя шифрование — это один из способов защитить корпоративные данные, есть и другие способы. Например, можно настроить блокировку экранов клиентских устройств и требовать ввода пароля для доступа. Политика устанавливает:

- минимальная длина пароля — 6 символов;
- максимальное число попыток ввода пароля — 10;
- экран автоматически блокируется после 15 минут простоя.

Если применить использование этих настроек, любое устройство, не поддерживающее эти требования, не сможет получить доступ к рабочим папкам.

По умолчанию синхронизируемые общие ресурсы недоступны таким же способом, как стандартные файловые ресурсы. Именно поэтому для доступа к общим ресурсам синхронизации нужно использовать клиент рабочих папок. Если необходимо сделать синхронизируемые ресурсы доступными таким же способом, как и обычные общие ресурсы, нужно включить SMB-доступ. После того как SMB-доступ будет включен, пользователи смогут получить доступ к файлам, хранящимся в рабочих папках, как используя клиент рабочих папок, так и подключив ресурс как сетевой диск.

Когда пользователь вносит изменения в рабочие папки, изменения не сразу станут доступны другим пользователям, обращающимся к тем же рабочим папкам. Например, если пользователь удаляет файл из рабочей папки с помощью SMB, другие пользователи, получающие доступ к рабочей папке, будут видеть этот файл как доступный. Такое несоответствие возникает потому, что по умолчанию синхронизация происходит каждые 10 минут относительно изменений, вносимых по SMB.

Сервер синхронизации также использует клиента рабочих папок для периодической проверки изменений, внесенных пользователями по SMB. Интервал опроса по умолчанию составляет 5 минут. Когда сервер идентифицирует изменения, он передает изменения в следующий раз при синхронизации клиента. Именно поэтому для полного распространения изменений, внесенных по SMB, на самом деле требуется 15 минут.

> ***Практический совет***
>
> Для минимизации проблем при работе с рабочими папками нужно, чтобы пользователи знали, как работает технология. В частности, пользователи должны понимать, что изменения не сразу будут внесены и нужно немного подождать, пока изменения будут синхронизированы.

Администратор может определить, как часто сервер будет проверять наличие изменений, внесенных локально на сервере или по SMB посредством параметра — `MinimumChangeDetectionMins` командлета `Set-SyncServerSetting`. Однако поскольку сервер при проверке изменений проверяет каждый файл, хранящийся на общем ресурсе синхронизации, не нужно устанавливать очень маленький интервал. Сервер, который проверяет наличие изменений слишком часто, может стать перегруженным. Помните, обнаружение изменений требует много ресурсов, особенно когда в синхронизируемых ресурсах находится много файлов.

Если разворачиваются роли и компоненты, требующие полной версии роли IIS, внимательный администратор обнаружит, что эти роли и компоненты или сама функция рабочих папок не взаимодействуют. Также может возникнуть конфликт, поскольку полная версия IIS (роль **Веб-сервер**) использует порты 80 и 443 (для протоколов HTTP и HTTPS соответственно). Например, запуск рабочих папок и Windows Essentials Experience на одном и том же сервере требует специальной конфигурации. Как правило, нужно изменить порты, используемые Windows Essentials Experience, так, чтобы они не конфликтовали с портами, используемыми рабочими папками.

Чтобы включить детализированное журналирование рабочих папок, нужно включить и настроить настройку политики **Аудит доступа к объектам** (Audit Object Access) для GPO (Group Policy Object) сервера. Данная настройка находится в разделе **Конфигура-**

ция компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита (Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policies). После включения параметра **Аудит доступа к объектам** следует добавить контрольную запись для определенных папок, которые нужно контролировать. В Проводнике щелкните правой кнопкой мыши по папке, которую нужно контролировать, и выберите команду **Свойства**. В диалоговом окне **Свойства** перейдите на вкладку **Безопасность**, нажмите кнопку **Дополнительно** (Advanced). В диалоговом окне **Дополнительные параметры безопасности** (Advanced Security Settings) настройте контроль на вкладке **Аудит** (Auditing).

Создание общих ресурсов синхронизации и включение SMB-доступа

Общий ресурс синхронизации создается для идентификации локальной папки, которая будет синхронизироваться и будет доступна пользователем домена через клиента рабочих папок. Поскольку такие ресурсы сопоставляются с локальными путями на серверах синхронизации, мы рекомендуем создавать любые папки, которые нужно использовать, перед созданием общих ресурсов синхронизации. Это упростит выбор точных папок, с которыми пользователи будут работать. Для получения дополнительной информации по добавлению роли **Рабочие папки** и настройке рабочих папок посредством групповой политики обратитесь к *главе 6*.

Для создания синхронизируемого общего ресурса выполните следующие действия:

1. В диспетчере серверов выберите узел **Файловые службы и службы хранилища** (File And Storage Services), затем выберите **Рабочие папки** (Work Folders). На панели **Рабочие папки** выберите список **Задачи** (Tasks), а затем — команду **Новый общий ресурс синхронизации** (New Sync Share), чтобы открыть окно **Мастер создания общего ресурса синхронизации** (New Sync Share Wizard). Если будет отображена страница **Перед началом работы** (Before You Begin), нажмите кнопку **Далее** (Next).
2. На странице **Выбор сервера и пути** (Select The Server And Path), изображенной на рис. 3.13, выберите сервер, с которым нужно работать. Помните, что в этом окне отображаются только серверы, на которых установлена роль **Рабочие папки**.
3. При настройке общих ресурсов синхронизации есть несколько опций.
   - Добавление синхронизации к существующему общему ресурсу, для этого выберите опцию **Выбор по общему файловому ресурсу** (Select by file share), а затем выберите общий ресурс, который должен быть синхронизирован.
   - Добавление синхронизации к существующей общей папке, для этого выберите опцию **Введите локальный путь** (Enter a local path), затем нажмите кнопку **Обзор** (Browse) и в окне **Выбор папки** (Select Folder) выберите папку, к которой будет добавлена синхронизация.
   - Добавление синхронизации к новой папке, для этого выберите опцию **Введите локальный путь** (Enter a local path), а затем введите в предоставленное текстовое поле путь, который будет использоваться.

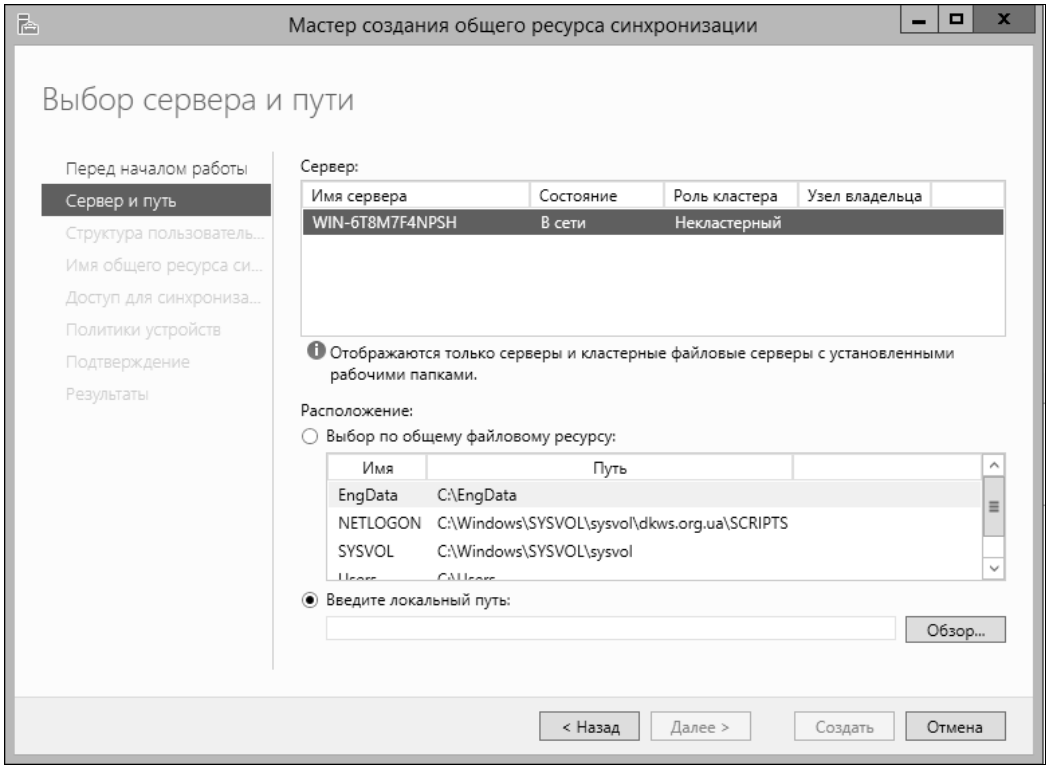


Рис. 3.13. Укажите, какой сервер и папку использовать

4. Когда будете готовы продолжить, нажмите кнопку **Далее**. Если была указана новая папка, мастер попросит подтвердить ее создание. Нажмите кнопку **OK** для создания папки и продолжения.
5. На странице **Укажите структуру для пользовательских папок** (Specify the structure for user folders) выберите формат именования папок для подпапок, в которых будут храниться пользовательские данные. Чтобы использовать только псевдоним пользователя, выберите переключатель **Псевдоним пользователя** (User Alias), а для использования полного имени выберите переключатель **Пользовательский адрес псевдоним@домен** (Useralias@domain).
6. По умолчанию все файлы и папки в выбранной пользовательской папке будут автоматически синхронизироваться. Если нужно, чтобы синхронизировалась только определенная папка, отметьте флажок **Синхронизировать только следующую папку** (Sync only the following folder), а затем введите имя папки, например Documents. Нажмите кнопку **Далее** для продолжения.
7. На странице **Введите имя общего ресурса синхронизации** (Enter the sync share name) введите имя ресурса и описание перед тем, как нажмете кнопку **Далее**.
8. На странице **Предоставление доступа к синхронизации для групп** (Grant sync access to groups), как показано на рис. 3.14, используйте предоставленные опции для указания пользователей и групп, у которых будет возможность получить доступ

к общему ресурсу синхронизации. Для добавления пользователя или группы нажмите кнопку **Добавить** (Add), а затем используйте окно **Выбор: "Пользователь" или "Группа"** (Select User Or Group) для указания пользователя или группы, у которых должен быть доступ к общему ресурсу синхронизации.

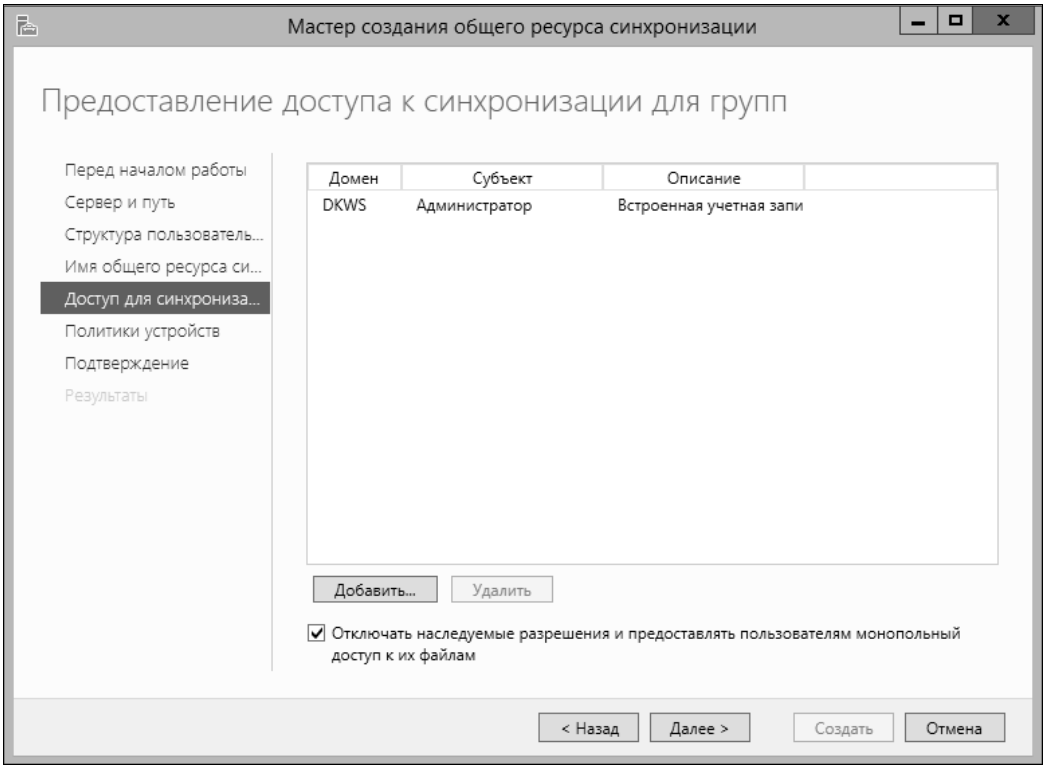


Рис. 3.14. Укажите пользователя или группу, у которых должен быть доступ к общему ресурсу синхронизации

Внимание!

Любым пользователям и группам, которым предоставлен доступ к базовой папке, разрешается создавать файлы и подпапки в базовой папке. В частности, **Создателю/Владельцу** (Creator/Owner) предоставляется полный доступ (Full Control). Пользователям и группам предоставляются разрешения **Список содержимого папки**, **Чтение данных**, **Создание папки** и некоторые другие. Локальной системе предоставляется полный доступ к базовой папке, подпапке и файлам. Администратору предоставляется доступ только для чтения для базовой папки.

9. По умолчанию наследование разрешения отключено и у пользователей есть эксклюзивный доступ к их пользовательским папкам. Поэтому доступ к файлу есть только у пользователя, создавшего этот файл на общем ресурсе. Если у базовой для общего ресурса папки есть полномочия, которые нужно применить к пользовательским папкам, нужно сбросить флажок **Отключить наследуемые разрешения** (Disable inherited permissions). Нажмите кнопку **Далее**.

10. На странице **Указать политики устройств** (Specify device policies) есть два параметра. Можно включить шифрование рабочих папок, установив флажок **Шифрование рабочих папок** (Encrypt work folders) для шифрования файлов в рабочих папках на клиентских устройствах. Параметр **Автоматически блокировать экран и требовать пароль** (Automatically lock screen and require a password) позволяет автоматически блокировать экран и требовать пароль на клиентских устройствах.
11. Нажмите **Далее** для продолжения, затем подтвердите сделанный выбор. Нажмите кнопку **Создать** (Create) для создания общего ресурса синхронизации. Если мастеру не получится создать общий ресурс синхронизации, будет отображена ошибка, а администратору нужно внести соответствующие корректирующие действия. Распространенная ошибка, которую допускают новички, заключается в том, что сервер содержит две роли — **Рабочие папки** (которые используют ограниченное вебядро) и **Веб-сервер**. Прежде чем использовать общие ресурсы синхронизации, нужно модифицировать порты, чтобы они не конфликтовали друг с другом, или же установить роль **Рабочие папки** на другой сервер, где нет роли **Веб-сервер**.
12. Если не был выбран существующий общий ресурс во время установки общего ресурса синхронизации, но необходимо включить для него SMB-доступ, откройте Проводник, в нем щелкните правой кнопкой мыши по папке, после чего выберите команду **Поделиться** (Share With), затем — **Отдельные люди** (Specific People). После этого настройте совместный доступ к файлам, как было ранее показано в этой главе.

Получение доступа к рабочим папкам на клиентах

Пользователи с учетной записью домена могут получить доступ к рабочим папкам из клиентского устройства через Интернет или по корпоративной сети. Для настройки доступа к рабочим папкам на клиентском устройстве нужно выполнить следующие действия:

1. Откройте Панель управления, выберите раздел **Система и безопасность** (System and Security), затем — **Рабочие папки** (Work Folders). На странице **Управление рабочими папками** (Manage Work Folders) щелкните по ссылке **Настроить рабочие папки** (Set Up Work Folders).
2. На странице **Введите свой рабочий адрес электронной почты** (Enter Your Work Email Address) введите адрес электронной почты пользователя, например amyh@cpandl.com, а затем нажмите кнопку **Далее**. Если устройство клиента подключено к домену, вводить учетные данные (имя пользователя и пароль) не нужно, в противном случае будут запрошены учетные данные пользователя. После того как они будут введены, можно сбросить флажок **Запомнить мои учетные данные** (Remember my credentials), чтобы запомнить учетные данные и не вводить их в будущем. Нажмите кнопку **OK** для продолжения.
3. На странице **Введение в рабочие папки** (Introducing Work Folders) обратите внимание, где будут храниться рабочие файлы пользователя. По умолчанию рабочие файлы хранятся в подпапке **Рабочие папки** профиля пользователя. Например, рабочие файлы для пользователя Amyh будут сохранены в каталоге *%SystemDrive%*

Users\Amyh\WorkFolders. Чтобы сохранить их в другом расположении, нажмите кнопку **Изменить** (Change) и используйте предоставленные опции для выбора нового расположения рабочих файлов. Когда будете готовы продолжить, нажмите кнопку **Далее**.

4. На странице **Политики безопасности** (Security Policies) просмотрите политики безопасности, которые будут применены, и установите флажок **Я принимаю эти политики** (I accept these policies on my pc). Продолжить не получится, если не включить этот флажок.
5. Выберите **Настроить рабочие папки** (Set Up Work Folders) для создания рабочих папок на клиентском устройстве.

После того как рабочие папки будут настроены на клиентском устройстве, пользователь может получить доступ к ним посредством Проводника. Когда пользователь открывает Проводник, по умолчанию активным является узел **Этот компьютер**. Поэтому для доступа к рабочим папкам пользователю нужно дважды щелкнуть по элементу **Рабочие папки** для просмотра рабочих файлов. Если Проводник уже открыт и узел **Этот компьютер** не выбран, нужно выбрать узел **Этот компьютер** на панели слева.

Изменения в рабочих файлах вызывают действия синхронизации. Если пользователь не изменяет локально никакие файлы на протяжении длительного периода времени, клиент подключается к серверу каждые 10 минут, чтобы определить, нет ли изменений для синхронизации.

ГЛАВА 4

Безопасность данных и аудит

Данные — основа любого предприятия, и очень важно убедиться, что они защищены. Хотя разрешения файла и папки защищают важные ресурсы, ограничивая доступ к ним, защита данных предприятия заключается не только в этом. Для надлежащей защиты данных предприятия администратор нуждается в твердом понимании управления объектами, владения, наследования и аудита. Также администратору нужно знать, как использовать квоты для ограничения объемов данных, которые могут храниться на сервере.

Управление объектами, владением и наследованием

Операционная система Windows Server 2012 R2 использует объектно-ориентированный подход для описания ресурсов и управления разрешениями. Объекты, которые описывают ресурсы, определены на NTFS-томе и в Active Directory. В случае с NTFS-томами можно установить разрешения для файлов и папок. В Active Directory можно установить разрешения для других типов объектов, например пользователей, компьютеров и групп. Эти разрешения могут использоваться для точного управления доступом.

Объекты и диспетчеры объектов

Независимо от того, где определены объекты, на NTFS-томе или в Active Directory, у каждого типа объектов есть диспетчер объектов и основные средства управления. Диспетчер объектов контролирует параметры и разрешения объекта. Основные средства управления — это средства для работы с объектом. Объекты, их диспетчеры и средства управления представлены в табл. 4.1.

Таблица 4.1. *Объекты Windows Server 2012 R2*

Тип объекта	Диспетчер объекта	Средство управления
Файлы и папки	NTFS	Проводник
Принтеры	Диспетчер очереди печати	Принтеры в Панели управления

Таблица 4.1 *(окончание)*

Тип объекта	Диспетчер объекта	Средство управления
Ключи реестра	Реестр Windows	Редактор реестра
Службы	Контроллеры служб	Набор инструментов настройки безопасности
Общие ресурсы	Служба **Сервер**	Проводник, оснастка **Управление компьютером**, Управление общими ресурсами и хранилищами

Владение объектом и передача владения

Важно понимать концепцию владения объектом. В Windows Server 2012 R2 владелец объекта не обязательно должен быть его создателем. Вместо этого, владелец объекта — это лицо, обладающее непосредственным контролем над объектом. Владельцы объектов могут назначить разрешения доступа и передать владение объектом другим пользователям.

Администратор может получить право владения объектов в сети. Это гарантирует, что для авторизированных администраторов не будет блокироваться доступ к файлам, папкам, принтерам и другим ресурсам. В большинстве случаев, как только администратор получит владение файлом, он не сможет вернуть его предыдущему владельцу. Это сделано специально, чтобы администраторы не могли получить доступ к файлам, а затем не пытались скрыть этот факт.

Способ назначения владения первоначально зависит от расположения создаваемого объекта. В большинстве случаев группа **Администраторы** является текущим владельцем, а фактический создатель указан как лицо, которое может получить владение объектом.

Передача владения может осуществляться несколькими способами:

- если группа **Администраторы** изначально назначена владельцем, создатель объекта получит владение при условии, что он сделает это раньше других;
- текущий владелец может предоставить разрешение **Смена владельца** (Take Ownership) другим пользователям, позволяя этим пользователям принять владение объектом;
- администратор может стать владельцем объекта при условии, что объект находится под его административным контролем.

Чтобы стать владельцем объекта, выполните эти действия:

1. Откройте программу управления объектом. Например, если нужно работать с файлами и папками, откройте Проводник.
2. Щелкните правой кнопкой мыши на объекте, владельцем которого нужно стать, а затем выберите команду **Свойства**. В окне **Свойства** перейдите на вкладку **Безопасность**.
3. На вкладке **Безопасность** нажмите кнопку **Дополнительно**, чтобы открыть окно **Дополнительные параметры безопасности** (Advanced Security Settings). В нем текущий владелец выводится под названием файла или папки.

4. Нажмите кнопку **Изменить**. Используйте окно **Выбор: "Пользователь", "Компьютер", "Учетная запись службы" или "Группа"** (Select Users, Computers, Service Accounts, or Groups) для выбора нового владельца.
5. Нажмите кнопку **OK** дважды, когда будете готовы.

> ***Совет***
>
> При изменении владельца папки также можно изменить и владельца для всех вложенных объектов (подпапок и файлов), установив флажок **Сменить владельца вложенных контейнеров и объектов** (Replace owner on subcontainers and objects). Эта опция работает не только с файлами, но и с другими объектами. Она изменяет владельца всех дочерних объектов.

Наследование объекта

Объекты определяются посредством родительско-дочерней структуры. Родительский объект — это объект верхнего уровня. Дочерний объект — это объект, определенный ниже родительского объекта в иерархии. Например, папка C:\ является родительской для папок C:\Data и C:\Backups. Любые папки, созданные в C:\Data и C:\Backups, являются дочерними для этих папок и "внуками" для C:\.

Дочерние объекты могут наследовать разрешения из родительских объектов. Фактически, все объекты Windows Server 2012 R2 по умолчанию созданы с включенным наследованием. Это означает, что дочерние объекты автоматически наследуют разрешения родительского объекта. Поэтому разрешения родительского объекта контролируют доступ к дочернему объекту. Если нужно сменить разрешения дочернего объекта, необходимо сделать следующее:

- отредактируйте разрешения родительского объекта;
- остановите наследование разрешений из родительского объекта и затем назначьте разрешения дочернему объекту;
- выберите противоположное разрешение, чтобы переопределить наследованное разрешение. Например, если родитель разрешает какое-то право, необходимо его запретить на дочернем объекте.

Для остановки наследования разрешений из родительского объекта выполните эти действия:

1. Откройте утилиту управления объектом. Например, если нужно работать с файлами и папками, откройте Проводник.
2. Щелкните правой кнопкой мыши на объекте, владельцем которого нужно стать, а затем выберите команду **Свойства**. В окне **Свойства** перейдите на вкладку **Безопасность**.
3. Нажмите кнопку **Дополнительно**, чтобы отобразить окно **Дополнительные параметры безопасности**.
4. На вкладке **Разрешения** нажмите кнопку **Изменить разрешения** для отображения редактируемой версии вкладки **Разрешения**.
5. На вкладке **Разрешения**, если наследование в данный момент включено, будет отображена кнопка **Отключение наследования** (Disable Inheritance). Нажмите ее.

6. Теперь можно преобразовать наследованные разрешения в явные разрешения объекта или удалить все наследованные разрешения и применить только те, которые явно установлены на папке или файле.

Помните, что если удалить наследованные разрешения и не назначить никаких других разрешений, то всем, кроме владельца, будет запрещен доступ к объекту. Это эффективно блокирует доступ каждого, кроме владельца файла или папки. Однако администраторы все еще имеют право захватить владение объектом, независимо от установленных разрешений. Таким образом, если доступ к файлу или папке блокирован для администратора, он может стать владельцем файла и затем получить неограниченный доступ.

Для включения наследования выполните следующие действия:

1. Откройте утилиту управления объектом, например Проводник.
2. Щелкните правой кнопкой мыши на объекте, владельцем которого нужно стать, а затем выберите команду **Свойства**. В окне **Свойства** перейдите на вкладку **Безопасность**.
3. Нажмите кнопку **Дополнительно**, чтобы отобразить окно **Дополнительные параметры безопасности**.
4. На вкладке **Разрешения** нажмите кнопку **Включение наследования**, а затем кнопку **OK**. Обратите внимание, что кнопка **Включение наследования** доступна, только если наследование в данный момент выключено.

Разрешения файла и папки

Разрешения NTFS всегда обрабатываются, как только происходит доступ к файлу. На томах NTFS и ReFS можно установить права доступа к файлам и папкам. Эти разрешения предоставляют или запрещают доступ к файлам и папкам. Поскольку ОС Windows Server 2012 R2 добавляет новые уровни безопасности, полномочия NTFS теперь охватывают следующие виды разрешений:

- базовые разрешения;
- разрешения на основе требований;
- особые разрешения.

Можно просмотреть NTFS-разрешения для папок и файлов так:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду **Свойства**. В окне **Свойства** перейдите на вкладку **Безопасность**.
2. В списке **Группы или пользователи** (Group or user names) выберите учетную запись пользователя, компьютера или группы, разрешения которой нужно просмотреть. Если разрешения недоступны, то они наследуются из родительского объекта.

Как было сказано ранее в этой главе, у общих папок есть и разрешения общего доступа, и разрешения NTFS. Можно просмотреть разрешения NTFS для общих папок так:

1. В диспетчере серверов перейдите в узел **Общие ресурсы**, показывающий существующие общие ресурсы серверов, добавленных для управления.

2. Щелкните правой кнопкой мыши на папке и выберите команду **Свойства**. Откроется окно **Свойства**.
3. Выберите **Разрешения** на панели слева, будут показаны разрешения общего ресурса и разрешения NTFS.
4. Чтобы получить больше информации, нажмите кнопку **Настройка разрешений** (Customize Permissions) для отображения окна **Дополнительные параметры безопасности**.

На файловых серверах под управлением Windows Server 2012 R2 также можно использовать централизованные политики доступа для точного определения специальных атрибутов, которые должны иметь пользователи и устройства для доступа к ресурсам.

Подробности о разрешениях файлов и папок

Базовые разрешения, которые можно назначить файлам и папкам, представлены в табл. 4.2. Разрешения файла включают **Полный доступ**, **Изменение**, **Чтение и выполнение**, **Чтение** и **Запись**. Разрешения папок включают **Полный доступ**, **Изменение**, **Чтение и выполнение**, **Список содержимого папки**, **Чтение** и **Запись**.

Таблица 4.2. *Разрешения файла и папки, используемые в Windows Server 2012 R2*

Разрешение	Значение для папок	Значение для файлов
Чтение (Read)	Разрешает обзор папок и просмотр списка файлов и подпапок	Разрешает просмотр или доступ к содержимому файла
Запись (Write)	Разрешает добавлять файлы и подпапки	Разрешает запись в файл
Чтение и выполнение (Read & Execute)	Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется файлами и папками	Разрешает просмотр и доступ к содержимому файла, а также запуск исполняемого файла (программы)
Список содержимого папки (List Folder Contents)	Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется только папками	—
Изменение (Modify)	Разрешает просмотр содержимого и создание файлов и подпапок; разрешает удаление папки	Разрешает чтение и запись данных в файл; разрешает удаление файла
Полный доступ (Full Control)	Разрешает просмотр содержимого, а также создание, изменение и удаление файлов и подпапок	Разрешает чтение и запись данных, а также изменение и удаление файла

При работе с разрешениями файла и папки нужно помнить о следующем:

- чтение — единственное право, необходимое для запуска сценариев. Право выполнения здесь не имеет значения;
- для доступа к ярлыку и связанному объекту требуется разрешение на чтение;
- разрешение на запись в файл при отсутствии разрешения на удаление файла все еще позволяет пользователю удалять содержимое файла;

- если пользователь получит разрешение **Полный доступ** к папке, он может удалять любые файлы в такой папке, независимо от разрешений на доступ к этим файлам.

Базовые разрешения созданы при помощи объединения в логические группы особых разрешений. В табл. 4.3 представлены особые разрешения, предусмотренные для создания базовых разрешений для файлов. Используя дополнительные параметры безопасности, можно индивидуально назначать эти особые разрешения, если необходимо. При изучении особых разрешений для файлов нужно учитывать следующее:

- по умолчанию, если пользователю явно не предоставлены права доступа, то доступ к файлу для него закрыт;
- действия, которые пользователи могут выполнять, основываются на сумме всех назначенных пользователю разрешений и разрешений всех групп, членом которых он является. Например, если пользователь GeorgeJ имеет доступ на чтение и в то же время входит в группу Techies, у которой есть доступ на изменение, то в результате у пользователя GeorgeJ тоже появляется доступ на изменение. Если группу Techies включить в группу **Администраторы** с полным доступом, то GeorgeJ будет полностью контролировать файл.

Таблица 4.3. *Особые разрешения для файлов*

Особые разрешения	**Базовые разрешения**				
	Полный доступ	**Изменение**	**Чтение и выполнение**	**Чтение**	**Запись**
Траверс папок/выполнение файлов (Traverse Folder/ Execute File)	Да	Да	Да		
Содержание папки/чтение данных (List Folder/Read Data)	Да	Да	Да	Да	
Чтение атрибутов (Read Attributes)	Да	Да	Да	Да	
Чтение дополнительных атрибутов (Read Extended Attributes)	Да	Да	Да	Да	
Создание файлов/запись данных (Create Files/Write Data)	Да	Да			Да
Создание папок/дозапись данных (Create Folders/Append Data)	Да	Да			Да
Запись атрибутов (Write Attributes)	Да	Да			Да
Запись дополнительных атрибутов (Write Extended Attributes)	Да	Да			Да
Удаление подпапок и файлов (Delete Subfolders And Files)	Да				

Таблица 4.3 *(окончание)*

Особые разрешения	Базовые разрешения				
	Полный доступ	**Изменение**	**Чтение и выполнение**	**Чтение**	**Запись**
Удаление (Delete)	Да	Да			
Чтение разрешений (Read Permissions)	Да	Да	Да	Да	Да
Смена разрешений (Change Permissions)	Да				
Смена владельца (Take Ownership)	Да				

В табл. 4.4 перечислены особые разрешения, используемые для создания базовых разрешений для папок. Здесь необходимо учитывать, что при создании файлов и папок они наследуют некоторые разрешения из родительских объектов. Эти разрешения показываются как разрешения по умолчанию.

Таблица 4.4. *Особые разрешения для папок*

Особые разрешения	Базовые разрешения					
	Полный доступ	**Изменение**	**Чтение и выполнение**	**Список содержимого папки**	**Чтение**	**Запись**
Траверс папок/ выполнение файлов (Traverse Folder/ Execute File)	Да	Да	Да	Да		
Содержание папки/ чтение данных (List Folder/Read Data)	Да	Да	Да	Да	Да	
Чтение атрибутов (Read Attributes)	Да	Да	Да	Да	Да	
Чтение дополнительных атрибутов (Read Extended Attributes)	Да	Да	Да	Да	Да	
Создание файлов/ запись данных (Create Files/Write Data)	Да	Да				Да
Создание папок/ дозапись данных (Create Folders/Append Data)	Да	Да				Да
Запись атрибутов (Write Attributes)	Да	Да				Да
Запись дополнительных атрибутов (Write Extended Attributes)	Да	Да				Да

Таблица 4.4 *(окончание)*

Особые разрешения	Базовые разрешения					
	Полный доступ	**Изменение**	**Чтение и выполнение**	**Список содержимого папки**	**Чтение**	**Запись**
Удаление подпапок и файлов (Delete Subfolders And Files)	Да					
Удаление (Delete)	Да	Да				
Чтение разрешений (Read Permissions)	Да	Да	Да		Да	Да
Смена разрешений (Change Permissions)	Да					
Смена владельца (Take Ownership)	Да					

Установка базовых разрешений файла и папки

Чтобы установить базовые NTFS-разрешения для файлов и папок, выполните следующие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду **Свойства**. В окне **Свойства** перейдите на вкладку **Безопасность**.
2. Нажмите кнопку **Изменить** для отображения редактируемой версии вкладки **Безопасность** (рис. 4.1).
3. Пользователи или группы, которые уже имеют доступ к файлу или папке, выводятся в списке **Группы или пользователи**. Можно изменить разрешения для этих пользователей или групп так:
   - выберите пользователей или группы, которые нужно изменить;
   - разрешите или запретите разрешения в списке **Разрешения для**.

   Совет

   Наследованные разрешения отображаются серым (недоступны). Если нужно переопределить наследованные разрешения, выберите противоположные разрешения.
4. Для установки разрешений доступа для дополнительных пользователей, компьютеров или групп нажмите кнопку **Добавить**. Появится окно **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.
5. Введите имя пользователя, компьютера или группы в текущем домене и нажмите кнопку **Проверить имена**. Далее возможен один из следующих сценариев:
   - если найдено одно совпадение, диалоговое окно будет обновлено и найденная запись будет подчеркнута;
   - если совпадения не были найдены, введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку **Размещение** для выбора нового размещения;

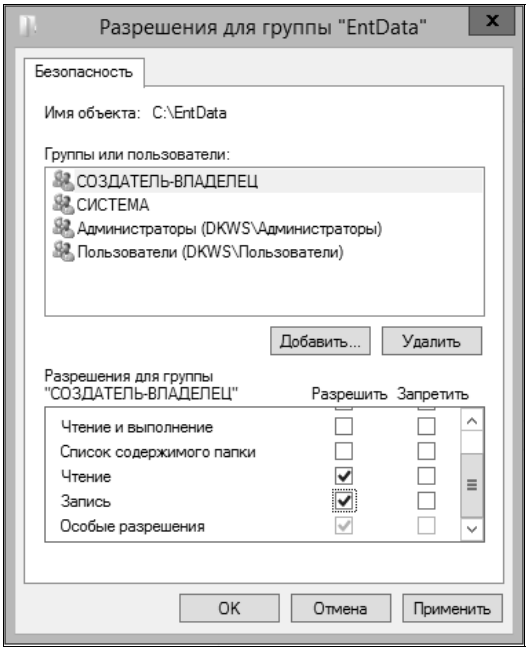


Рис. 4.1. Настройка базовых разрешений для файла или папки на вкладке **Безопасность**

- если найдено несколько совпадений, выберите имя или имена, которые нужно использовать, и нажмите кнопку **OK**. Для добавления нескольких пользователей, компьютеров или групп введите точку с запятой (;) и затем повторите этот шаг.

Совет

Кнопка **Размещение** позволяет получить доступ к именам учетных записей в других доменах. Нажмите кнопку **Размещение**, чтобы увидеть список из текущего домена, доверенных доменов и других ресурсов, к которым есть доступ. Благодаря транзитивным доверияем в Windows Server 2012 R2 обычно можно получить доступ ко всем доменам в доменном дереве или лесу.

6. В списке **Группы или пользователи** выберите учетную запись пользователя, компьютера, группы, которую нужно настроить, и установите разрешения в списке **Разрешения для**. Повторите этот процесс для других пользователей, компьютеров или групп.
7. Нажмите кнопку **OK**.

Поскольку у общих папок также есть NTFS-разрешения, может понадобиться установить базовые NTFS-разрешения с использованием диспетчера серверов. Чтобы сделать это, выполните следующие действия:

1. В консоли **Диспетчер серверов** выберите **Файловые службы и службы хранилища**, выберите сервер, с которым вы хотите работать, а затем — подузел **Общие ресурсы**.
2. Щелкните правой кнопкой мыши на папке и выберите команду **Свойства**. Откроется одноименное окно.

3. Выберите на левой панели элемент **Разрешения**, будут отображены текущие разрешения общего ресурса и NTFS-разрешения на основной панели.
4. Нажмите кнопку **Настройка разрешения** для открытия окна **Дополнительные параметры безопасности** с активной вкладкой **Разрешения**.
5. Пользователи и группы, уже имеющие доступ к файлу или папке, перечислены в списке **Элементы разрешений** (Permission entries). Используйте предоставленные параметры для просмотра, редактирования, добавления или удаления разрешений для пользователей или групп.

Установка особых разрешений для файлов и папок

Для установки особых NTFS-разрешений для файлов и папок выполните следующие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду **Свойства**.
2. В окне **Свойства** перейдите на вкладку **Безопасность** и нажмите кнопку **Дополнительно** для отображения окна **Дополнительные параметры безопасности**. Перед изменением разрешений нужно нажать кнопку **Изменить разрешения**. Разрешения будут представлены в том порядке, в котором они находятся на вкладке **Безопасность** (рис. 4.2). Основные отличия — отображаются индивидуальные наборы разрешений, указано, наследованы ли разрешения и от кого, а также перечислены ресурсы, к которым применены разрешения.

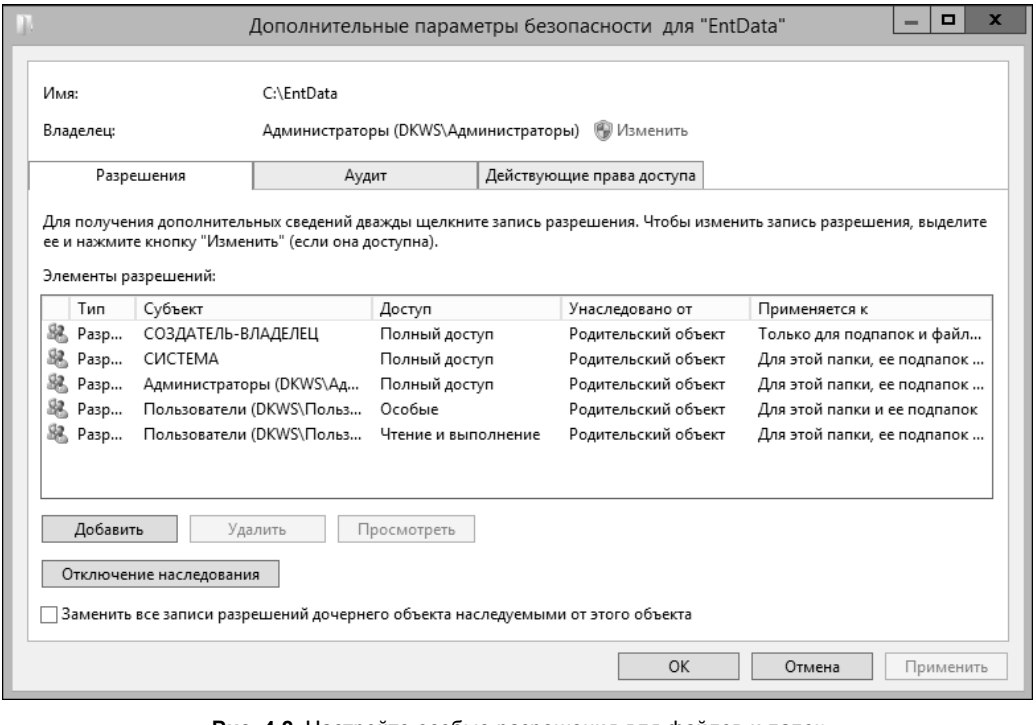


Рис. 4.2. Настройте особые разрешения для файлов и папок

3. Если для пользователя или группы уже установлены разрешения для папки или файла (и эти разрешения не наследуются), можно изменить специальные разрешения, выбрав пользователя или группу и нажав кнопку **Изменить**. Пропустите шаги 4–7 и следуйте оставшимся рекомендациям в этой процедуре.
4. Чтобы добавить особые разрешения для пользователя или группы, нажмите кнопку **Добавить** для отображения окна **Элемент разрешения** (Permission Entry). Щелкните по ссылке **Выберите субъект** (Select a principal) для отображения окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.
5. Введите имя учетной записи пользователя или группы. Убедитесь, что ссылаетесь на имя учетной записи, а не на полное имя пользователя. Только одно имя может быть введено за один раз.
6. Нажмите кнопку **Проверить имена**. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку **Размещение** для выбора нового размещения. Если найдено несколько совпадений, в окне **Найдено несколько имен** (Multiple Names Found) выберите имя, которое нужно использовать, и нажмите кнопку **OK**.
7. Нажмите кнопку **OK**. Пользователь или группа будут добавлены как **Субъект** (Principal), и окно **Элемент разрешения** обновится для отображения этого факта.
8. По умолчанию отображаются только базовые разрешения. Щелкните по ссылке **Отображение дополнительных разрешений** (Show advanced permissions) для отображения особых разрешений (рис. 4.3).
9. Используйте раскрывающийся список **Тип**, чтобы указать, что нужно сделать: разрешить или запретить особые разрешения. А затем выберите особые разрешения, которые нужно разрешить или запретить. Если разрешение недоступно, значит, оно наследуется от родительской папки.

> ***Примечание***
>
> Можно разрешать и запрещать любые особые разрешения выборочно. Поэтому, если нужно и разрешить, и запретить особые разрешения, необходимо настроить разрешение, а потом повторить эту процедуру, начиная с шага 1, для запрещения.

10. Если доступен раскрывающийся список **Применяется к** (Applies to), выберите надлежащую опцию. Доступны следующие опции:
    - **Только для этой папки** (This folder only) — разрешения будут применены только для выбранной в данный момент папки;
    - **Для этой папки, ее подпапок и файлов** (This folder, subfolders and files) — разрешения применяются к этой папке, ко всем ее подпапкам и ко всем файлам в этих папках;
    - **Для этой папки и ее подпапок** (This folder and subfolders) — разрешения применяются к этой папке и к любой подпапке этой папки. Они не применяются к файлам в этих папках;

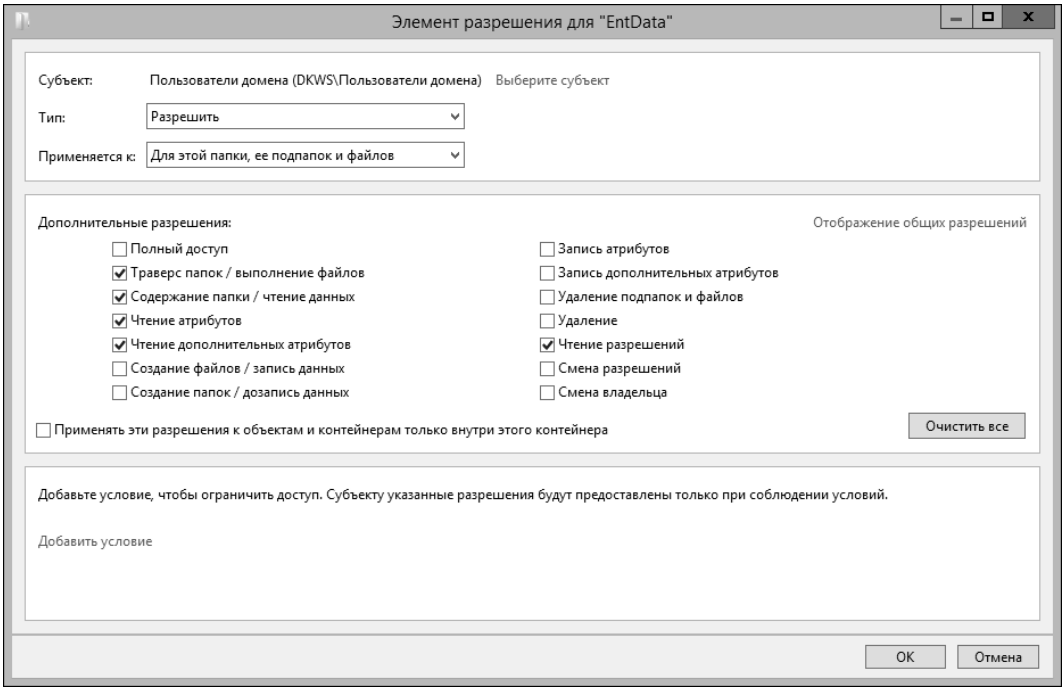


Рис. 4.3. Настройте особые разрешения, которые должны быть разрешены или запрещены

- **Для этой папки и ее файлов** (This folder and files) — разрешения применяются к этой папке и к любому файлу в ней. Они не применяются к подпапкам этой папки;
- **Только для подпапок и файлов** (Subfolders and files only) — разрешения применяются к любой подпапке этой папки и к любому файлу в этих папках. Но они не применяются к самой папке;
- **Только для подпапок** (Subfolders only) — разрешения применяются только к подпапкам, но не затрагивают ни файлы, ни саму папку;
- **Только для файлов** (Files only) — разрешения применяются к любым файлам в папке и в ее подпапках. Разрешения не применяются к самой папке и ее подпапкам.

11. Нажмите кнопку **OK**.

Поскольку у общих папок также есть NTFS-разрешения, можно задать особые NTFS-разрешения, используя консоль **Диспетчер серверов**:

1. В консоли **Диспетчер серверов** выберите узел **Файловые службы и службы хранилища**, а затем — **Общие ресурсы**. Щелкните правой кнопкой мыши по папке и выберите команду **Свойства**. Откроется одноименное окно.
2. В разделе **Разрешения** (на левой панели) отображаются текущие разрешения общего доступа и NTFS-разрешения.
3. Нажмите кнопку **Настройка разрешений**, чтобы открыть окно **Дополнительные параметры безопасности** с активной вкладкой **Разрешения**.

4. Пользователь и группы, для которых разрешения уже установлены, приведены в списке **Элементы разрешений**. Используйте предоставленные параметры для просмотра, редактирования, добавления или удаления разрешений для пользователей или групп. При редактировании выполните шаги 8–11 предыдущей процедуры для работы с особыми разрешениями.

Установка разрешений на основе требований

Средства управления доступом на основе требований используют комплексную проверку подлинности, включающую типы требований, которые являются утверждениями об объектах на базе атрибутов Active Directory, и свойства ресурса, классифицирующие объекты, и описывают их атрибуты. Когда доступ к ресурсам осуществляется удаленно, средства управления доступом на основе требований и центральные политики доступа полагаются на защиту Kerberos (Kerberos with Armoring) для аутентификации требований устройства. Защита Kerberos улучшает защиту домена, разрешая присоединенным к домену клиентам и контроллерам домена взаимодействовать по зашифрованным каналам.

Для тонкой настройки доступа используются разрешения на основе требований. Администратор определяет условия, ограничивающие доступ; это делается как часть установки дополнительных разрешений безопасности ресурса. Обычно эти условия добавляют требования устройств или требования пользователя к средствам управления доступом. Требования пользователя идентифицируют пользователей, а требования устройства — устройства. Например, можно определить типы требований на основе бизнес-категории или кода страны с помощью атрибутов Active Directory: businessCode и countryCode соответственно. Используя эти типы требований, можно гибко настроить доступ и гарантировать, что только пользователям, устройствам или обоим типам, принадлежащим определенной деловой категории или конкретной стране, будет предоставлен доступ к ресурсу. Также можно определить свойства ресурса Project для еще более тонкой настройки доступа.

> ***Дополнительная информация***
>
> С помощью централизованных политик доступа определяют централизованные правила доступа в Active Directory, эти правила применяются динамически по всему предприятию. Централизованные правила доступа используют условные выражения, требующие определения свойств ресурса, типы требований и/или группы безопасности, необходимые для политики, а также серверы, где должна быть применена политика.

Перед определением и применением условий требований к файлам и папкам компьютера нужно включить политику на основе требований. Для компьютеров, не подсоединенных к домену, это можно сделать путем включения и настройки политики **Поддержка KDC требований, комплексной проверки подлинности и защиты Kerberos** (KDC Support For Claims, Compound Authentication And Kerberos Armoring) в разделе **Конфигурация компьютера\Административные шаблоны\Система\Центр распространения ключей** (Computer Configuration\Administrative Templates\System\KDC). Можно задать один из режимов работы политики:

- **Поддерживается** (Supported) — контроллеры домена поддерживают требования (утверждения), комплексную проверку подлинности и защиту Kerberos. Компью-

теры клиентов, не поддерживающие защиту Kerberos, могут быть аутентифицированы;

- **Всегда предоставлять утверждения** (Always Provide Claims) — то же самое, что и режим **Поддерживается**, но контроллеры домена всегда поддерживают утверждения для учетных записей;
- **Отклонять запросы проверки подлинности без защиты** (Fail Unarmored Authentication) — защита Kerberos обязательна. Клиенты, не поддерживающие ее, не могут быть аутентифицированы.

Политика **Поддержка KDC требований, комплексной проверки подлинности и защиты Kerberos** контролирует, будут ли клиенты Kerberos, работающие под управлением Windows 8.1 и Windows Server 2012 R2, запрашивать утверждения и комплексную аутентификацию. Политика должна быть включена для Kerberos-совместимых клиентов для запроса утверждений и комплексной аутентификации. Данная политика называется **Поддержка динамического контроля доступа и защиты Kerberos** (Dynamic Access Control and Kerberos armoring) и находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Система\Центр распространения ключей**.

Нужно включить политику на основе требований для приложений по всему домену для всех контроллеров домена, чтобы гарантировать непротиворечивость приложения. Для этого она обычно включается и настраивается через объект групповой политики Default Domain Controllers или GPO самого высокого уровня, связанного с организационным подразделением контроллеров домена.

Как только основанная на требованиях политика включена и настроена, можно определить условия требования так:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите **Свойства**. В открывшемся окне перейдите на вкладку **Безопасность** и нажмите кнопку **Дополнительно**, чтобы открыть окно **Дополнительные параметры безопасности**.
2. Если у пользователя или группы уже есть разрешения для файла или папки, можно отредактировать их существующие разрешения. Выберите пользователя, с которым нужно работать, и нажмите кнопку **Изменить**, а после пропустите шаги 3–6.
3. Нажмите кнопку **Добавить** для отображения окна **Элемент разрешения** (Permission Entry). Щелкните по ссылке **Выберите субъект** для отображения окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.
4. Введите имя пользователя или группы. Убедитесь, что ссылаетесь на учетную запись пользователя, а не на его полное имя. За один раз можно добавить только одно имя.
5. Нажмите кнопку **Проверить имена**. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку **Размещение** для выбора нового размещения.

Если будет найдено несколько совпадений, откроется окно **Найдено несколько имен**, выберите имя и нажмите кнопку **OK**.

6. Нажмите кнопку **OK**, и группа или пользователь будут добавлены как **Субъект** (Principal). Щелкните по ссылке **Добавить условие** (Add a condition).
7. Используйте предоставленные опции для определения условия или условий, при соответствии которым будет предоставлен доступ. Для пользователей и групп установите базовые требования на основе членства в группе и/или ранее определенных типов требований. Для устройств определите условия для правильных значений.
8. Нажмите кнопку **OK**.

Поскольку общие папки также имеют NTFS-разрешения, можно установить разрешения на основе требований с использованием диспетчера серверов. Чтобы сделать это, выполните следующие действия:

1. В консоли **Диспетчер серверов** выберите узел **Файловые службы и службы хранилища**, а затем — **Общие ресурсы**.
2. Щелкните правой кнопкой мыши на папке и выберите команду **Свойства** для отображения одноименного окна.
3. На панели слева выберите элемент **Разрешения**, на основной панели будут отображены разрешения общего ресурса и NTFS-разрешения.
4. Нажмите кнопку **Настройка разрешений**, чтобы открыть окно **Дополнительные параметры безопасности** с активной вкладкой **Разрешения**.
5. Пользователи и группы, у которых уже есть доступ к файлу или папке, перечислены в списке **Элементы разрешений**. Используйте предоставленные опции для просмотра, редактирования, добавления или удаления разрешений для пользователей или групп. При редактировании или добавлении разрешений в окне **Элемент разрешения** можете добавить условия, как было показано в действиях 6–8 предыдущей процедуры.

Аудит системных ресурсов

Аудит — лучший способ для отслеживания событий в системах Windows Server 2012 R2. Аудит можно использовать для сбора информации, связанной с использованием какого-либо ресурса. Примерами событий для аудита могут являться доступ к файлу, вход в систему и изменение конфигурации системы. После включения аудита объекта в журнал безопасности системы заносятся записи при любой попытке доступа к этому объекту. Журнал безопасности можно просмотреть из оснастки **Просмотр событий** (Event Viewer).

> ***Примечание***
>
> Для изменения большинства настроек аудита необходимо войти в систему с учетной записью **Администратор** или члена группы **Администраторы** или иметь право **Управление аудитом и журналом безопасности** (Manage Auditing and Security Log) в групповой политике.

Установка политик аудита

Политики аудита существенно повышают безопасность и целостность систем. Практически каждая система в сети должна вести журналы безопасности. Можно настроить политики аудитов для отдельных компьютеров с помощью локальной групповой политики и для всех компьютеров в доменах с помощью групповой политики Active Directory. Посредством групповой политики можно установить политики аудита для целого сайта, домена или подразделения. Также возможно задать политики для персональных рабочих станций или серверов.

Выберите GPO и выполните следующие действия для установки политик аудита:

1. В редакторе управления групповыми политиками (рис. 4.4) перейдите к узлу **Политика аудита** (Audit Policy). Для этого разверните узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита** (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy).

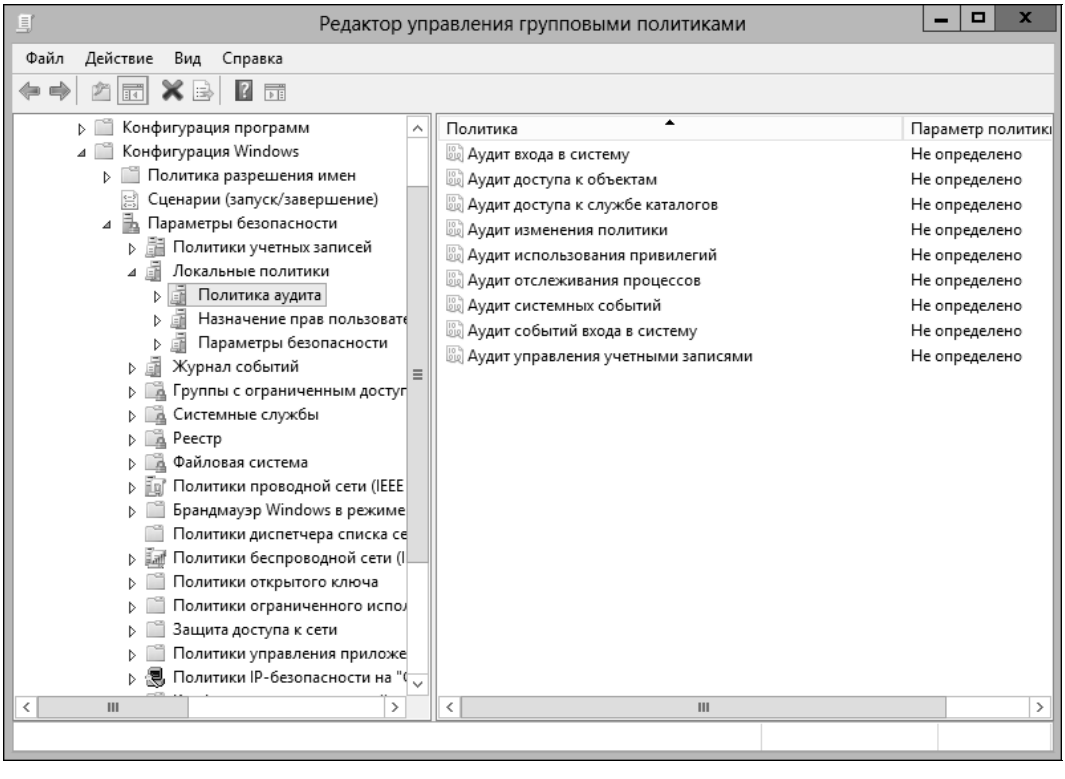


Рис. 4.4. Установите политики аудита в узле **Политика аудита**

2. Существуют следующие категории аудита:
   - **Аудит событий входа в систему** (Audit Account Logon Events) — отслеживает события, связанные с входом пользователя в систему и выходом из нее;

- **Аудит управления учетными записями** (Audit Account Management) — отслеживает все события, связанные с управлением учетными записями средствами оснастки **Active Directory — пользователи и компьютеры**. Записи аудита генерируются при создании, изменении или удалении учетных записей пользователя, компьютера или группы;
- **Аудит доступа к службе каталогов** (Audit Directory Service Access) — отслеживает события доступа к каталогу Active Directory. Записи аудита генерируются каждый раз при доступе пользователей или компьютеров к каталогу;
- **Аудит входа в систему** (Audit Logon Events) — отслеживает события входа в систему или выхода из нее, а также удаленные сетевые подключения;
- **Аудит доступа к объектам** (Audit Object Access) — отслеживает использование системных ресурсов файлами, каталогами, общими ресурсами и объектами Active Directory;
- **Аудит изменения политики** (Audit Policy Change) — отслеживает изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений;
- **Аудит использования привилегий** (Audit Privilege) — отслеживает каждую попытку применения пользователем предоставленного ему права или привилегии. Например, права архивировать файлы и каталоги;
- **Аудит отслеживания процессов** (Audit Process Tracking) — отслеживает системные процессы и ресурсы, используемые ими;
- **Аудит системных событий** (Audit System Events) — отслеживает события запуска, перезагрузки или выключения компьютера, а также события, влияющие на системную безопасность или отражаемые в журнале безопасности.

3. Для настройки политики аудита дважды щелкните на нужной политике или щелкните правой кнопкой мыши на записи и выберите команду **Свойства**.
4. В появившемся окне установите флажок **Определить следующие параметры политики** (Define these policy settings), а затем установите либо флажок **Успех** (Success), либо флажок **Отказ** (Failure), либо оба флажка. Флажок **Успех** регистрирует успешные события, например успешные попытки входа. Флажок **Отказ** регистрирует неудачные события, например неудачные попытки входа в систему.
5. Нажмите кнопку **OK**.

> ***Примечание***
>
> Политика **Аудит использования привилегий** не отслеживает события, связанные с доступом к системе, такие как использование права на интерактивный вход в систему или на доступ к компьютеру из сети. Эти события отслеживаются с помощью политики аудита входа в систему.

Когда аудит включен, журнал безопасности будет отображать следующее:

- идентификаторы события 560 и 562 — аудит пользователя;
- идентификаторы события 592 и 593 — аудит процесса.

Аудит файлов и папок

Если GPO настроен для включения политики **Аудит доступа к объектам**, можно установить уровень аудита для отдельных файлов и папок. Это позволит точно отслеживать их использование. Данная возможность доступна только на томах с файловой системой NTFS.

Для настройки аудита файлов и папок выполните следующие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду **Свойства**.
2. Перейдите на вкладку **Безопасность** и нажмите кнопку **Дополнительно**. Откроется окно **Дополнительные параметры безопасности**.
3. На вкладке **Аудит** (Auditing) можно просматривать и управлять настройками аудита (рис. 4.5).

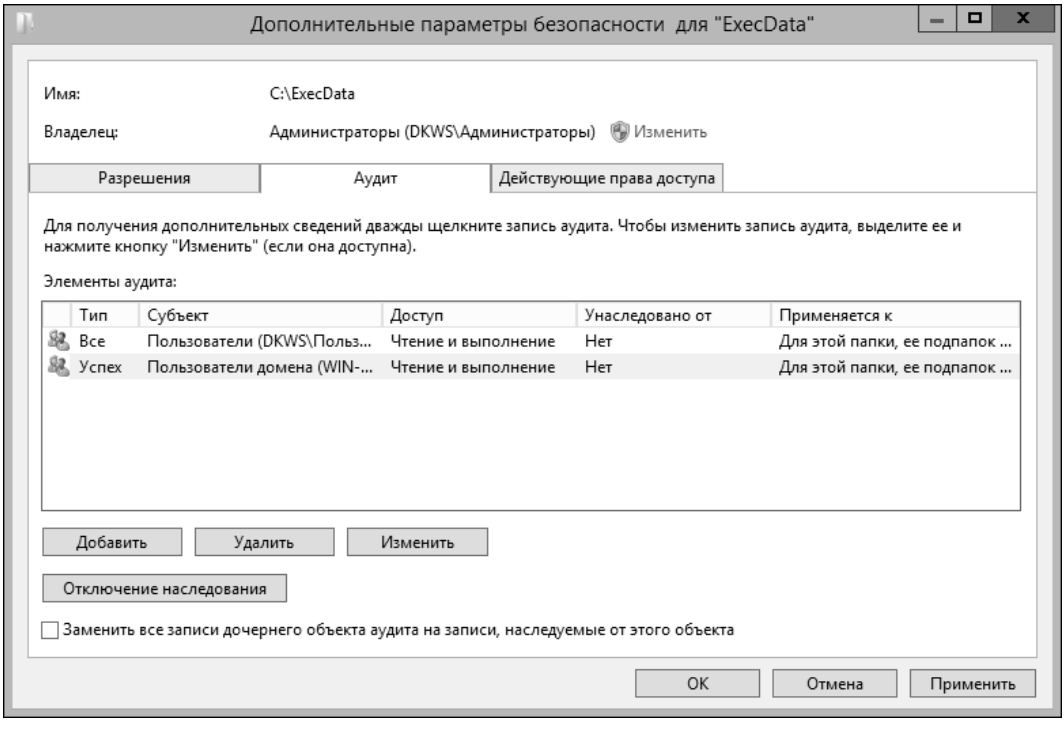


Рис. 4.5. Настройка политик аудита для отдельных файлов или папок на вкладке **Аудит**

4. Используйте список **Элементы аудита** (Auditing entries) для выбора пользователей, компьютеров или групп, действия которых будут отслеживаться. Для удаления учетной записи из этого списка выберите ее и нажмите кнопку **Удалить**.
5. Для аудита дополнительных пользователей, компьютеров или групп нажмите кнопку **Добавить**. Откроется окно **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.

6. Введите имя пользователя, компьютера или группы в текущем домене или нажмите кнопку **Проверить имена**. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку **Размещение** (Locations) для выбора нового размещения. Если найдено несколько совпадений, в окне **Найдено несколько имен** выберите имя или имена, которые нужно использовать, и нажмите кнопку **OK**.

7. Нажмите кнопку **OK**. Пользователь или группа будут добавлены как **Субъект**, а окно **Элемент аудита** будет обновлено, чтобы отобразить это. По умолчанию отображены только базовые разрешения. Если нужно работать с расширенными разрешениями, установите флажок **Отображение дополнительных разрешений** (Show Advanced Permissions).

8. Если необходимо, используйте список **Применяется к** (Applies to), чтобы указать объекты для применения настроек аудита. Если производится работа с папкой и нужно заменить записи аудита на всех дочерних объектах этой папки (но не на самой папке), установите флажок **Применять эти параметры аудита к объектам и контейнерам только внутри этого контейнера** (Only apply these settings to objects and/or containers within this container). Помните, что список **Применить к** позволяет указать места, *где* будут применяться настройки аудита. Флажок **Применять эти параметры аудита к объектам и контейнерам только внутри этого контейнера** определяет, *как* будут применяться настройки аудита. Когда этот флажок включен, параметры аудита родительского объекта заменяют настройки дочерних объектов. Когда этот флажок сброшен, параметры аудита родительского объекта будут объединены с существующими параметрами на дочерних объектах.

9. Используйте раскрывающийся список **Тип** для уточнения, какие события (успешные, неудачные или оба типа) будут регистрироваться. **Успех** — это успешные события, например успешное чтение файла. **Отказ** — неудачные события, например неудачное удаление файла. События для аудита совпадают с особыми разрешениями (см. табл. 4.3 и 4.4) за исключением синхронизации автономных файлов и папок, аудит которых невозможен. Для важных файлов и папок обычно отслеживают следующее:

   - запись атрибутов — успех;
   - запись расширенных атрибутов — успех;
   - удаление подпапок и файлов — успех;
   - удаление — успех;
   - смена разрешений — успех.

   Совет

   Если нужно отслеживать действия всех пользователей, выберите особую группу **Все**. В противном случае используйте специфическую группу пользователей и/или пользователей, которых нужно отслеживать.

10. Если применяются политики на основе требований и нужно ограничить область элемента аудита, можно добавить условия в элемент аудита. Например, если все корпоративные компьютеры являются членами группы **Компьютеры домена**, можно контролировать доступ устройств, которые не являются членами этой группы.
11. Нажмите кнопку **OK**. Повторите этот процесс для аудита других пользователей, групп или компьютеров.

Аудит реестра

Если объект групповой политики настроен для включения опции **Аудит доступа к объектам**, можно установить уровень аудита для ключей реестра. Это позволяет отслеживать, когда изменялись значения ключей, когда создавались подключи, когда удалялись ключи.

Настроить аудит реестра можно с помощью следующих действий:

1. Откройте редактор реестра (regedit.exe). В командной строке или в поле поиска приложений введите `regedit` и нажмите клавишу <Enter>.
2. Перейдите к ключу реестра, который нужно отслеживать. Далее из меню **Правка** (Edit) выберите команду **Разрешения** (Permissions).
3. В окне **Разрешения** нажмите кнопку **Дополнительно**. В окне **Дополнительные параметры безопасности** перейдите на вкладку **Аудит**.
4. Нажмите кнопку **Добавить** для отображения окна **Элемент аудита**. Щелкните по ссылке **Выберите субъект** для отображения окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.
5. В этом окне введите **Все** (Everyone) и нажмите кнопку **Проверить имена**, а затем нажмите кнопку **OK**.
6. В окне **Элемент аудита** отображаются только базовые разрешения. Щелкните по ссылке **Отображения дополнительных разрешений**, чтобы отобразить особые разрешения.
7. Используйте список **Применяется к**, чтобы указать, как будет применяться элемент аудита.
8. Используйте раскрывающийся список **Тип** для уточнения, какие события (успешные, неудачные или оба типа) будут регистрироваться. Обычно нужно отслеживать следующие особые разрешения:
   - задание значения — успех и отказ;
   - создание подраздела — успех и отказ;
   - удаление — успех и отказ.
9. Нажмите кнопку **OK** три раза, чтобы закрыть все открытые диалоговые окна и применять настройки аудита.

Аудит объектов Active Directory

Если задействована политика **Аудит доступа к службе каталогов**, можно использовать аудит на уровне объектов службы каталогов Active Directory. Это позволит точно отслеживать их использование.

Для настройки аудита объекта проделайте следующее:

1. В оснастке **Active Directory — пользователи и компьютеры** убедитесь, что в меню **Вид** выбрана опция **Дополнительные компоненты**, а затем перейдите в контейнер, содержащий объект.
2. Дважды щелкните по объекту для аудита. Будет открыто окно **Свойства**.
3. Перейдите на вкладку **Безопасность**, затем нажмите кнопку **Дополнительно**.
4. В окне **Дополнительные параметры безопасности** перейдите на вкладку **Аудит**. Список **Элементы аудита** показывает пользователей, группы или компьютеры, действия которых уже отслеживаются. Для удаления учетной записи из этого списка выберите ее и нажмите кнопку **Удалить**.
5. Для добавления особых учетных записей нажмите кнопку **Добавить**, чтобы открыть окно **Элемент аудита**. Щелкните по ссылке **Выберите субъект** для отображения окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.
6. Введите имя пользователя, компьютера или группы в текущем домене или нажмите кнопку **Проверить имена**. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку **Размещение** для выбора нового размещения. Если найдено несколько совпадений, в окне **Найдено несколько имен** выберите имя или имена и нажмите кнопку **OK**.
7. Нажмите кнопку **OK** для возврата в окно **Элемент аудита**. Используйте список **Применяется к**, чтобы определить, как элемент аудита будет применен.
8. Используйте раскрывающийся список **Тип**, чтобы указать, какие события (успех, отказ или оба типа) нужно регистрировать. Успех регистрирует успешные события, например успешную попытку модификации разрешений объекта. Отказ регистрирует неудачные события, например неудачную попытку изменения владельца объекта.
9. Нажмите кнопку **OK**. Повторите этот процесс для аудита других пользователей, групп или компьютеров.

Использование, настройка и управление дисковых квот файловой системы NTFS

Операционная система Windows Server 2012 R2 поддерживает два взаимоисключающих типа дисковых квот.

- *Дисковые квоты файловой системы NTFS* поддерживаются всеми выпусками Windows Server 2012 R2 и позволяют администратору управлять использованием

дискового пространства пользователями. Квоты настраиваются для каждого тома. Хотя пользователи, которые превысили лимиты, увидят предупреждения, администраторы будут уведомлены через журнал событий.

- *Дисковые квоты диспетчера ресурсов* поддерживаются всеми выпусками Windows Server 2012 R2 и позволяют управлять использованием дискового пространства на уровне папки и тома. Пользователи, которые скоро превысят лимит или уже превысили его, могут быть автоматически уведомлены по электронной почте. Система уведомления также позволяет уведомлять по электронной почте администраторов, протоколировать соответствующие события и запускать команды.

Далее мы рассмотрим дисковые квоты NTFS.

Примечание

Независимо от того, какая система дисковых квот была выбрана, можно настроить квоты только на NTFS-тома. Нельзя создать квоты на FAT-, FAT32- или ReFS-томах.

Практический совет

Когда задаются дисковые квоты, нужно быть предельно внимательным при выборе способа их применения, особенно в отношении системных учетных записей, учетных записей служб или других учетных записей особого назначения. Неправильное применение дисковых квот к учетным записям этих типов может вызвать серьезные проблемы, которые трудно диагностировать и решить. Установив квоты на учетных записях **System**, **NetworkService** или **LocalService**, можно препятствовать выполнению важных задач операционной системы. Например, если эти учетные записи достигнут определенного лимита квоты, нельзя будет применить изменения в групповой политике, поскольку клиент групповой политики работает в контексте **LocalSystem** по умолчанию и не сможет записать данные на системный диск. Если служба не может записать данные на системный диск, изменения групповой политики также нельзя будет внести, что приведет к непредсказуемым последствиям, и ранее установленные настройки нельзя будет изменить. Например, нельзя будет даже отключить или изменить настройки квот через групповую политику.

В этом сценарии, где контексты службы достигли установленного лимита квоты, любые другие средства настройки, использующие эти контексты службы и требующие внесения изменений в файлы на диске, вероятно, также перестанут работать. Например, невозможно будет завершить установку или удаление ролей, служб роли и компонентов. Это оставит сервер в состоянии, в котором диспетчер серверов всегда выводит предупреждение о том, что нужно перезапустить компьютер для завершения задач конфигурации, но перезапуск компьютера не решит эти проблемы.

Чтобы решить эту проблему, нужно отредактировать записи дисковых квот для системного диска, повысить лимит на учетных записях служб и затем перезагрузить компьютер. Перезагрузка компьютера инициирует задачи завершения и позволит компьютеру выполнять любые задачи конфигурации в состоянии ожидания. Поскольку клиентская служба групповой политики сможет обработать изменения и записать их на системный диск, изменения в групповой политике также будут применены.

Что такое дисковые квоты файловой системы NTFS, или как используются квоты

Администраторы применяют дисковые квоты файловой системы NTFS для управления использованием дискового пространства критически важных томов, например, тех, на которых размещены корпоративные общие ресурсы или пользовательские общие ресурсы.

При включении дисковых квот можно будет настроить два значения:

- *предел квоты* устанавливает верхнюю границу использования дискового пространства, превышение которой запретит пользователям запись дополнительной информации на том или зарегистрирует событие относительно пользователя, превышающего лимит, либо будут выполнены оба действия;
- *порог выдачи предупреждения* уведомляет пользователей о превышении квоты и записывает событие-предупреждение, когда пользователи почти достигли установленного предела.

> ***Совет***
>
> Можно установить дисковые квоты, но не ограничивать действия пользователей при превышении предела квоты. Иногда, когда нужно отслеживать использование дискового пространства на уровне пользователей, гораздо важнее знать, кто именно превысит лимит, чем запрещать им выделение дополнительного дискового пространства. Можно протоколировать превышение лимита. Также можно отправить пользователю предупреждение или найти другие способы уменьшения использования дискового пространства.

Дисковые квоты NTFS применяются только к конечным пользователям. Дисковые квоты не применяются к администраторам, которым нельзя запретить доступ к диску, даже если они превысили установленные лимиты дисковой квоты.

В обычном окружении ограничивается использование дискового пространства в мегабайтах (Мбайт) или гигабайтах (Гбайт). Например, на корпоративном общем ресурсе, с которым работают многие пользователи подразделения, можно установить предел использования дискового пространства от 20 до 100 Гбайт. Для пользовательского общего ресурса можно задать предел на уровень меньше, например, от 5 до 20 Гбайт, что не позволит пользователю создавать большие объемы персональных данных. Часто устанавливается порог предупреждения как процент от предела дисковой квоты. Например, предупреждение будет отображено, если достигнуто 90–95% от установленного предела квоты.

Поскольку дисковые квоты NTFS отслеживаются на уровне тома и на уровне пользователя, дисковое пространство, занимаемое одним пользователем, не влияет на дисковые квоты других пользователей. Поэтому, если один пользователь превысит свой предел, любые ограничения, применимые к этому пользователю, не распространяются на других пользователей. Например, если пользователь превысит свой лимит в 5 Гбайт и том сконфигурирован так, чтобы предотвратить запись после превышения лимита, пользователь больше не может записать данные на том. Однако пользователи могут удалить файлы и папки, чтобы освободить дисковое пространство. Они могут переместить файлы и папки на сжатую область тома, что также поможет освободить пространство, или же они могут просто сжать сами файлы. Перемещение файлов в другое место на томе не влияет на ограничение квоты. Сумма файлового пространства будет та же, за исключением ситуации, когда пользователь переместит несжатые файлы и папки в папку со сжатием. В любом случае ограничение одного пользователя не влияет на возможность других пользователей записывать данные на том (до тех пор, пока на этом томе есть свободное дисковое пространство).

Можно включить дисковые квоты NTFS на следующих типах томов.

- **Локальные тома.** Для управления дисковыми квотами на локальных томах нужно работать непосредственно с самим локальным диском. При включении дисковых

квот на локальном томе системные файлы Windows также учитываются при вычислении использования дискового пространства — для пользователя, который установил эти файлы. Иногда это приводит к превышению лимита квоты. Чтобы предотвратить это, нужно установить более высокий лимит на томе локальной рабочей станции.

- **Удаленные тома.** Для управления квотами на удаленных томах нужно предоставить общий доступ к корневому каталогу тома и затем установить квоту на томе. Помните, что установка квот производится отдельно для каждого тома, поэтому если на удаленном файловом сервере есть два разных тома для двух различных типов данных — том с корпоративными данными и том с пользовательскими данными, у этих томов будут разные квоты.

Настраивать дисковые квоты могут только члены группы **Администраторы домена** или группы **Администраторы** локальной системы. Первым делом нужно включить квоты в групповой политике. Можно сделать это на двух уровнях:

- *на локальном* — с помощью локальной групповой политики можно включить дисковые квоты для отдельного компьютера;
- *на корпоративном* — с помощью групповой политики, которая применяется к сайту, домену или организационному подразделению, можно включить дисковые квоты для групп пользователей или компьютеров.

Необходимость отслеживать дисковые квоты действительно вызывает некоторые издержки на компьютерах. Эти издержки — функция числа дисковых квот, общий размер томов и их данных и число пользователей, к которым применяются квоты.

Хотя дисковые квоты устанавливаются для имен пользователей, негласно ОС Windows Server 2012 R2 управляет дисковыми квотами с помощью идентификаторов безопасности (SID). Поскольку для отслеживания дисковых квот используются SID, можно безопасно изменить имена пользователей, что никак не отразится на конфигурации дисковых квот. Отслеживание SID действительно вызывает некоторые дополнительные издержки, когда просматривается статистика дисковых квот для пользователей. ОС Windows Server 2012 R2 должна преобразовывать SID в имена пользователей, чтобы показать их в диалоговых окнах. А это означает, что нужно связываться с локальным диспетчером пользователя или с контроллером домена Active Directory в случае необходимости.

После того как операционная система Windows Server 2012 R2 преобразует имена, она кэширует их в локальном файле, поэтому они будут моментально доступны в следующий раз, когда понадобятся. Кэш запроса нечасто обновляется — если заметите несоответствие между тем, что отображено, и тем, что настроено, нужно обновить информацию. Обычно следует выбрать команду **Обновить** (Refresh) из меню **Вид** (View) или просто нажать клавишу <F5> в текущем окне.

Установка политик дисковых квот файловой системы NTFS

Лучший способ настроить дисковые квоты NTFS — применить групповую политику. При настройке дисковых квот с помощью локальной политики или через политику

организационного подразделения, домена или сайта определяется общая политика, которая будет установлена автоматически, как только будет включено управление квотами на отдельных томах. Таким образом, вместо настройки каждого отдельного тома можно использовать один и тот же набор правил и применять их поочередно к каждому тому, которыми нужно управлять.

Политики, контролирующие дисковые квоты NTFS, применяются на уровне системы и находятся в разделе **Конфигурация компьютера\Административные шаблоны\Система\Дисковые квоты** (Computer Configuration\Administrative Templates\System\Disk Quotas). В табл. 4.5 представлены доступные политики.

Таблица 4.5. *Политики для установки дисковых квот NTFS*

Имя политики	Описание
Применять политику к съемным носителям (Apply Policy To Removable Media)	Определяет, должны ли политики квот применяться к NTFS-томам на съемных дисках. Если не включить эту политику, дисковые квоты будут применяться только к фиксированным (внутренним) дискам (к жестким дискам)
Включить дисковые квоты (Enable Disk Quotas)	Включает или выключает дисковые квоты для всех NTFS-томов компьютера и запрещает пользователям изменять эту настройку
Обеспечить соблюдение дисковой квоты (Enforce Disk Quota Limit)	Если система будет обеспечивать соблюдение квоты, пользователи не смогут записать данные на диск, если они превысят предел квоты. Эта политика переопределяет значение, установленное на вкладке **Квота** (Quota) окна свойств NTFS-тома
Записать в журнал событие при превышении квоты (Log Event When Quota Limit Exceeded)	Определяет, будет ли записано событие, когда пользователи превысят квоту, и запрещает пользователям изменять их параметры протоколирования
Записать в журнал событие, возникающее при превышении порога предупреждений квоты (Log Event When Quota Warning Level Exceeded)	Определяет, регистрирует ли система в локальном журнале приложений событие, возникающее при достижении пользователями порога предупреждений для дисковой квоты
Определить квоту и порог предупреждений по умолчанию (Specify Default Quota Limit And Warning Level)	Устанавливает дисковую квоту и порог предупреждений по умолчанию для всех пользователей. Эта настройка переопределяет другие параметры и применима только для новых пользователей

При работе с пределами квоты нужно использовать стандартный набор политик на всех системах. Как правило, не нужно включать все политики. Вместо этого необходимо выборочно включить политики и затем использовать стандартные функции NTFS, чтобы управлять квотами на разных томах. Для включения квот выполните следующие действия:

1. Откройте групповую политику для системы (например, для файлового сервера). Перейдите к узлу **Дисковые квоты** (Disk Quotas), развернув узел **Конфигурация компьютера\Административные шаблоны\Система** (Computer Configuration\Administrative Templates\System).

2. Дважды щелкните по параметру политики **Включить дисковые квоты** (Enable disk quotas). Выберите **Включено** (Enabled) и нажмите кнопку **OK**.
3. Дважды щелкните по элементу **Обеспечить соблюдение дисковой квоты** (Enforce Disk Quota Limit). Если нужно обеспечить соблюдение дисковых квот на всех NTFS-томах этого компьютера, выберите значение **Включено** (Enabled), в противном случае выберите значение **Выключено** (Disabled) и затем установите квоты отдельно для каждого тома. Нажмите кнопку **OK**.
4. Дважды щелкните по параметру политики **Определить квоту и порог предупреждений по умолчанию** (Specify default quota limit and warning level). В диалоговом окне (рис. 4.6) установите переключатель **Включено**.

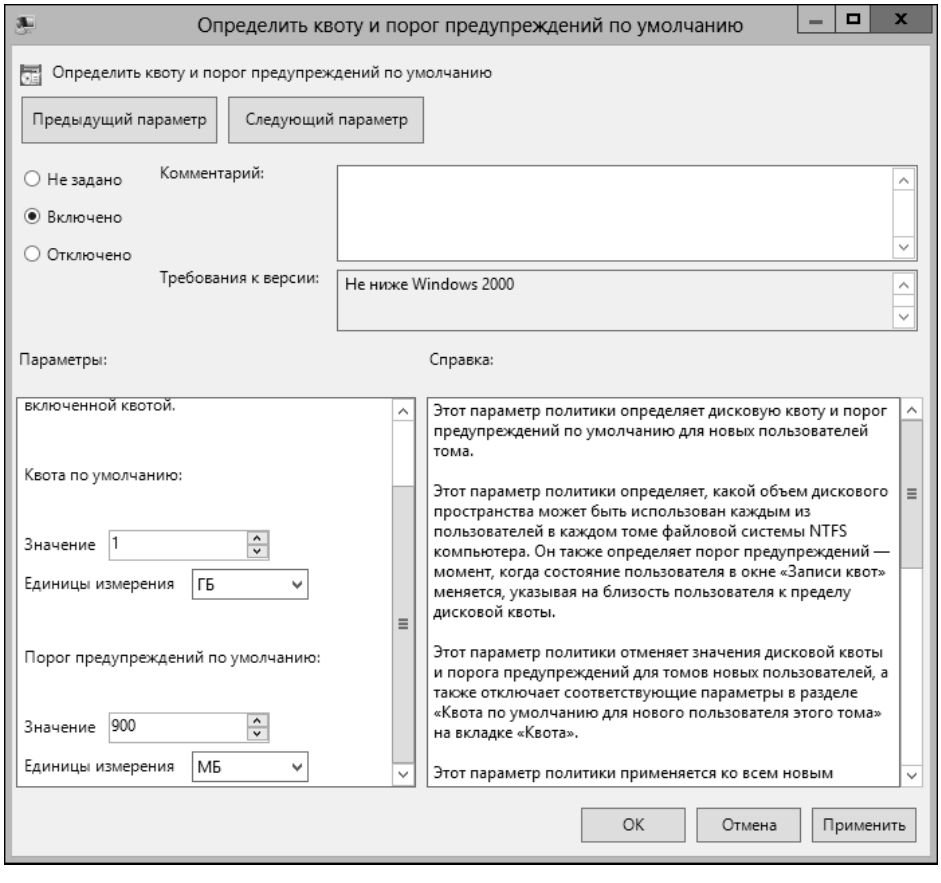


Рис. 4.6. Установите квоту и порог предупреждения

5. В поле **Квота по умолчанию** (Default quota limit) установите лимит дискового пространства по умолчанию, который будет применен к пользователям, когда они впервые запишут данные на том с этими включенными квотами. Квота не применяется к текущим пользователям. Для корпоративного общего ресурса, например, используемого членами команды проекта, можно установить квоту от 5 до 10 Гбайт. Конечно, размер квоты зависит от размера файлов, с которыми работают пользова-

тели, от числа пользователей и размера тома. Дизайнерам и инженерам данных может понадобиться больше дискового пространства.

6. Для установки порога предупреждений пролистайте вниз окно **Параметры** (Options). Хороший порог — 90% от квоты по умолчанию, это означает, что если установлена квота размером 10 Гбайт, порог предупреждения нужно установить в 9 Гбайт. Нажмите кнопку **OK**.
7. Дважды щелкните на параметре **Записать в журнал событие при превышении квоты** (Log event when quota limit exceeded). Установите переключатель **Включено**, чтобы при достижении пользователями предела квоты соответствующее событие записывалось в журнал приложений, и нажмите кнопку **OK**.
8. Дважды щелкните на параметре **Записать в журнал событие при превышении порога предупреждения** (Log event when quota warning level exceeded). Установите переключатель **Включено**, чтобы при достижении пользователями порога предупреждения соответствующее событие записывалось в журнал приложений, и нажмите кнопку **OK**.
9. Дважды щелкните на параметре **Применить политику к съемным носителям** (Apply policy to removable media). Установите переключатель **Отключено** — квоты не будут применяться к съемным томам компьютера. Затем нажмите кнопку **OK**.

> ***Совет***
>
> Чтобы убедиться, что политики были применены немедленно, перейдите в узел **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика** (Computer Configuration\Administrative Templates\System\Group Policy) и дважды щелкните на политике **Настройка обработки политики дисковых квот** (Configure Disk Quota Policy Processing). Выберите переключатель **Включено**, а затем — **Обрабатывать, даже если объекты групповой политики не изменились** (Process Even If The Group Policy Objects Have Not Changed). Нажмите кнопку **OK**.

Включение дисковых квот на томах NTFS

Установить дисковые квоты NTFS можно отдельно для каждого тома. Дисковые квоты могут быть включены только для томов с файловой системой NTFS. После настройки надлежащих групповых политик можно использовать оснастку **Управление компьютером** для установки дисковых квот локальных и удаленных томов.

> ***Примечание***
>
> Если используется параметр политики **Обеспечить соблюдение дисковой квоты** (Enforce Disk Quota Limit), пользователи не смогут записать данные на диск, превысив квоту. Этот параметр перезаписывает параметр на вкладке **Квота** (Quota) тома NTFS.

Для включения дисковых квот на NTFS-томе выполните следующие действия:

1. Откройте оснастку **Управление компьютером**. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства**, а затем выберите **Управление дисками**. На основной панели будут отображены тома, настроенные на компьютере.

3. Используйте представление **Список томов** или **Графическое представление**, щелкните на томе и выберите команду **Свойства**.
4. На вкладке **Квота** установите флажок **Включить управление квотами** (Enable quota management) (рис. 4.7). Если квоты уже включены через групповую политику, эти параметры будут недоступны, и их нельзя изменить. Вместо этого нужно модифицировать параметры через групповую политику.

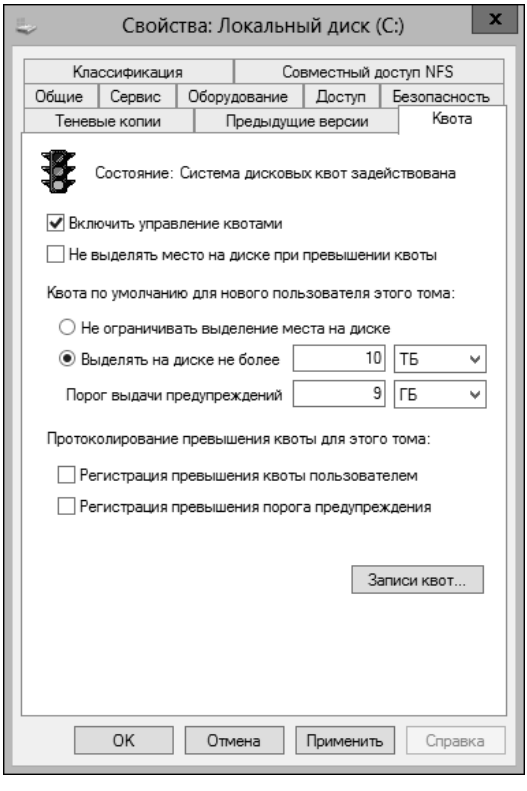


Рис. 4.7. После включения управления квотами можно настроить квоту и порог выдачи предупреждений

Рекомендации

При работе с вкладкой **Квота** обратите особое внимание на текст **Состояние** (Status) и значок светофора. Если квоты не настроены, светофор показывает красный свет, а состояние сообщит, что дисковые квоты отключены. Если операционная система обновляет квоты, светофор покажет желтый свет, а **Состояние** отобразит выполняемое действие. Если квоты настроены, светофор покажет зеленый свет, а текст состояния сообщит, что квоты активны.

5. Для установки квоты по умолчанию для всех пользователей выберите переключатель **Выделять на диске не более** (Limit disk space to). В текстовом поле введите лимит в килобайтах, мегабайтах, гигабайтах, терабайтах, петабайтах или эксабайтах. Затем установите параметр **Порог выдачи предупреждений** (Set warning level to). Обычно порог выдачи предупреждений соответствует 90–95% от дисковой квоты.

Совет

Хотя квота и порог предупреждения по умолчанию применяются ко всем пользователям, можно настроить разные уровни для отдельных пользователей. Это можно сделать в окне **Записи квот** (Quota Entries). Если создано много уникальных записей квот и нет желания создавать их на томе с одинаковыми характеристиками и использованием, можно экспортировать записи квот и импортировать их на другой том.

6. Чтобы обеспечить соблюдение квоты и запретить пользователям запись данных на диск после превышения лимита, установите флажок **Не выделять место на диске при превышении квоты** (Deny disk space to users exceeding quota limit). Помните, что включение этого параметра создаст фактическое физическое ограничение для пользователей, но не для администраторов.
7. Для настройки протоколирования, когда пользователи превысят порог предупреждения или квоту, установите флажки **Регистрация...** (Log event...). Нажмите кнопку **OK** для сохранения изменений.
8. Если квоты системы в данный момент выключены, будет отображено окно, спрашивающее разрешения включить квоты. Нажмите кнопку **OK** для разрешения Windows Server 2012 R2 пересканировать том и обновить статистику использования диска. Против пользователей, превышающих квоту или порог, могут быть предприняты меры. Эти меры могут включать предотвращение записи на том, уведомление и регистрацию событий в журнале приложений.

Просмотр записей квот

Дисковое пространство отслеживается отдельно для каждого пользователя. Если дисковые квоты включены, у каждого пользователя, записывающего данные на том, есть запись в файле дисковой квоты. Эта запись периодически обновляется, чтобы показать используемое в данный момент дисковое пространство, предельную квоту, порог предупреждения и процент допустимого использованного пространства. Администратор может изменить записи квот для установки разных квот и порогов предупреждения для определенных пользователей. Администратор также может создать записи квот для пользователей, у которых еще нет сохраненных данных на томе. Основная причина создания записи заключается в том, чтобы у пользователя, работающего с томом, была надлежащая квота и порог предупреждения.

Для просмотра текущих записей квот для тома выполните следующие действия:

1. Откройте оснастку **Управление компьютером**. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства**, а затем выберите **Управление дисками**. На основной панели будут отображены тома, настроенные на компьютере.
3. Используйте представление **Список томов** или **Графическое представление**, щелкните на томе и выберите команду **Свойства**.
4. На вкладке **Квоты** нажмите кнопку **Записи квот**. Откроется одноименное окно. Каждая запись приводится согласно состоянию. Состояние позволяет быстро узнать, превысил ли пользователь квоту. Состояние **OK** означает, что пользователь

работает в пределах квоты. Любое другое состояние обычно означает, что пользователь достиг либо порога предупреждения, либо предела квоты.

Создание записей квоты

Администратор может создать записи квот для пользователей, которые еще не сохраняли данные на томе. Это позволяет установить квоту и порог предупреждения для конкретного пользователя. Обычно эта функция используется, когда пользователь часто сохраняет больше информации, чем другие пользователи, и надо разрешить ему использовать больше пространства, чем остальным пользователям, либо когда нужно установить определенный лимит для администраторов. Как было ранее отмечено, администраторы не являются субъектами дисковых квот, поэтому если нужно задать квоты для отдельных администраторов, необходимо создать записи квот для каждого администратора, которого надо ограничить.

> ***Практический совет***
>
> Нельзя создавать отдельные записи квот хаотически. Необходимо тщательно отслеживать отдельные записи. В идеале, можно хранить журнал, который детализирует любые отдельные записи так, чтобы другие администраторы поняли, какие политики используются и как они применены. При изменении основных правил томов на томе нужно повторно исследовать отдельные записи, чтобы увидеть, применимы ли они все еще или должны быть обновлены. Я обнаружил, что определенные типы пользователей — чаще исключение, чем правило, и поэтому иногда лучше поместить отдельные классы пользователей на разные тома и затем применять дисковые квоты к каждому тому. Таким образом, у каждого класса пользователей будет квота, подходящая для типичных задач, выполняемых пользователями. Например, можно создать отдельные тома для руководителей, менеджеров и обычных пользователей или можно создать отдельные тома для управляющих, дизайнеров, инженеров и всех остальных пользователей.

Для создания записи квоты на томе выполните следующие действия:

1. Откройте окно **Записи квот**, как было описано ранее в этой главе. Окно содержит записи квот для всех пользователей. Для обновления окна нажмите клавишу <F5> или выберите команду **Вид | Обновить**.
2. Если у пользователя еще нет записи на этом томе, можно создать ее, выбрав команду **Квота | Создать запись квоты** (Quota | New quota entry). Откроется окно **Выбор: "Пользователи"**.
3. В этом окне введите имя пользователя в поле **Введите имя выбираемых объектов** (Enter the object names to select), а затем нажмите кнопку **Проверить имена**. Если совпадение найдено, выберите учетную запись и нажмите кнопку **OK**. Если совпадений не будет, введите другое имя и повторите поиск снова. Повторите этот шаг при необходимости и затем нажмите кнопку **OK**.
4. После выбора пользователя появится окно **Добавление новой квоты** (Add New Quota Entry) (рис. 4.8). Есть две опции. Можно удалить все ограничения квот для этого пользователя, выбрав переключатель **Не ограничивать выделение места на диске** (Do not limit disk usage), или установить определенную квоту и порог предупреждений, выбрав переключатель **Выделять на диске не более** (Limit disk space to) (после этого нужно ввести надлежащие значения). Нажмите кнопку **OK**.

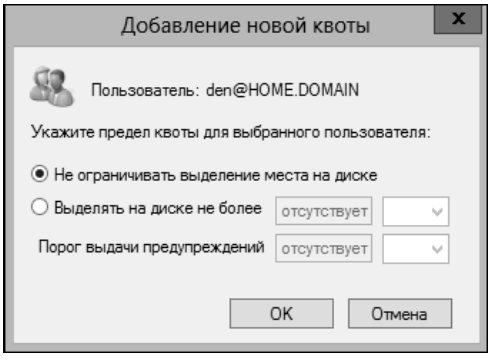


Рис. 4.8. В окне **Добавление новой квоты** можно настроить квоту для пользователя и порог выдачи предупреждения или удалить ограничения квоты вообще

Удаление записей квот

Если пользователю больше не нужно использовать том, а для него созданы записи квот, можно удалить соответствующие записи. При удалении записи квоты все файлы связанного с записью пользователя будут собраны и отображены в окне, и можно будет безвозвратно удалить эти файлы, сменить их владельца или переместить эти файлы в папку на другом томе.

Для удаления записи квоты для пользователя и управления оставшимися файлами пользователя выполните следующие действия:

1. Откройте окно **Записи квот**, как было описано ранее в этой главе. Окно содержит записи квот для всех пользователей. Для обновления окна нажмите клавишу <F5> или выберите команду **Вид | Обновить**.
2. Выберите запись дисковой квоты, которую нужно удалить, и нажмите клавишу <Delete> или выберите команду **Удалить запись квоты** (Delete Quota Entry) из меню **Квота**. Несколько записей можно выделить с помощью клавиш <Shift> и <Ctrl>.
3. Для подтверждения действия нажмите кнопку **Да**. Откроется окно **Дисковая квота**, содержащее список файлов, принадлежащих выбранному пользователю (пользователям).
4. В списке **Файлы, которыми владеет** (List files owned by) отображаются файлы для пользователя, чья запись квоты удаляется. Можно обработать каждый файл отдельно, выбрав отдельные файлы и надлежащее действие, а можно выбрать несколько файлов с помощью клавиш <Shift> и <Ctrl>. Доступны следующие опции:
   - **Удалить** (Permanently delete files) — выберите файлы для удаления и нажмите кнопку **Удалить**. Для подтверждения действия нажмите кнопку **Да**;
   - **Сменить владельца** (Take ownership of files) — выберите файлы, для которых нужно сменить владельца, и нажмите кнопку **Сменить владельца**;
   - **Переместить** (Move files to) — выберите файлы, которые нужно переместить, и затем введите путь к папке на другом томе. Если не знаете точный путь, исполь-

зуйте кнопку **Обзор** для отображения окна **Обзор папок**. Как только будет найдена надлежащая папка, нажмите кнопку **Переместить** (Move).

5. Нажмите кнопку **Закрыть**. Если надлежащим образом были обработаны все файлы пользователя, запись квоты будет удалена[1].

Экспорт и импорт дисковых квот NTFS

Вместо повторного создания пользовательских записей квот на отдельных томах можно экспортировать настройки с исходного тома и затем импортировать их на другой том. Оба тома должны быть отформатированы в NTFS. Для экспорта и последующего импорта записей квот выполните следующие действия:

1. Откройте окно **Записи квот**, как было описано ранее в этой главе. Окно содержит записи квот для всех пользователей. Для обновления окна нажмите клавишу <F5> или выберите команду **Вид | Обновить**.
2. Выберите запись квоты и команду **Квота | Экспорт** (Quota | Export). Будет отображено окно **Параметры экспорта квоты** (Export Quota Settings). Выберите размещение для файла квоты, введите его имя в поле **Имя файла** и нажмите кнопку **Сохранить**.

   Примечание

   В окне сохранения файла квоты можно просто ввести имя файла и нажать кнопку **Сохранить**. Так будет проще импортировать файл. Файлы квоты очень маленькие, поэтому не нужно беспокоиться об использовании дискового пространства.

3. Выберите команду **Квота | Закрыть** (Quota | Close) для закрытия окна **Записи квот**.
4. Щелкните правой кнопкой мыши на узле **Управление компьютером** и выберите команду **Подключиться к другому компьютеру** (Connect to another computer). В окне **Выбор компьютера** (Select Computer) выберите компьютер, содержащий целевой том. Целевой том — это тот том, на который нужно импортировать экспортированные записи квот.
5. Как было описано ранее, откройте окно **Свойства** целевого тома. Перейдите на вкладку **Квота** и нажмите кнопку **Записи квот**. Откроется одноименное окно для целевого тома.
6. Выберите команду **Квота | Импорт** (Quota | Import). В окне **Параметры импорта квоты** (Import Quota Settings) выберите ранее сохраненный файл и нажмите кнопку **Открыть**.
7. Если том содержит предыдущие записи квот, можно либо заменить существующие записи, либо сохранить их. Нажмите кнопку **Да** для замены существующей записи или кнопку **Нет** для сохранения существующей записи. Для применения своего вы-

[1] Если вы в окне **Дисковая квота** не обрабатывали файлы пользователя, а просто нажали кнопку **Закрыть**, запись квоты удалена не будет. Место на диске распределяется для пользователя с учетной записью. Пока на диске есть файлы, принадлежащие учетной записи, запись квоты не может быть удалена. — *Прим. пер.*

бора ко всем записям квот установите флажок **Применить ко всем записям квот** (Do this for all quota entries), а затем нажмите кнопку **Да** или **Нет**.

Отключение дисковых квот NTFS

Отключить квоты можно для отдельных пользователей или для всех пользователей на томе. При отключении квоты для отдельного пользователя этот пользователь больше не является предметом ограничения квот, но дисковые квоты все еще отслеживаются для других пользователей. При отключении квот на томе отслеживание и управление квотами будут полностью удалены. Для отключения квот конкретного пользователя следуйте рекомендациям из *разд. "Просмотр записей квот" ранее в этой главе*. Для отключения отслеживания квот на всем томе выполните следующие действия:

1. Откройте оснастку **Управление компьютером** и при необходимости подключитесь к удаленному компьютеру.
2. Откройте окно **Свойства** для тома, на котором нужно отключить квоты NTFS.
3. На вкладке **Квота** установите флажок **Включить управление квотами**. Нажмите кнопку **ОК**. Когда увидите запрос, еще раз нажмите кнопку **ОК**.

> ***Внимание!***
>
> Отключение дисковых квот не удаляет существующие записи квот. Если позже дисковые квоты будут снова включены, будут применены ранее созданные записи квот.

Использование, настройка и управление квотами диспетчера ресурсов

Операционная система Windows Server 2012 R2 поддерживает расширенную систему управления квотами, называемую *дисковыми квотами диспетчера ресурсов* (Resource Manager disk quotas). Назначая эти квоты, администратор может управлять использованием дискового пространства папки и тома.

> ***Совет***
>
> Поскольку управление дисковыми квотами диспетчера ресурсов осуществляется отдельно от дисковых квот NTFS, можно настроить один том на использование обеих систем квотирования. Однако рекомендуется применять какую-то одну систему. Альтернативно, если уже настроены дисковые квоты NTFS, можно продолжить использовать их для ограничения дискового пространства на томах, а для важных папок задавать квоты диспетчера ресурсов.

Что такое дисковые квоты диспетчера ресурсов

При работе с Windows Server 2012 R2 можно использовать дисковые квоты диспетчера ресурсов — это еще один инструмент, который администратор может применять для управления использованием дискового пространства. Можно настроить квоты диспетчера ресурсов для ограничения дискового пространства тома или папки. Администратор устанавливает либо жесткий лимит — означает, что предел квоты не может быть превышен, либо мягкий лимит — предел квоты может быть превышен.

Вообще говоря, использовать жесткие лимиты необходимо, когда нужно запретить пользователям превышать определенное ограничение дискового пространства. Задавать мягкие лимиты нужно для простого контроля использования дискового пространства и предупреждения пользователей, которые превышают или собираются превысить квоты. У всех квот есть путь к основному файлу на томе или папке, к которому применена квота. Квота применяется к выбранному тому или папке и ко всем подпапкам выбранного тома или папки. В шаблоне квоты, определяющем свойства квоты, задается то, как квоты работают и как пользователи будут ограничены или предупреждены.

Шаблоны квот, имеющиеся в Windows Server 2012 R2, представлены в табл. 4.6. Используя утилиту **Диспетчер ресурсов файлового сервера** (File Server Resource Manager), можно легко определить дополнительные шаблоны, которые будут доступны при создании квот, или установить единожды свойства квот при определении квоты.

Шаблоны квот определяют следующее:

- предел — предел использования дискового пространства;
- тип квоты — жесткая или мягкая;
- порог уведомления — тип уведомления, возникающего при процентном превышении заданного предела.

Несмотря на то, что у каждой квоты есть определенный предел и тип, возможно определение нескольких порогов предупреждений. Порог предупреждения — процентное соотношение от порога квоты, которое меньше 100%. Например, можно инициировать предупреждения на 85 и 95% квоты и окончательное уведомление, когда будет достигнуто все 100% квоты.

Пользователи, которые вот-вот превысят предел или уже превысили его, могут быть автоматически уведомлены по электронной почте. Система уведомления также поддерживает уведомление администраторов по электронной почте, инициирование создания отчетов, запуск команд и журналирование событий.

Таблица 4.6. *Шаблоны дисковых квот*

Шаблон квоты	Предел	Тип квоты	Описание
Предел 100 Мбайт	100 Мбайт	Жесткая	Отправляет пользователям уведомления и не разрешает пользователям превышать предел
Предел 200 Мбайт с уведомлением пользователя	200 Мбайт	Жесткая	Отправляет отчет хранилища пользователям, превысившим предел
Предел 200 Мбайт с расширением 50 Мбайт	200 Мбайт	Жесткая	Использует команду `DIRQUOTA` для автоматического предоставления одноразового расширения в размере 50 Мбайт для пользователей, превысивших предел
Расширенный предел 250 Мбайт	250 Мбайт	Жесткая	Предназначен для тех пользователей, чей предел был расширен от 200 до 250 Мбайт
Наблюдение за томом размером 200 Гбайт	200 Гбайт	Мягкая	Наблюдает за использованием тома и предупреждает, когда будет превышен предел
Наблюдение за общим ресурсом размером 500 Мбайт	50 Мбайт	Мягкая	Наблюдает за использованием общего ресурса и предупреждает, когда будет превышен предел

Управление шаблонами квот

Шаблоны квот используются для определения свойств квоты, в том числе предела, типа квоты и порогов уведомлений. В утилите **Диспетчер ресурсов файлового сервера** можно просмотреть определенные в данный момент шаблоны квот, развернув узел **Управление квотами** и выбрав узел **Шаблоны квот**. В табл. 4.6 было представлено общее описание имеющихся шаблонов. В табл. 4.7 перечислены переменные, которые могут быть использованы для автоматического создания сообщений и событий.

Таблица 4.7. *Основные переменные, доступные для сообщений и событий дисковых квот*

Переменная	Описание
[Admin Email]	Вставляет электронные адреса администраторов, определенных в глобальных настройках
[File Screen Path]	Вставляет локальный путь к файлу, например, C:\Data
[File Screen Remote Path]	Вставляет удаленный путь, например, *\\server\share*
[File Screen System Path]	Вставляет канонический путь к файлу, например, *\\?\VolumeGUID*
[Server Domain]	Вставляет домен сервера, на котором произошло уведомление
[Server]	Вставляет имя сервера, на котором произошло уведомление
[Source File Owner]	Вставляет имя пользователя — владельца файла/папки
[Source File Owner Email]	Вставляет электронный адрес владельца файла/папки
[Source File Path]	Вставляет исходный путь к файлу/папке

Изменить существующие шаблоны квот можно так:

1. В утилите **Диспетчер ресурсов файлового менеджера** разверните узел **Управление квотами**, а затем выберите **Шаблоны квот**. Будут отображены определенные в данный момент шаблоны квот.
2. Чтобы модифицировать свойства шаблона квоты, дважды щелкните на нем. Откроется окно **Свойства шаблона квоты** (рис. 4.9).
3. На вкладке **Параметры** (Settings) можно установить имя шаблона, предел и тип квоты. Также выводятся определенные в данный момент пороги уведомления. Для изменения существующего порога уведомления выделите его и нажмите кнопку **Изменить**. Для определения нового порога нажмите кнопку **Добавить**.
4. Когда закончите изменять параметры шаблона, нажмите кнопку **OK** для сохранения параметров.

Создать новый шаблон можно с помощью этих действий:

1. В утилите **Диспетчер ресурсов файлового менеджера** разверните узел **Управление квотами**, а затем выберите **Шаблоны квот**.

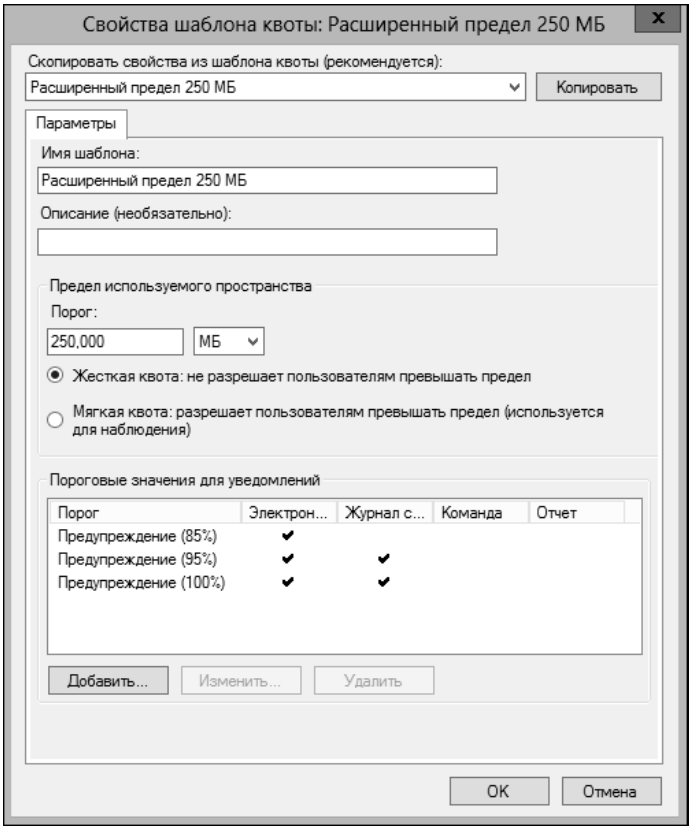


Рис. 4.9. Используйте свойства квоты для настройки предела, типа квоты и порогов уведомления

2. Из меню **Действие** или на панели **Действия** выберите команду **Создать шаблон квот** (Create Quota Template). Откроется окно **Создание шаблона квоты** (Create Quota Template).
3. На вкладке **Параметры** установите имя шаблона, предел и тип квоты. Сначала нужно установить порог используемого пространства, а затем задать дополнительные пороговые значения для уведомлений. В поле **Порог** (Limit) введите значение и укажите, в каких единицах будет измеряться предел — в килобайтах, мегабайтах, гигабайтах или терабайтах.
4. Нажмите кнопку **Добавить**, чтобы добавить пороговое значение для уведомлений. В окне **Добавление порога** (Add Threshold) введите значение в поле **Создавать уведомления, когда достигает (%)** (Generate notifications when usage reaches (%)). Процентное значение порога уведомления должно быть меньше 100. Предельный порог фиксируется, когда достигается 100% квоты.
5. На вкладке **Сообщение электронной почты** (E-Mail Message) можно настроить уведомления так.
   - Для уведомления администратора, что достигнут порог квоты, установите флажок **Отправить сообщения следующим администраторам** (Send e-mail to the

following administrators) и введите электронные адреса или адрес. Несколько адресов разделяются точкой с запятой. Используйте переменную `[Admin Email]`, чтобы указать администратора по умолчанию, ранее указанного в глобальных параметрах.

- Для уведомления пользователей установите флажок **Отправить сообщения пользователям, превысившим порог** (Send e-mail to the user who exceeded the threshold).
- Укажите содержимое письма уведомления в полях **Тема** (Subject) и **Текст сообщения** (Message body). В табл. 4.7 содержатся имена доступных переменных и их значения.

6. На вкладке **Журнал событий** (Event Log) можно настроить журналирование событий. Установите флажок **Записывать предупреждения в журнал событий** (Send Warning To Event Log) для включения журналирования и затем укажите текст записи журнала в поле **Запись журнала** (Log entry). В табл. 4.7 приведены доступные переменные и их описание.
7. На вкладке **Команда** (Command) можно указать команду или сценарий для запуска, аргументы, которые будут переданы этой команде или сценарию, и рабочий каталог. Контекст безопасности по умолчанию для команд — **Локальная служба** (Local Service), что гарантирует стандартный пользовательский доступ к ресурсам, но запрещает доступ к сетевым ресурсам. Если же команда требует, как локальные, так и сетевые ресурсы, можно запустить команду как сетевую службу (Network Service).
8. На вкладке **Отчет** (Report) установите флажок **Создать отчет** (Generate reports) для включения отчета об инциденте и затем выберите типы отчетов для создания. Отчеты по умолчанию сохраняются в папке *%SystemDrive%*\StorageReports\Incident, и они могут также быть отправлены назначенным администраторам. Используйте переменную `[Admin Email]`, чтобы указать администраторов по умолчанию, ранее заданных в глобальных параметрах.
9. Повторите действия 5–7 для определения дополнительных порогов уведомлений.
10. Нажмите кнопку **OK**, когда закончите создавать шаблон.

Создание квот диспетчера ресурсов

Чтобы просмотреть определенные в данный момент дисковые квоты, запустите утилиту **Диспетчер ресурсов файлового сервера** и разверните узел **Управление квотами**, а затем выберите узел **Квоты**. Перед определением дисковых квот нужно сначала определить группы файлов, к которым будут применяться квоты, и шаблоны квот, как было показано в *разд. "Управление шаблонами квот" ранее в этой главе*.

После определения необходимых групп файлов и шаблонов квот можно создать квоты так:

1. В утилите **Диспетчер ресурсов файлового сервера** разверните узел **Управление квотами**, а затем выберите узел **Квоты**.

2. Из меню **Действие** или из панели **Действия** выберите команду **Создать квоту**.
3. В окне **Создание квоты** укажите локальный путь для квоты, нажмите кнопку **Обзор** и затем, используя окно **Обзор папок**, укажите путь, например C:\Data. Нажмите кнопку **OK**.
4. В списке **Наследовать свойства из следующего шаблона** (Derive properties from this quota template) выберите шаблон квот, который будет использоваться.
5. Нажмите кнопку **Создать**.

ГЛАВА 5

Улучшение безопасности компьютера

Методы обеспечения безопасности важны для успешного системного администрирования. Существуют два ключевых способа сконфигурировать настройки безопасности: использование шаблонов безопасности и политик безопасности. Обеими функциями вы можете управлять посредством групповой политики.

Использование шаблонов безопасности

Шаблоны безопасности предоставляют централизованный способ управления настройками, связанными с безопасностью рабочих станций и серверов. Можно использовать шаблоны безопасности для применения их к определениям групповой политики на конкретных компьютерах.

Эти определения политики обычно влияют на следующие политики.

- **Политики учетных записей** (Account policies). Контролируют безопасность паролей, учетных записей пользователей и безопасность Kerberos.
- **Локальные политики** (Local policies). Управляют аудитом, назначением прав пользователям и другими настройками безопасности.
- **Политики протоколирования событий** (Event log policies). Управляют безопасностью для протоколирования событий.
- **Политики ограниченных групп** (Restricted groups policies). Управляют безопасностью локальной группы.
- **Политики системных служб** (System services policies). Контролируют безопасность и режим запуска локальных служб.
- **Политики файловой системы** (File system policies). Контролируют безопасность для файлов и папок локальной файловой системы.
- **Политики реестра** (Registry policies). Контролируют права доступа на ключах реестра, связанных с безопасностью.

Примечание

Шаблоны безопасности доступны во всех установках Microsoft Windows Server и могут быть импортированы в любой объект групповой политики. Шаблоны безопасности применяются только к области **Конфигурация компьютера** (Computer Configuration) групповой политики. Они не действуют на область **Конфигурация пользователя** (User Configuration). В групповой политике находятся применяемые параметры в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности** (Computer Configuration\Windows Settings\Security Settings). Некоторые параметры безопасности не включены, например, те, которые применяются к беспроводным сетям, публичным ключам, ограничениям программного обеспечения и IP-безопасности.

Работа с шаблонами безопасности — сложный процесс, состоящий из следующих шагов:

1. Используйте оснастку **Шаблоны безопасности** (Security Templates) для создания нового шаблона или выбора существующего шаблона, который нужно изменить.
2. Используйте оснастку **Шаблоны безопасности** для внесения необходимых изменений в настройки шаблона и для сохранения изменений.
3. Используйте оснастку **Анализ и настройка безопасности** (Security Configuration And Analysis) для анализа различий между выбранным шаблоном и текущими настройками компьютерной безопасности.
4. При необходимости пересмотрите шаблон после того, как найдете различия между настройками шаблона и текущими настройками компьютера.
5. Используйте оснастку **Анализ и настройка безопасности** для применения шаблона и перезаписи существующих настроек безопасности.

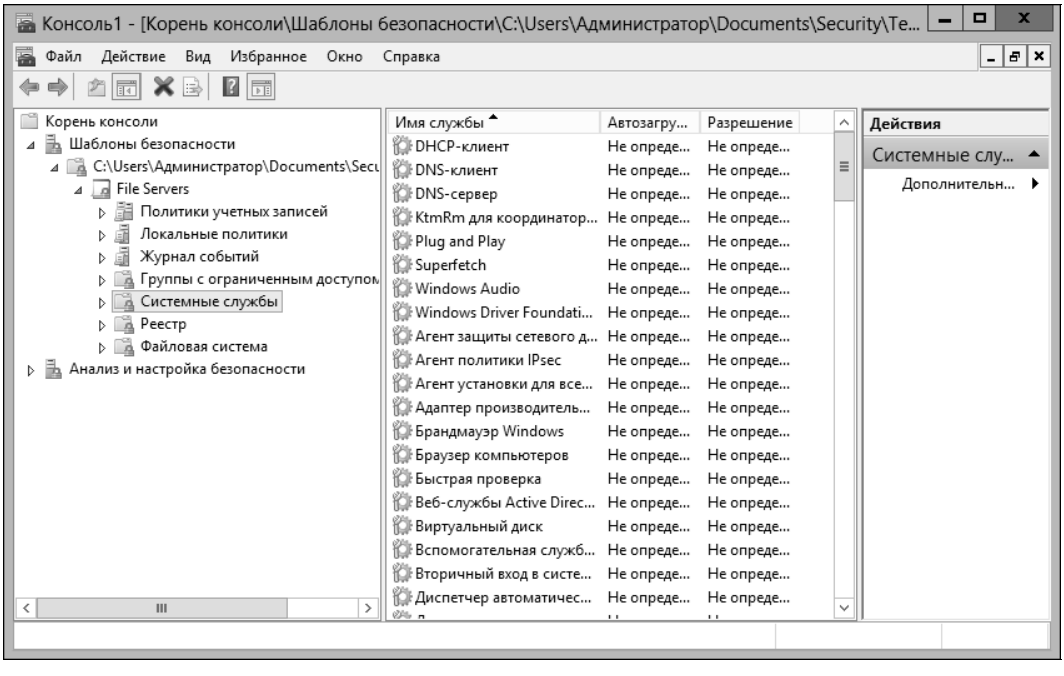


Рис. 5.1. Просмотрите и создайте шаблоны безопасности с помощью оснастки **Шаблоны безопасности**

При работе с шаблонами безопасности нужно определить, можно ли использовать существующий шаблон в качестве отправной точки. Другие администраторы, возможно, тоже создали шаблоны или у организации есть базовые шаблоны, которые нужно использовать. Также можно создать новый шаблон и принять его в качестве начальной точки (рис. 5.1).

> ***Совет***
>
> При выборе шаблона, который нужно использовать в качестве начальной точки, необходимо пройти через каждую установку, которую применяет шаблон. Оцените, как эта установка влияет на среду. Если установка нецелесообразна, нужно изменить или удалить ее.

Не используйте оснастку **Шаблоны безопасности** для применения шаблонов. Для этого нужно использовать оснастку **Анализ и настройка безопасности**. Она также применяется для сравнения настроек шаблона с текущими настройками компьютера. Результаты анализа указывают, где текущие настройки не соответствуют настройкам в шаблоне.

Использование оснасток *Шаблоны безопасности* и *Анализ и настройка безопасности*

Для открытия оснастки **Шаблоны безопасности** выполните следующие действия:

1. Запустите консоль управления Microsoft (MMC). Один из способов сделать это — нажать клавишу <Windows>, ввести `mmc.exe` и нажать клавишу <Enter>.
2. В консоли управления выберите команду **Файл | Добавить или удалить оснастку** (File | Add/Remove Snap-In).
3. В окне **Добавление и удаление оснасток** (Add Or Remove Snap-Ins) выберите оснастку **Шаблоны безопасности** и нажмите кнопку **Добавить**.
4. Выберите оснастку **Анализ и настройка безопасности**, нажмите кнопку **Добавить**, а потом кнопку **OK**.

По умолчанию оснастка **Шаблоны безопасности** ищет шаблоны в каталоге *%SystemDrive%*\Users*%UserName%*\Documents\Security\Templates. Можно добавить другие пути для поиска шаблонов с помощью следующих действий:

1. Выберите оснастку **Шаблоны безопасности** в MMC, в меню **Действие** (Action) выберите команду **Новый путь для поиска шаблонов** (New Template Search Path).
2. В окне **Обзор папок** (Browse For Folder) выберите папку с шаблонами, например *%SystemRoot%*\Security\Templates\Policies, и нажмите кнопку **OK**.

Теперь местоположение для поиска шаблонов определено, выберите шаблон и просмотрите его настройки.

Создать новый шаблон можно так:

1. В оснастке **Шаблоны безопасности** щелкните правой кнопкой мыши по пути, в котором нужно создать шаблон, и выберите команду **Создать шаблон** (New Template).
2. Введите имя и описание шаблона в появившемся окне.

3. Нажмите кнопку **OK** для создания шаблона. Будет создан шаблон, но ни один из параметров не будет настроен, поэтому нужно внимательно настроить шаблон перед его использованием.
4. После изменения настроек шаблона щелкните на его названии и выберите команду **Сохранить** (Save). Либо можно использовать команду **Сохранить как** (Save As), чтобы назначить шаблону новое имя.

Просмотр и изменение настроек шаблона

В следующих разделах рассказывается, как работать с настройками шаблона. Вы увидите, что способы управления шаблонами разных типов немного отличаются.

Изменение настроек для политики учетных записей, локальных политик и журнала событий

Настройки политики учетных записей контролируют безопасность паролей, блокировки учетных записей, а также безопасность Kerberos. Параметры локальных политик контролируют безопасность для аудита, назначения прав пользователям и другие параметры безопасности. Параметры журнала событий контролируют его безопасность. Подробно параметры политик учетных записей и локальных политик будут обсуждаться в *главе 8*, а параметры журналирования уже были рассмотрены в *главе 3*.

Настройки политики учетных записей, локальных политик и журнала безопасности можно изменить с помощью следующих действий:

1. В оснастке **Шаблоны безопасности** разверните узел **Политики учетных записей** (Account Policies), **Локальные политики** (Local Policies) или **Журнал событий** (Event Log). А затем выберите соответствующий подузел, например **Политика паролей** (Password Policy) или **Политика блокировки учетной записи** (Account Lockout Policy).
2. На правой панели в алфавитном порядке выводятся параметры политики. Значение в колонке **Параметр компьютера** (Computer Setting) отображает текущее значение. Если шаблон изменяет настройки так, что политика больше не определена, в этой колонке будет значение **Не определено** (Not Defined).
3. Дважды щелкните на параметре, чтобы отобразить окно **Свойства** (рис. 5.2). Для определения назначения параметра перейдите на вкладку **Объяснение** (Explain). Для определения политики в шаблоне включите флажок **Определить следующий параметр политики в шаблоне** (Define this policy setting in the template). Для отмены применения политики снимите этот флажок.
4. При включении настройки политики укажите ее значение и любые другие дополнительные параметры.
5. Нажмите кнопку **OK** для сохранения изменений. Будет открыто окно **Предлагаемые изменения значений** (Suggested Value Changes), показанное на рис. 5.3. Это окно информирует о других значениях, которые модифицированы на основании измененных значений. Например, при изменении настройки **Пороговое значение**

блокировки (Account lockout threshold) Windows также может изменить настройки **Продолжительность блокировки учетной записи** (Account lockout duration) и **Время до сброса счетчика блокировки** (Reset account lockout counter after).

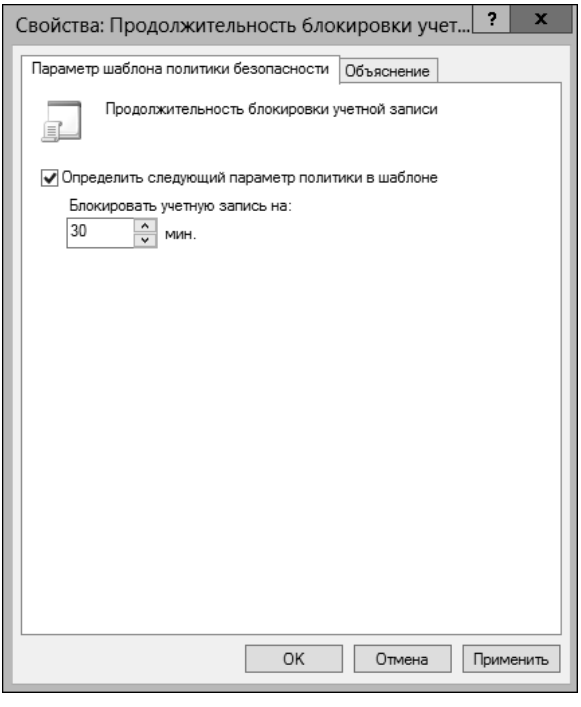


Рис. 5.2. Изменение настроек шаблона для учетных записей и локальных политик

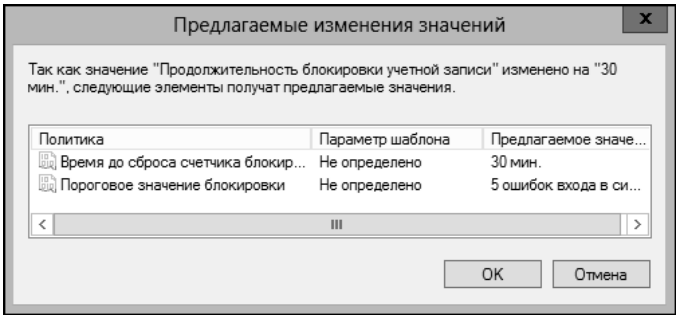


Рис. 5.3. Предлагаемые изменения значений

Настройка групп с ограниченным доступом

Настройки политики групп с ограниченным доступом управляют списком членов групп, а также группами, к которым принадлежит настроенная группа. Настроить ограниченную группу можно так:

1. В оснастке **Шаблоны безопасности** выберите узел **Группы с ограниченным доступом** (Restricted Groups). На правой панели будут отображены уже настроенные

группы с ограниченным доступом в алфавитном порядке. Также будут перечислены члены группы.

2. Для добавления ограниченной группы щелкните правой кнопкой мыши по узлу **Группы с ограниченным доступом** и выберите команду **Добавить группу** (Add Group). В окне **Добавление группы** (Add Group) нажмите кнопку **Обзор**.
3. В окне **Выбор: "Группы"** (Select Groups) введите группу, которую нужно ограничить, или нажмите кнопку **Проверить имена** (Check Names). Если будет найдено несколько совпадений, выберите учетную запись, которую нужно использовать, и затем нажмите кнопку **OK**. Если совпадения не будут найдены, измените введенное имя и попытайтесь поискать снова. Повторите этот шаг столько раз, сколько будет необходимо, а затем нажмите кнопку **OK**.
4. В окне **Свойства** (рис. 5.4) можно использовать кнопку **Добавить членов группы** (Add Members) для добавления членов в группу. Нажмите эту кнопку, а затем укажите членов группы. Если в группе не должно быть никаких членов, выделите всех членов и нажмите кнопку **Удалить** (Remove). Любые члены, которые не определены в установке политики для ограниченной группы, будут удалены при применении шаблона безопасности.
5. В окне **Свойства** нажмите кнопку **Добавить группы** (Add Groups) для указания групп, к которым эта группа будет принадлежать. Если не определить членство в группах, группы, которым принадлежит эта группа, не будут изменены при применении шаблона.
6. Нажмите кнопку **OK** для сохранения настроек.

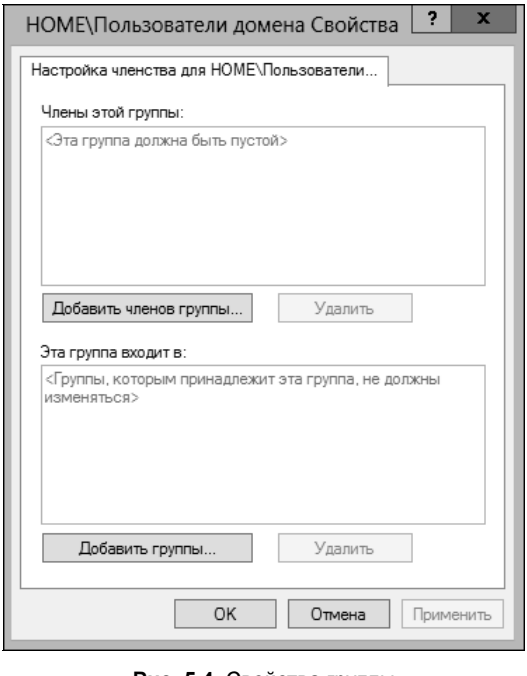


Рис. 5.4. Свойства группы

Для удаления ограниченной группы выполните эти действия:

1. В оснастке **Шаблоны безопасности** (Security Templates) выберите узел **Группы с ограниченным доступом** (Restricted Groups). На панели справа в алфавитном порядке будут выведены группы. Члены группы будут выведены напротив имени группы.
2. Щелкните правой кнопкой мыши (или нажмите и удерживайте имя группы пальцем) и выберите команду **Удалить** (Delete). Когда вас попросят подтвердить действие, нажмите кнопку **Да**.

Включение, отключение и настройка системных служб

Настройки политики для системных служб контролируют общую безопасность и режим запуска локальных служб. Можно включить, выключить и настроить системные службы:

1. В оснастке **Шаблоны безопасности** выберите узел **Системные службы** (System Services). На панели справа будут отображены установленные в данный момент службы, выводится имя службы, тип запуска и настройка разрешений. Когда работаете со службами, помните следующее:
   - если шаблон не изменяет тип запуска службы, в колонке **Автозагрузка** (Startup) выводится **Не определено** (Not Defined). В противном случае выводится одно из следующих значений: **автоматический** (Automatic), **вручную** (Manual), **запрещен** (Disabled);
   - если шаблон не изменяет конфигурацию безопасности службы, в колонке **Разрешение** (Permission) выводится значение **Не определено** (Not Defined). В противном случае выводится **Настроено** (Configured).
2. Дважды щелкните по записи службы, чтобы открыть ее окно **Свойства** (рис. 5.5). Чтобы определить и применить параметры политики, установите флажок **Определить следующий параметр политики в шаблоне** (Define this policy setting in the template). Для очистки политики и отмены ее применения снимите этот флажок.
3. При включении настройки политики укажите тип запуска службы: **автоматический**, **вручную**, **запрещен**. Помните следующее:
   - **автоматический** (Automatic) — гарантирует, что служба будет запущена автоматически при запуске операционной системы. Выберите эту установку для важных служб, которые точно безопасны. Эти службы будут запущены на всех компьютерах, к которым применяется шаблон безопасности, если, конечно, службы установлены на этих компьютерах;
   - **вручную** (Manual) — предотвращает автоматический запуск службы, но разрешает запуск службы вручную пользователем, приложением или другой службой. Выберите эту установку, когда необходимо ограничить ненужные, неиспользуемые либо не совсем безопасные службы;
   - **запрещен** (Disabled) — предотвращает запуск службы, автоматический или ручной. Выберите эту установку для службы, запуск которой нужно запретить.

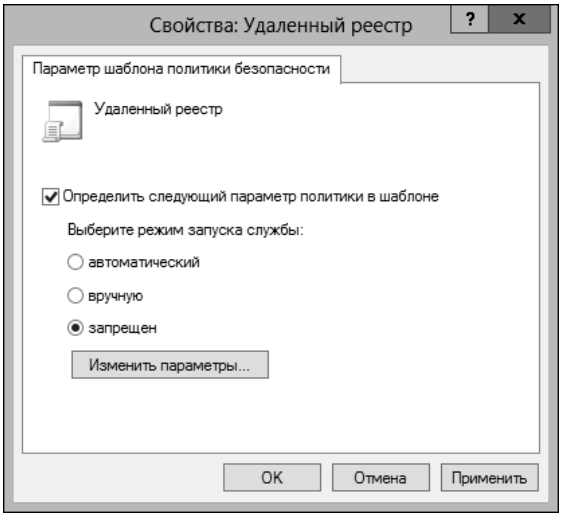


Рис. 5.5. Изменяем настройки шаблона для системных служб

4. Если надо изменить (или просто просмотреть) конфигурацию безопасности, нажмите кнопку **Изменить параметры** (Edit Security). Появится окно **Безопасность для** (Security For), где можно установить разрешения для определенных пользователей и групп, которые могут запускать, останавливать и приостанавливать службу на компьютере.
5. Нажмите кнопку **OK**.

Настройка параметров безопасности для реестра и файловой системы

Настройки политик для файловой системы контролируют безопасность для файлов и папок в локальной файловой системе. Параметры политик для реестра контролируют значения ключей реестра, связанных с безопасностью. Можно просмотреть или изменить параметры для определенных в данный момент ключей реестра и путей файловой системы с помощью следующих действий:

1. В оснастке **Шаблоны безопасности** выберите узел **Реестр** (Registry) или **Файловая система** (File System) в зависимости от того, с чем нужно работать. На правой панели будет выведен список всех защищенных путей.
2. Дважды щелкните на пути реестра или файловой системы для просмотра его параметров (рис. 5.6).
3. Чтобы убедиться, что путь или ключ не заменяется, установите переключатель **Запретить замену разрешений в этом разделе** (Do not allow permissions on this key to be replaced), а затем нажмите кнопку **OK**. Пропустите оставшиеся шаги этой процедуры.
4. Чтобы заменить разрешения, установите переключатель **Настроить этот раздел** (Configure this key then), а затем одну из двух опций:
   - **Распространить наследуемые разрешения на все подразделы** (Propagate inheritable permissions to all subkeys) — выберите эту опцию для применения всех

наследуемых разрешений к этому пути реестра или файловой системы и ко всем вложенным путям реестра/файловой системы. Существующие разрешения будут заменены только, если они конфликтуют с разрешениями безопасности для этого пути;

- **Заменить текущие разрешения во всех подразделах наследуемыми** (Replace existing permissions on all subkeys with inheritable permissions) — выберите эту опцию для замены всех существующих разрешений для этого пути реестра или пути файловой системы и для всех вложенных путей реестра или путей файловой системы. Любые существующие разрешения будут удалены, останутся только текущие разрешения.

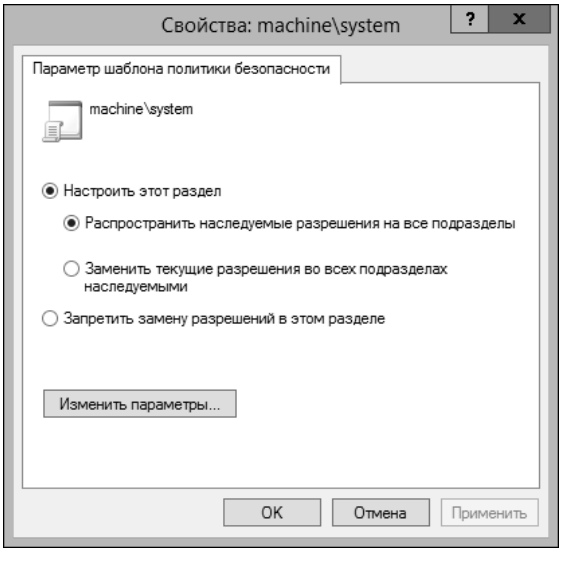


Рис. 5.6. Измените параметры шаблона для файлов и ключей реестра

5. Нажмите кнопку **Изменить параметры** (Edit Security). В окне **Безопасность для** (Security For) приводятся настройки разрешения безопасности для пользователей и групп. Установка разрешений подобна аналогичной процедуре для файлов/папок на файловой системе NTFS (подробности *см. в главе 3)*.
6. Нажмите кнопку **OK** дважды для сохранения изменений.

Определить параметры безопасности для ключей реестра можно следующим образом:

1. В оснастке **Шаблоны безопасности** щелкните правой кнопкой мыши по узлу **Реестр** и выберите команду **Добавить раздел** (Add Key). На экране появится окно **Выбор раздела реестра** (Select Registry Key), изображенное на рис. 5.7.
2. Выберите раздел или значение, с которым нужно работать, и нажмите кнопку **OK**. Записи в разделе `CLASSES_ROOT` относятся к разделу `HKEY_CLASSES_ROOT`. Записи в разделе `MACHINE` — к разделу `HKEY_LOCAL_MACHINE`, а записи в разделе `USERS` — к `HKEY_USERS`.
3. В окне **Безопасность базы данных для** (Database Security For) настройте разрешения безопасности для пользователей и групп. Разрешения безопасности устанавли-

ваются так же, как и для файлов/папок при использовании NTFS. Более детальные сведения приводятся в *главе 3*.

4. Нажмите кнопку **OK**. На экране появится окно **Добавление объекта** (Add Object). Чтобы убедиться, что разрешения раздела не заменяются, выберите переключатель **Запретить замену разрешений в этом разделе** (Do not allow permissions on this key to be replaced) и затем нажмите кнопку **OK**. Пропустите оставшуюся часть данной процедуры.

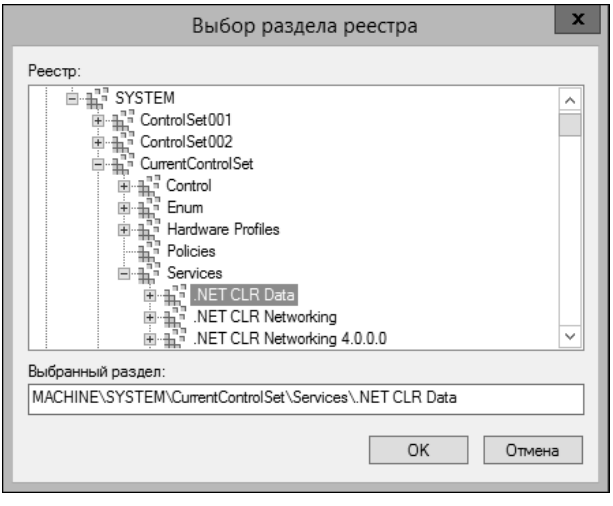


Рис. 5.7. Выберите раздел или значение реестра для его защиты

5. Чтобы настроить разрешения, выберите переключатель **Настроить этот раздел** (Configure this key then), а затем одну из двух опций:
   - **Распространить наследуемые разрешения на все подразделы** (Propagate inheritable permissions to all subkeys) — выберите эту опцию для применения всех наследуемых разрешений к этому пути реестра и ко всем вложенным путям реестра. Существующие разрешения будут заменены только, если они конфликтуют с разрешениями безопасности для этого пути;
   - **Заменить текущие разрешения во всех подразделах наследуемыми** (Replace existing permissions on all subkeys with inheritable permissions) — выберите эту опцию для замены всех существующих разрешений для этого пути реестра и для всех вложенных путей. Любые существующие разрешения будут удалены, останутся только текущие разрешения.
6. Нажмите кнопку **OK**.

Определить параметры безопасности для файловой системы можно следующим образом:

1. В оснастке **Шаблоны безопасности** щелкните правой кнопкой мыши по узлу **Файловая система** и выберите команду **Добавить файл**. На экране появится окно **Добавление файла или папки** (Add a file or folder), изображенное на рис. 5.8.

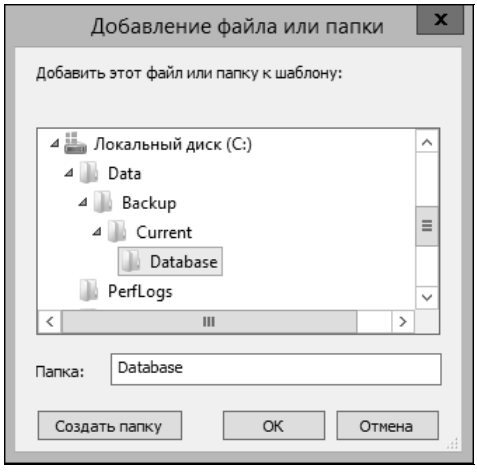


Рис. 5.8. Выберите файл или папку для защиты

2. В окне **Добавление файла или папки** выберите файл или папку, с которым нужно работать, и затем нажмите кнопку **OK**.
3. В окне **Безопасность базы данных для** (Database Security For) настройте разрешения безопасности для пользователей и групп. Разрешения безопасности устанавливаются так же, как и для файлов/папок при использовании NTFS. Более подробные сведения приводятся в *главе 3*.
4. Нажмите кнопку **OK**. На экране появится окно **Добавление объекта**. Чтобы убедиться, что разрешения пути не заменяются, выберите переключатель **Запретить замену разрешений для этого файла или папки** (Do not allow permissions on this file or folder to be replaced) и затем нажмите кнопку **OK**. Пропустите оставшуюся часть данной процедуры.
5. Чтобы настроить разрешения, выберите **Настроить разрешения для этого файла или папки** (Configure this path then), а затем одну из двух опций:
   - **Распространить наследуемые разрешения на все подпапки и файлы** (Propagate inheritable permissions to all subfolders) — выберите эту опцию для применения всех наследуемых разрешений к этому пути файловой системы и ко всем вложенным путям. Существующие разрешения будут заменены только, если они конфликтуют с разрешениями безопасности для этого пути;
   - **Заменить существующие разрешения для всех подпапок и файлов на наследуемые разрешения** (Replace existing permissions on all subfolders with inheritable permissions) — выберите эту опцию для замены всех существующих разрешений для этого пути файловой системы и для всех вложенных путей файловой системы. Любые существующие разрешения будут удалены, останутся только текущие разрешения.
6. Нажмите кнопку **OK**.

Анализ, просмотр и применения шаблонов безопасности

Как было указано ранее, оснастка **Анализ и настройка безопасности** используется для применения шаблонов и для их сравнения с текущими настройками компьютера. Использование шаблона позволяет удостовериться, что параметры шаблона были применены к конфигурации компьютера. Сравнение настроек может помочь идентифицировать любые несоответствия между тем, что реализовано в настоящее время и что определено в шаблоне безопасности. Это может также быть полезно для определения, изменялись ли настройки безопасности в течение долгого времени.

> ***Практический совет***
>
> Основной недостаток использования оснастки **Анализ и настройка безопасности** в том, что нельзя сконфигурировать несколько компьютеров сразу. Настроить безопасность можно только на том компьютере, на котором запущена оснастка. Если нужно использовать этот инструмент, чтобы развернуть конфигурации безопасности, следует войти в систему и запустить ее на каждом компьютере. Этот метод нормально работает на автономных компьютерах, но является далеко не оптимальным в домене. В домене необходимо импортировать настройки шаблонов в объект групповой политики (GPO) и затем развернуть конфигурацию безопасности сразу на множестве компьютеров. Об этом мы поговорим позже.

Оснастка **Анализ и настройка безопасности** использует базу данных для хранения настроек шаблона безопасности и затем применяет настройки из этой базы данных. Для анализа и сравнения настройки шаблона перечислены как настройки базы данных, а конфигурация компьютера — как настройки компьютера. Имейте в виду, что при активном редактировании шаблона в оснастке **Шаблоны безопасности** нужно сохранить шаблон, чтобы изменения могли быть проанализированы и использованы.

После создания шаблона (или выбора существующего шаблона) можно проанализировать и затем настроить шаблон следующим образом:

1. Откройте оснастку **Анализ и настройка безопасности**.
2. Щелкните правой кнопкой мыши на узле **Анализ и настройка безопасности**, затем выберите команду **Открыть базу данных** (Open Database). Будет открыто одноименное окно.
3. По умолчанию путь в появившемся окне будет установлен в *%SystemDrive%*\Users*%UserName%*\Documents\Security\Database. При необходимости смените каталог. В поле **Имя файла** (File Name) введите описательное имя базы данных, например `Текущее сравнение конфигурации`, и нажмите кнопку **Открыть** (Open). База данных безопасности будет создана в формате Security Database Files (расширение sdb).
4. Откроется окно **Импорт шаблона** (Import Template). По умолчанию путь для поиска шаблонов — *%SystemDrive%*\Users*%UserName%*\Documents\Security\Templates. При необходимости можно перейти в другую папку. Выберите шаблон безопасности, который нужно использовать, и нажмите кнопку **Открыть**. Файл шаблона безопасности имеет расширение inf.
5. Щелкните правой кнопкой мыши по узлу **Анализ и настройка безопасности** и выберите команду **Анализ компьютера** (Analyze Computer Now). Когда оснастка попросит установить путь для журнала, нажмите кнопку **OK**, чтобы использовать путь по умолчанию.

6. Дождитесь, пока оснастка выполнит анализ шаблона. Если во время анализа произойдет ошибка, можно просмотреть журнал ошибок, щелкнув правой кнопкой мыши по узлу **Анализ и настройка безопасности** и выбрав команду **Показать файл журнала** (View Log File).

При работе с оснасткой **Анализ и настройка безопасности** можно просмотреть, чем отличаются друг от друга настройки шаблона и текущие настройки компьютера. Как показано на рис. 5.9, настройки шаблона выводятся в колонке **Параметр базы данных** (Database Setting), а настройки компьютера — в колонке **Параметр компьютера** (Computer Setting). Если настройка не анализируется, выводится значение **Не определено** (Not Defined).

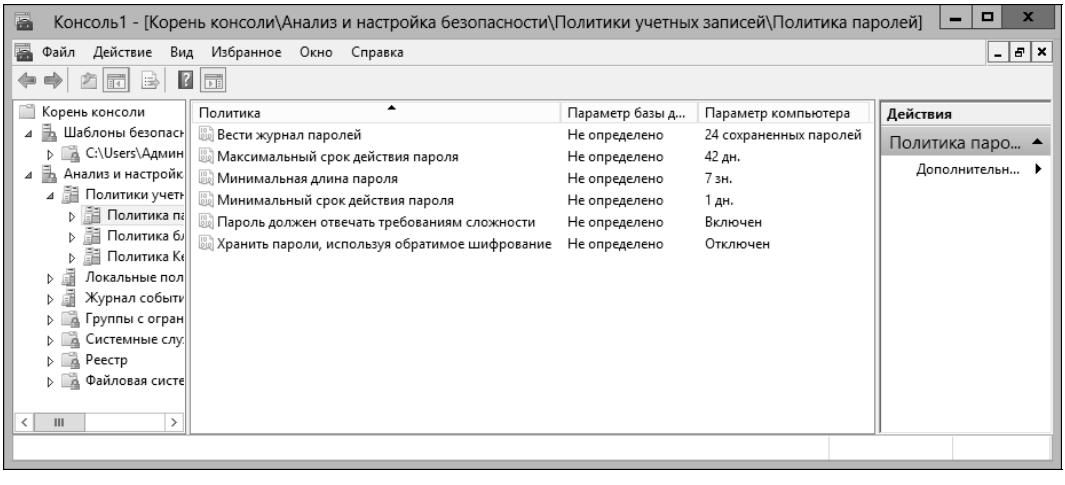


Рис. 5.9. Просмотрите разницу между настройками шаблона и компьютера

Внести изменения в базу данных (т. е. изменить значение в колонке **Параметр базы данных**) можно следующим образом:

1. В оснастке **Анализ и настройка безопасности** дважды щелкните на значении, которое нужно изменить.
2. В окне **Свойства** (рис. 5.10) выводится текущее значение, установленное в настройках компьютера. Если назначение параметра непонятно, перейдите на вкладку **Объяснение** (Explain).
3. Для определения значения политики установите флажок **Определить следующую политику в базе данных** (Define this policy in the database). Для очистки политики и отмены ее применения сбросьте этот флажок.
4. При включении настройки политики укажите, как значение политики должно использоваться, задав любые дополнительные параметры.
5. При необходимости повторите этот процесс. Для сохранения изменений в базе данных щелкните правой кнопкой мыши по узлу **Анализ и настройка безопасности** и выберите команду **Сохранить**.

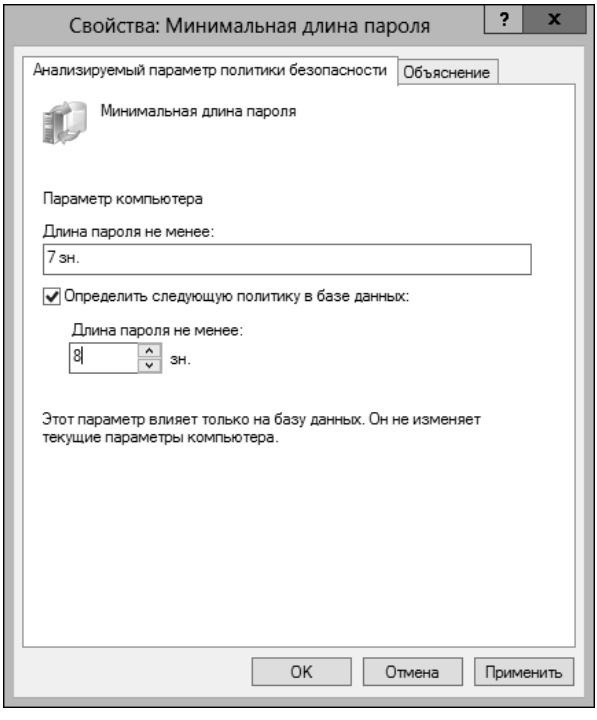


Рис. 5.10. Изменяем настройку политики в базе данных перед применением шаблона

Для анализа, просмотра и применения шаблонов безопасности также можно использовать утилиту командной строки Secedit. Подход следующий:

1. Откройте окно командной строки с правами администратора.
2. Используйте команду `Secedit /Import` для импорта шаблона безопасности в базу данных.
3. Используйте команду `Secedit /Analyze` для сравнения шаблона безопасности с параметрами компьютера.
4. Используйте команду `Secedit /Configure` для применения шаблона безопасности.

Независимо от того, используется ли мастер с графическим интерфейсом или утилита командной строки, необходимо создать шаблон отката перед применением любых настроек. *Шаблон отката* — это обратный шаблон, позволяющий удалить большинство настроек, которые использовались с шаблоном. Настройки, которые не могут быть удалены, — списки управления доступом (ACL) для файловой системы и реестра.

Создать шаблон отката можно с помощью утилиты Secedit, запустив ее в командной строке с правами администратора. Введите команду:

```
secedit /generaterollback /db DatabaseName /cfg TemplateName /rbk RollBackName /log LogName
```

Где *DatabaseName* — имя новой базы данных, которая будет использоваться для создания отката, а *TemplateName* — имя существующего шаблона безопасности, для которого создается шаблон отката. Параметр *RollBackName* устанавливает имя нового шаблона без-

опасности, в котором будут храниться обратные настройки, а *LogName* — имя журнала, который будет использоваться для отслеживания состояния процесса отката.

В следующем примере создается шаблон отката для шаблона "File Servers":

```
secedit /generaterollback /db rollback.db /cfg
"file servers.inf" /rbk fs-orig.inf /log rollback.log
```

Когда будете готовы применить шаблон, щелкните правой кнопкой мыши по узлу **Анализ и настройка безопасности** и выберите команду **Настроить компьютер** (Configure Computer Now). Когда оснастка попросит ввести путь к журналу ошибок, нажмите кнопку **OK** для использования пути по умолчанию. Для просмотра журнала ошибок щелкните правой кнопкой мыши по узлу **Анализ и настройка безопасности** и выберите команду **Показать файл журнала** (View Log File). Обратите внимание на любую проблему и примите соответствующие меры.

Если перед применением шаблона безопасности создан шаблон отката, можно восстановить настройки компьютера в предыдущее состояние. Для применения шаблона отката выполните следующие действия:

1. В оснастке **Анализ и настройка безопасности** щелкните правой кнопкой мыши на узле **Анализ и настройка безопасности** и выберите команду **Импорт шаблона** (Import Template).
2. В одноименном окне **Импорт шаблона** выберите шаблон отката.
3. Установите флажок **Очистить эту базу данных** (Clear This Database Before Importing) перед импортом и нажмите кнопку **Открыть**.
4. Щелкните правой кнопкой мыши по узлу **Анализ и настройка безопасности** и выберите команду **Настроить компьютер**. Нажмите кнопку **OK**.

Не могут быть восстановлены только списки контроля доступа для файловой системы и реестра. Как только разрешения файловой системы или реестра было применено, этот процесс обратить автоматически нельзя — придется все редактировать вручную.

Развертывание шаблонов безопасности на нескольких компьютерах

Вместо применения шаблона безопасности к каждому компьютеру отдельно можно развернуть конфигурацию безопасности сразу на множестве компьютеров с помощью групповой политики. Чтобы сделать это, нужно импортировать шаблон безопасности в GPO, обрабатываемый компьютерами, к которым должны примениться настройки шаблона. Затем, при обновлении политики, все компьютеры в рамках GPO получат конфигурацию безопасности.

Шаблоны безопасности применяются только к разделу **Конфигурация компьютера** (Computer Configuration) групповой политики. Перед развертыванием конфигурации безопасности нужно внимательно изучить структуру домена и организационного подразделения компании и при необходимости внести изменения и убедиться, что конфигурация безопасности применена только к соответствующим типам компьютеров. По существу это означает, что необходимо создать организационные подразделения для разных типов компьютеров в организации, а затем переместить учетные записи ком-

пьютеров в соответствующие организационные подразделения. Позже нужно создать и связать GPO с каждым организационным подразделением. Например, можно создать следующие организационные подразделения:

- Domain Controllers — организационное подразделение для контроллеров домена вашего предприятия. Это организационное подразделение создается в домене автоматически;
- Hight-Security Member Servers — организационное подразделение для рядовых серверов, требующих более высокого уровня безопасности;
- Member Server — организационное подразделение для рядовых серверов с обычными настройками безопасности;
- High-Security User Workstations — организационное подразделение для рабочих станций, требующих более высокого уровня безопасности;
- User Workstations — организационное подразделение для рабочих станций, требующих стандартных настроек безопасности;
- Remote Access Computers — организационное подразделение для компьютеров, получающих удаленный доступ к сети предприятия;
- Restricted Computers — организационное подразделение для компьютера с ограниченным доступом, например компьютеры в лаборатории.

> ***Практический совет***
>
> Нужно быть предельно осторожным при развертывании шаблонов безопасности с помощью GPO. Если у вас до этого не было подобной практики, потренируйтесь сначала на тестовом окружении, а затем убедитесь, что научились откатывать назад настройки, сделанные шаблоном безопасности. Если создать GPO и связать его с соответствующим уровнем в структуре Active Directory, можно восстановить компьютеры в их исходное состояние путем удаления ссылки на GPO. Поэтому чрезвычайно важно создать и связать новый GPO, а не использовать существующий GPO.

Для развертывания шаблона безопасности в GPO компьютера выполните следующие действия:

1. После настройки шаблона безопасности и его тестирования откройте ранее созданный GPO и свяжите его с соответствующим уровнем структуры Active Directory. В редакторе групповой политики разверните узел **Конфигурация компьютера\ Конфигурация Windows\Параметры безопасности** (Computer Configuration\ Windows Settings\Security Settings).
2. Щелкните правой кнопкой мыши на узле **Параметры безопасности** (Security Settings) и выберите команду **Импорт политики** (Import Policy).
3. В окне **Импорт политики из** (Import Policy From) выберите шаблон безопасности и нажмите кнопку **Открыть**. У файлов шаблонов безопасности расширение inf.
4. Проверьте состояние конфигурации настроек безопасности и убедитесь, что настройки были импортированы, как ожидалось, а затем закройте окно редактора политики. Повторите этот процесс для каждого шаблона безопасности и настроенного GPO компьютера. По умолчанию понадобится 90–120 минут для того, чтобы настройки групповой политики вступили в силу.

Использование мастера настройки безопасности

Мастер настройки безопасности может помочь в создании и применении всесторонней политики безопасности. Политика безопасности — XML-файл, который можно использовать для настройки служб, сетевой безопасности, значений реестра и политик аудита. Поскольку политика безопасности основывается на роли и на компоненте, обычно нужно создать отдельную политику для каждой из стандартных конфигураций сервера. Например, если организация использует контроллеры домена, файловые серверы и серверы печати, можно создать отдельные политики для каждого из этих типов серверов. Если у организации есть почтовые серверы, серверы баз данных и объединенные серверы (файловый сервер и серверы печати), а также контроллеры доменов, нужно создать отдельные политики, адаптированные в соответствии с этими типами серверов.

Мастер настройки безопасности (Security Configuration Wizard) можно использовать для выполнения следующих операций:

- создания политики безопасности;
- редактирования политики безопасности;
- применения политики безопасности;
- отмены последней примененной политики безопасности.

Политика безопасности может состоять из одного или более шаблонов безопасности. Как и в случае с шаблонами безопасности, можно применить политику безопасности к локальному компьютеру с помощью мастера настройки безопасности (Security Configuration Wizard). Посредством групповой политики можно применить политику безопасности к множеству компьютеров сразу. По умолчанию политика безопасности, создаваемая мастером настройки безопасности, сохраняется в папке *%SystemRoot%*\security\msscw\Policies.

В дополнение к мастеру с графическим интерфейсом можно применять утилиту командной строки Scwcmd (Scwcmd.exe): используйте команду `Scwcmd Analyze` для определения, соответствует ли компьютер политике безопасности, и `Scwcmd Configure` для применения политики безопасности.

Создание политик безопасности

Утилита **Мастер настройки безопасности** (Security Configuration Wizard) позволяет настроить политику только для ролей и компонентов, установленных на компьютере на момент запуска мастера. Пошаговый процесс создания политики определяет роли сервера и компоненты на текущем компьютере. Однако общие разделы конфигурации, представленные в мастере, одинаковы независимо от конфигурации компьютера.

У мастера настройки безопасности есть следующие разделы конфигурации:

- **Настройка служб на основе ролей** (Role-Based Service Configuration) — настраивает режим запуска системных служб на основе установленных ролей, компонентов, опций и требуемых служб;

- **Сетевая безопасность** (Network Security) — настраивает правила входящих и исходящих соединений для Брандмауэра Windows в режиме расширенной конфигурации;
- **Параметры реестра** (Registry Settings) — настраивает протоколы, используемые для взаимодействия с другими компьютерами на основе установленных ролей и компонентов;
- **Политика аудита** (Audit Policy) — настраивает аудит на выбранном сервере в соответствии с вашими предпочтениями;
- **Сохранение политики безопасности** (Save Security Policy) — позволяет сохранить и просмотреть политику безопасности. Также можно добавить один или более шаблонов безопасности.

Создать политику безопасности можно следующим образом:

1. Запустите мастер настройки безопасности. В диспетчере серверов выберите команду **Средства | Мастер настройки безопасности** (Tools | Security Configuration Wizard). На странице приветствия мастера нажмите кнопку **Далее**.
2. На странице **Действие настройки** (Configuration Action) выберите нужное действие (рис. 5.11). По умолчанию выбран переключатель **Создать новую политику безопасности** (Create a new security policy). Нажмите кнопку **Далее**.

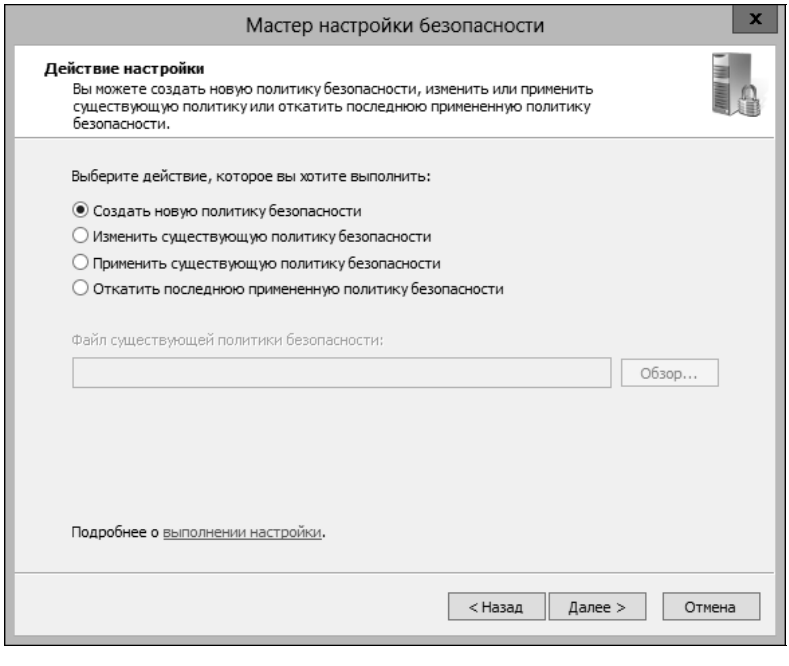


Рис. 5.11. Выберите действие настройки

3. На странице **Выбор сервера** (Select Server) укажите сервер, который нужно использовать в качестве образца для этой политики безопасности. Образец — это сервер с установленными ролями, компонентами и опциями, с которыми необходимо рабо-

тать. По умолчанию выбран компьютер, на котором запущен мастер настройки безопасности. Для выбора другого компьютера нажмите кнопку **Обзор**. В окне **Выбор: "Компьютер"** введите имя компьютера и нажмите кнопку **Проверить имена** (Check Names). Выберите учетную запись компьютера, которую нужно использовать, и нажмите кнопку **OK**.

4. После нажатия кнопки **Далее** мастер соберет конфигурацию безопасности и сохранит ее в базе данных безопасности. На странице **Обработка базы данных** (Processing Security Configuration Database) настройки безопасности нажмите кнопку **Просмотр базы данных** для просмотра настроек в базе данных. После просмотра настроек в SCW Viewer вернитесь в окно мастера и нажмите кнопку **Далее** для продолжения.
5. У каждого раздела конфигурации есть вводная страница. Первая вводная страница — это страница для раздела **Настройка служб на основе ролей** (Role-Based Service Configuration). Нажмите кнопку **Далее**.
6. На странице **Выбор ролей сервера** (Select Server Roles) выводится список установленных ролей сервера (рис. 5.12). Выберите роли, которые должны быть включены. Установите флажок напротив имени каждой роли, которая должна быть включена. Сброшенный флажок выключает службы, входящие порты и настройки для этой роли при условии, что они не требуют какой-то включенной роли. Нажмите кнопку **Далее**.

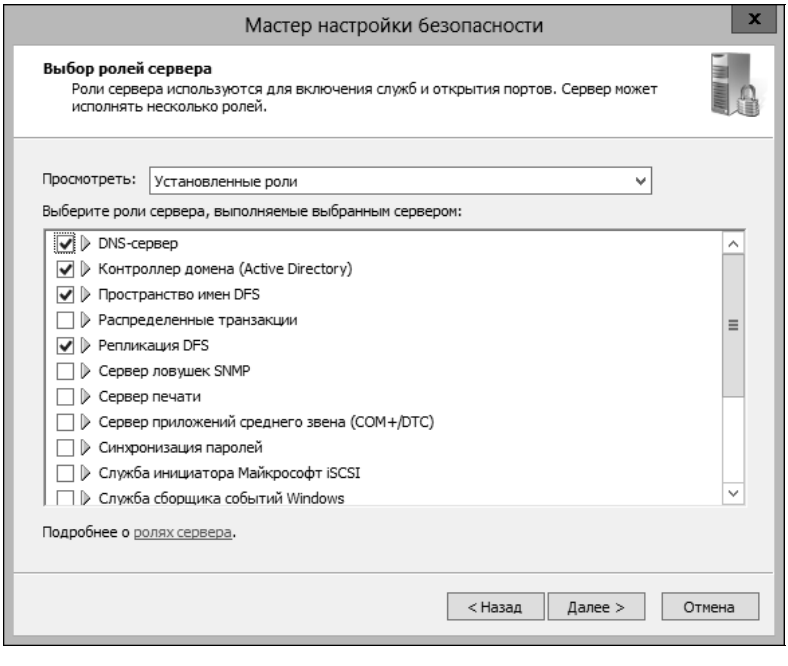


Рис. 5.12. Выберите роли, которые нужно включить

7. На странице **Выбор клиентских возможностей** (Select Client Features) будут отображены установленные компоненты, используемые для включения служб. Выберите компоненты, которые должны быть включены, и отметьте флажки напротив

тех компонентов, которые нужно выключить. Выключение компонента отключает службы, требуемые для этого компонента, при условии, что они не нужны другому активному компоненту. Нажмите кнопку **Далее**.

8. На странице **Выбор управления и других параметров** (Select Administration And Other Options) будут отображены установленные параметры, используемые для включения служб и открытия портов. Выберите каждый параметр, который нужно включить. Снимите флажок с каждого параметра, который нужно выключить. Выбор параметра включает службы, связанные с ним. Отключение параметра отключает службы, необходимые для этого параметра, при условии, что ни один другой параметр в них не нуждается. Нажмите кнопку **Далее**.
9. Страница **Выбор дополнительных служб** (Select Additional Services) отображает дополнительные службы, найденные на выбранном сервере при обработке базы данных безопасности. Как обычно, включаем нужные службы и отключаем ненужные. При включении службы будут также включены службы, необходимые для этой службы. Отключение параметра отключает службы, необходимые для этой службы, при условии, что ни одна другая служба в них не нуждается. Нажмите кнопку **Далее**.
10. На странице **Обработка неопределенных служб** (Handling Unspecified Services) можно выбрать, как должны обрабатываться неопределенные службы. Неопределенные службы — это службы, которые не устанавливаются на выбранном сервере и не заносятся в базу данных безопасности. По умолчанию режим запуска неопределенных служб не изменяется. Чтобы отключить неопределенные службы, выберите **Отключить эту службу** (Disable The Service). Нажмите кнопку **Далее**.
11. На странице **Подтверждение изменений для служб** (Confirm Service Changes) просмотрите службы, которые будут изменены на выбранном сервере, если политика безопасности будет применена. Обратите внимание на текущий режим запуска и режим запуска, который будет применен политикой. Нажмите кнопку **Далее**.
12. На вводной странице для **Сетевой безопасности** (Network Security) нажмите кнопку **Далее**. На странице **Правила сетевой безопасности** (Network Security Rules) будет отображен список правил брандмауэра, необходимых для ранее выбранных ролей, компонентов и параметров. Можно добавить, изменить или удалить входящие/исходящие правила брандмауэра. Нажмите кнопку **Далее**, когда будете готовы продолжить.
13. На вводной странице для раздела **Параметры реестра** (Registry Setting) нажмите кнопку **Далее**. На странице **Требовать цифровую подпись SMB** (Require SMB Security Signatures) просмотрите параметры цифровой подписи SMB (Server Message Block). Обычно не нужно изменять параметры по умолчанию. Нажмите кнопку **Далее**.
14. Для контроллеров домена и серверов с LDAP на странице **Требовать цифровую подпись LDAP** (Require SMB Security Signatures) можно установить минимальные требования операционной системы для всех поддерживающих каталог компьютеров, которые получают доступ к Active Directory.

15. На странице **Исходящие методы проверки подлинности** (Outbound Authentication Methods) выберите методы, которые использует выбранный сервер для аутентификации удаленных компьютеров. Указанные варианты устанавливают уровень аутентификации LAN Manager для исходящих соединений, который будет использоваться. Если компьютер взаимодействует только с компьютерами домена, выберите вариант **Учетные записи в домене** (Domain Accounts), но не выбирайте другие параметры. Это позволяет убедиться, что компьютер использует наивысший уровень исходящей аутентификации LAN Manager. Если компьютер взаимодействует и с компьютерами домена, и с компьютерами рабочей группы, выберите параметры **Учетные записи в домене** (Domain Accounts) и **Локальные учетные записи на удаленных компьютерах** (Local Accounts On The Remote Computers). В большинстве случаев не нужно выбирать параметры общего доступа к файлам, потому что это приведет к существенному сниженному уровню аутентификации. Нажмите кнопку **Далее**.
16. Выбранные исходящие методы аутентификации определяют, какие дополнительные страницы настроек реестра будут отображены. Помните следующее.
    - Если не выбрать ни один исходящий метод аутентификации, будет установлен уровень **Отправлять только NTLMv2 ответ** (Send NTLMv2 Response Only). Также будет отображена дополнительная страница, позволяющая установить методы аутентификации для входящих соединений. На странице **Исходящая проверка подлинности с использованием учетных записей домена** (Inbound Authentication Using Domain Accounts) укажите типы компьютеров, от которых выбранный сервер будет принимать соединения. Указанные варианты установят используемый уровень аутентификации LAN Manager для входящих соединений. Если компьютер взаимодействует только с компьютерами на базе Windows XP Professional и более поздних версий, очистите обе опции. В этом случае компьютер будет использовать наивысший уровень аутентификации LAN Manager. Если компьютер взаимодействует с более старыми компьютерами, примите параметры по умолчанию. Нажмите кнопку **Далее**.
    - Если выбрать учетные записи домена или локальные учетные записи (либо оба варианта), будут отображены дополнительные страницы, позволяющие установить уровень аутентификации LAN Manager при работе с исходящими соединениями. Также появится возможность указать, нужно ли синхронизировать время компьютеров со временем сервера. Будут приниматься все входящие соединения.
    - Если разрешить общий доступ для ранних версий Windows, уровень безопасности LAN Manager будет установлен в значение **Отправлять ответы LM и NTLM** (Send LM & NTLM Only). Будут приниматься все входящие соединения. Нажмите кнопку **Далее**, после чего будет отображена страница **Сводка параметров реестра** (Registry Settings Summary).
17. На странице **Сводка параметров реестра** (Registry Settings Summary) просмотрите значения, которые будут изменены на выбранном сервере, если будет применена политика безопасности. Обратите внимание на текущее значение и на значение, которое будет установлено в случае применения политики. Нажмите кнопку **Далее**.

18. На странице **Политика аудита** (Audit Policy) просто нажмите кнопку **Далее**. На странице **Политика аудита системы** (System Audit Policy) настройте желаемый уровень аудита. Для отключения аудита выберите **Не выполнять аудит** (Do Not Audit). Для включения аудита успешных событий выберите вариант **Выполнять аудит успешных действий** (Audit Successful Activities). Для включения аудита всех событий выберите **Выполнять аудит как успешных, так и неудачных действий** (Audit Successful And Unsuccessful Activities). Нажмите кнопку **Далее**.
19. На странице **Сводка политики аудита** (Audit Policy Summary) просмотрите параметры, которые будут изменены на выбранном сервере, если политика будет применена. Обратите внимание на текущие настройки и настройки, которые будут применены. Нажмите кнопку **Далее**.
20. На вводной странице **Сохранение политики безопасности** (Save Security Policy) нажмите кнопку **Далее**. На странице **Имя файла политики безопасности** (Security Policy File Name) можно указать параметры для сохранения политики и добавления одного или более шаблонов безопасности. Для просмотра политики безопасности в SCW Viewer нажмите кнопку **Просмотр политики безопасности** (View Security Policy). Когда закончите просмотр политики, вернитесь в окно мастера.
21. Чтобы добавить шаблоны безопасности, нажмите кнопку **Включение шаблонов безопасности**. В одноименном окне нажмите кнопку **Добавить**. В окне **Открытие** (Open) выберите шаблон безопасности для добавления в политику безопасности. Если добавить более одного шаблона безопасности, можно задать приоритет на случай, если некоторые настройки безопасности будут конфликтовать между собой. Чем выше шаблон в списке, тем выше его приоритет. Для изменения приоритета выберите его и используйте кнопки **Вверх** (Up) и **Вниз** (Down). Нажмите кнопку **OK**.
22. По умолчанию политика безопасности хранится в папке *%SystemRoot%*\Security\Msscw\Policies. Нажмите кнопку **Обзор**. В окне **Сохранить как** выберите другое место для хранения политики (в случае необходимости). После введения имени политики безопасности нажмите кнопку **Сохранить**. Путь по умолчанию или выбранный путь и имя файла будут отображены в поле **Имя файла политики безопасности** (Security Policy File Name).
23. Нажмите кнопку **Далее**. На странице **Применение политики безопасности** (Security Policy File Name) можно выбрать, когда применить политику, сейчас или позже. Нажмите кнопку **Далее**, а затем кнопку **Готово**.

Редактирование политик безопасности

Можно использовать мастер настройки безопасности для редактирования политики безопасности следующим образом:

1. Запустите мастер настройки безопасности. В диспетчере серверов его можно вызвать с помощью команды меню **Средства | Мастер настройки безопасности** (Tools | Security Configuration Wizard). После запуска мастера нажмите кнопку **Далее**.

2. На странице **Действие настройки** (Configuration Action) выберите переключатель **Изменить существующую политику безопасности** (Edit An Existing Security Policy), а затем нажмите кнопку **Обзор**. В окне открытия файла выберите политику безопасности и нажмите кнопку **Открыть**. Файлы политик безопасности имеют расширение xml. Нажмите кнопку **Далее**.
3. Повторите действия 3–23 процедуры, описанной в *разд. "Создание политик безопасности" ранее в этой главе*, для редактирования политики безопасности.

Применение политик безопасности

Мастер настройки безопасности можно использовать для применения политики безопасности следующим образом:

1. Запустите мастер настройки безопасности. В диспетчере серверов его можно вызвать с помощью команды меню **Средства | Мастер настройки безопасности**. После запуска мастера нажмите кнопку **Далее**.
2. На странице **Действие настройки** выберите переключатель **Применить существующую политику безопасности** (Apply An Existing Security Policy), а затем нажмите кнопку **Обзор**. В окне открытия файла выберите политику безопасности и нажмите кнопку **Открыть**. Файлы политик безопасности имеют расширение xml. Нажмите кнопку **Далее**.
3. На странице **Выбор сервера** выберите сервер, к которому необходимо применить политику безопасности. По умолчанию выбран локальный компьютер. Для выбора другого компьютера нажмите кнопку **Обзор**. В окне **Выбор: "Компьютер"** введите имя компьютера и нажмите кнопку **Проверить имена**. Выберите учетную запись компьютера и нажмите кнопку **OK**.
4. Нажмите кнопку **Далее**. На странице **Применение политики безопасности** (Apply Security Policy) нажмите кнопку **Просмотр политики безопасности** (View Security Policy), чтобы просмотреть настройку политики безопасности в SCW Viewer. Когда закончите просмотр политики, вернитесь к мастеру.
5. Нажмите кнопку **Далее** для применения политики на выбранном сервере. Когда мастер закончит применять политику, нажмите кнопку **Далее**, а затем кнопку **Готово**.

Откат последней примененной политики безопасности

Для отмены последней политики безопасности тоже можно использовать мастер настройки безопасности:

1. Запустите мастер настройки безопасности. В диспетчере серверов его можно вызвать с помощью команды меню **Средства | Мастер настройки безопасности**. После запуска мастера нажмите кнопку **Далее**.
2. На странице **Действие настройки** выберите переключатель **Откатить последнюю примененную политику безопасности** (Rollback The Last Applied Security Policy) и нажмите кнопку **Далее**.

3. На странице **Выбор сервера** выберите сервер, на котором нужно откатить политику безопасности. По умолчанию выбран локальный компьютер. Для выбора другого компьютера нажмите кнопку **Обзор**. В окне **Выбор: "Компьютер"** введите имя компьютера и нажмите кнопку **Проверить имена**. Выберите учетную запись компьютера и нажмите кнопку **OK**.
4. Нажмите кнопку **Далее**. На странице **Откат настройки безопасности** (On the Rollback Security Configuration) нажмите кнопку **Просмотр файла отката** (View Rollback File) для просмотра деталей последней примененной политики в SCW Viewer. Когда закончите просматривать политику, вернитесь в окно мастера.
5. Нажмите кнопку **Далее** для отката политики на выбранном сервере. Когда мастер завершит свою работу, нажмите кнопку **Далее**, а затем кнопку **Готово**.

Развертывание политики безопасности на нескольких компьютерах

Когда в организации много компьютеров, применять политику безопасности к каждому из них отдельно не очень удобно. Как было упомянуто в *разд. "Развертывание шаблонов безопасности на нескольких компьютерах" ранее в этой главе*, можно применить политику безопасности через групповую политику, а для этой цели нужно создать организационное подразделение.

Когда необходимые организационные подразделения созданы, можно использовать команду преобразования `Scwcmd`, чтобы создать GPO, включающий настройки в политике безопасности (и шаблоны безопасности, присоединенные к политике). Тогда можно развернуть настройки на компьютерах, присоединив новый GPO к соответствующим организационным подразделениям. По умолчанию политика безопасности, создаваемая мастером настройки безопасности, помещается в папку *%SystemRoot%*\security\msscw\Policies.

Используйте следующий синтаксис для преобразования политики безопасности:

```
scwcmd transform /p:FullFilePathToSecurityPolicy /g:GPOName
```

где *FullFilePathToSecurityPolicy* — полный путь к xml-файлу политики безопасности, а *GPOName* — отображаемое имя для нового GPO. Рассмотрим следующий пример:

```
scwcmd transform /p:"c:\users\wrs\documents\fspolicy.xml"
/g:"FileServer GPO"
```

При создании GPO его привязка осуществляется так:

1. В консоли управления групповой политикой выберите организационное подразделение. На панели справа на вкладке **Связанные объекты групповой политики** (Linked Group Policy Objects) показаны GPO, которые в данный момент связаны с выбранным организационным подразделением (если таковые есть).
2. Щелкните правой кнопкой мыши на организационном подразделении, к которому нужно привязать ранее созданный GPO, выберите команду **Связать существующий объект групповой политики** (Link An Existing GPO). В окне **Выбор объекта групповой политики** (Select GPO) выберите GPO, который нужно связать, и на-

жмите кнопку **OK**. Изменения вступят в силу, когда будет обновлена групповая политика.

Поскольку создан новый GPO и присоединен GPO с надлежащим уровнем в структуре Active Directory, можно восстановить исходное состояние, удалив ссылку на GPO.

Удалить ссылку на GPO можно так:

1. В GPMC выберите и разверните организационное подразделение. В правой части окна существует вкладка **Связанные объекты групповой политики** (Linked Group Policy Objects), которая отображает GPO, связанные с выбранным организационным подразделением.
2. Щелкните правой кнопкой мыши на GPO, связь с которым нужно разорвать. В контекстном меню сбросьте флажок **Связь включена** (Link Enabled) для удаления связи.

ГЛАВА 6

Управление пользователями и компьютерами с помощью групповой политики

Групповая политика используется для управления пользователями и компьютерами. В этом разделе мы рассмотрим некоторые специфические области управления, в том числе:

- перенаправление папок;
- сценарии компьютера и пользователя;
- развертывание программного обеспечения;
- настройка рабочих папок;
- регистрацию сертификатов компьютера и пользователя;
- параметры автоматического обновления.

Централизованное управление специальными папками

Посредством перенаправления папок можно управлять специальными папками, которые используются Windows Server. Это можно сделать с помощью перенаправления специальных папок в центральное сетевое хранилище вместо использования множества хранилищ по умолчанию — на каждом компьютере. Список папок, которыми можно управлять централизованно для Windows Vista и более поздних версий, таков: AppData (Roaming), Рабочий стол, Главное меню, Документы, Изображения, Музыка, Видео, Избранное, Контакты, Загрузки, Ссылки, Поиски и Сохраненные игры.

Обратите внимание: хотя перечень специальных папок в Windows Vista и более поздних версиях ОС немного отличается, управлять ними можно точно так же.

Имеются две основные опции перенаправления. Можно перенаправить специальную папку в одно общее для всех пользователей сетевое хранилище (расположение) или определить хранилище на основании членства пользователя в группах безопасности. В любом случае нужно убедиться, что сетевое расположение, которое планируется использовать, доступно как сетевой ресурс *(см. главу 4)*.

По умолчанию пользователи могут перенаправить папки независимо от того, какой компьютер они используют в домене. Windows 8.1 и Windows Server 2012 R2 позволяют изменять это поведение, определяя, с каких компьютеров пользователь может получить доступ к профилям роуминга и перенаправленным папкам. Это можно сделать с помощью определения основных компьютеров и задания политики домена, которая бы ограничивала загрузку профилей, перенаправленных папок (или и профилей, и перенаправленных папок) на основные компьютеры. Для получения дополнительной информации *см. главу 10*.

Перенаправление специальных папок в единое расположение

Перенаправить специальную папку в общее расположение можно с помощью этих действий:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO сайта, домена или организационного подразделения, с которыми нужно работать, и выберите команду **Изменить**. Откроется редактор политики для GPO.

   Примечание

   Если предпочитаете создать новый GPO, щелкните правой кнопкой мыши на домене или организационном подразделении и выберите команду **Создать объект групповой политики в этом домене и связать его** (Create A GPO... And Link It Here). В окне **Новый объект групповой политики** (New GPO) введите имя нового GPO и нажмите кнопку **OK**.

2. В редакторе политики разверните следующие узлы: **Конфигурация пользователя\Политика\Конфигурация Windows\Перенаправление папки** (User Configuration\Windows Settings\Folder Redirection).
3. В узле **Перенаправление папки** (Folder Redirection) щелкните правой кнопкой мыши по названию папки, параметры которой нужно изменить. Например, пусть это будет **AppData (перемещаемая)** (AppData(Roaming)). В появившемся меню выберите команду **Свойства**. Откроется одноименное диалоговое окно (рис. 6.1).
4. В раскрывающемся списке **Политика** (Setting) на вкладке **Конечная папка** (Target) установите значение **Перенаправлять папки всех пользователей в одно расположение** (Basic - Redirect everyone's folder to the same location).
5. В группе **Расположение целевой папки** (Target folder location) есть несколько опций, определяющих, с какой папкой происходит работа.

   - **Перенаправлять в домашний каталог пользователя** (Redirect to the user's home directory) — если выбрать эту опцию, папка будет перенаправлена в подкаталог в пределах домашнего пользовательского каталога. Можно указать расположение домашнего пользовательского каталога с помощью переменных среды `%HomeDrive%` и `%HomePath%`.
   - **Создать папку для каждого пользователя на корневом пути** (Create a folder for each user under the root path) — если выбрать эту опцию, для каждого пользователя в указанном расположении (поле **Корневой путь** (Root Path)) будет создан отдельный каталог. Имя папки пользователя — это имя пользователя, задан-

ное переменной `%UserName%`. Если указан корневой путь \\Zeta\UserDocuments, то папка пользователя Williams будет размещена в \\Zeta\UserDocuments\Williams.

- **Перенаправлять в следующее расположение** (Redirect to the following location) — при выборе этой опции папка будет перенаправлена в расположение, указанное в поле **Корневой путь**. Здесь обычно хочется использовать переменные среды, чтобы разграничить расположения для каждого пользователя. Например, можно установить такое расположение в качестве корневого пути: \\Zeta\UserData\`%UserName%`\docs.
- **Перенаправлять в расположение, определяемое локальным профилем** (Redirect to the local userprofile location) — при выборе этой опции папка будет перенаправлена в подкаталог в каталоге профилей пользователей. Можно выбрать расположение профиля пользователя с помощью переменной среды `%UserProfile%`.

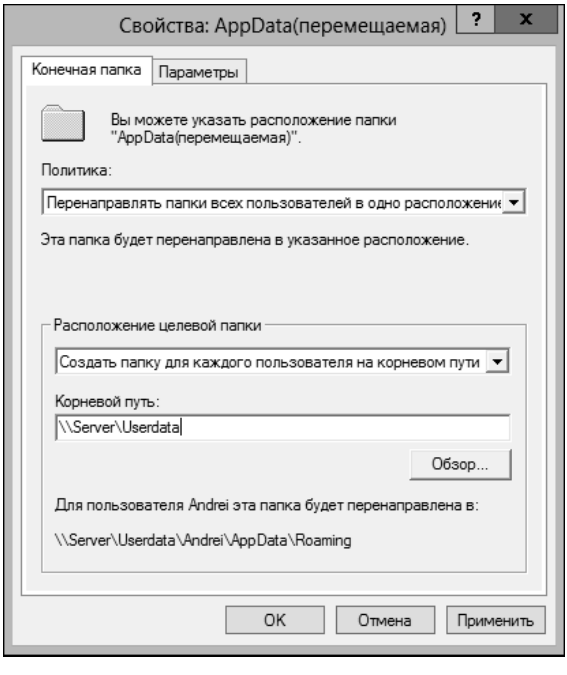


Рис. 6.1. Установите опции для перенаправления специальных папок

6. Перейдите на вкладку **Параметры** (Settings) для настройки дополнительных параметров и нажмите кнопку **OK** для завершения процесса:
   - **Предоставить права монопольного доступа к** (Grant the user exclusive rights to) — предоставляет пользователям полные права доступа к своим данным в специальной папке;
   - **Перенести содержимое <название папки> в новое расположение** (Move the contents of foldername to the new location) — перемещает данные в специальные папки из отдельных систем сети в центральную папку или папки;

- **Применить политику перенаправления также к** (Also apply redirection policy to) — применяет политику перенаправления к предыдущим версиям Windows.

Внимание!

При указании корневого пути убедитесь, что указываете UNC-путь для сервера, а не локальный путь. Базовый синтаксис UNC-пути — *\\ИмяСервера\ИмяРесурса*, например, \\CorpServer38\CorpData.

Перенаправление специальных папок на основании членства в группе

Можно перенаправить специальную папку на основании членства в группе, для этого выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO сайта, домена или организационного подразделения, с которыми нужно работать, и выберите команду **Изменить**. Откроется редактор политики для GPO.
2. В редакторе политики разверните следующие узлы: **Конфигурация пользователя\Политика\Конфигурация Windows\Перенаправление папки** (User Configuration\Windows Settings\Folder Redirection).
3. В узле **Перенаправление папки** (Folder Redirection) щелкните правой кнопкой мыши по названию папки, параметры которой нужно изменить. Например, пусть это будет **AppData (перемещаемая)** (AppData(Roaming)). В появившемся меню выберите команду **Свойства**.
4. На вкладке **Конечная папка** в списке **Политика** выберите значение **Указать различные расположения для разных групп пользователей** (Advanced-Specify Locations For Various User Groups). Как показано на рис. 6.2, появится группа **Членство в группе безопасности** (Security Group Membership).
5. Нажмите кнопку **Добавить**, чтобы открыть окно **Выбор группы и расположения** (Specify Group And Location). Или выберите запись группы и нажмите кнопку **Изменить** для редактирования ее параметров.
6. В поле **Членство в группе безопасности** (Security Group Membership) введите имя группы безопасности, для которой нужно настроить перенаправление, или нажмите кнопку **Обзор** для поиска группы безопасности.
7. Как и в случае базового перенаправления, доступны опции, позволяющие определить папку.
   - **Перенаправлять в домашний каталог пользователя** (Redirect to the user's home directory) — если выбрать эту опцию, папка будет перенаправлена в подкаталог в пределах домашнего пользовательского каталога. Можно указать расположение домашнего пользовательского каталога с помощью переменных среды `%HomeDrive%` и `%HomePath%`.
   - **Создать папку для каждого пользователя на корневом пути** (Create a folder for each user under the root path) — если выбрать эту опцию, для каждого пользователя в указанном расположении (поле **Корневой путь**) будет создан отдель-

ный каталог. Имя папки пользователя — это имя пользователя, заданное переменной `%UserName%`. Если указан корневой путь \\Zeta\UserDocuments, то папка пользователя Williams будет размещена в \\Zeta\UserDocuments\Williams.

- **Перенаправлять в следующее расположение** (Redirect to the following location) — при выборе этой опции папка будет перенаправлена в расположение, указанное в поле **Корневой путь**. Здесь обычно нужно использовать переменные среды, чтобы разграничить расположения для каждого пользователя. Например, можно установить такое расположение в качестве корневого пути: \\Zeta\UserData\`%UserName%`\docs.
- **Перенаправлять в расположение, определяемое локальным профилем** (Redirect to the local userprofile location) — при выборе этой опции папка будет перенаправлена в подкаталог в каталоге профилей пользователей. Можно выбрать расположение профиля пользователя с помощью переменной среды `%UserProfile%`.

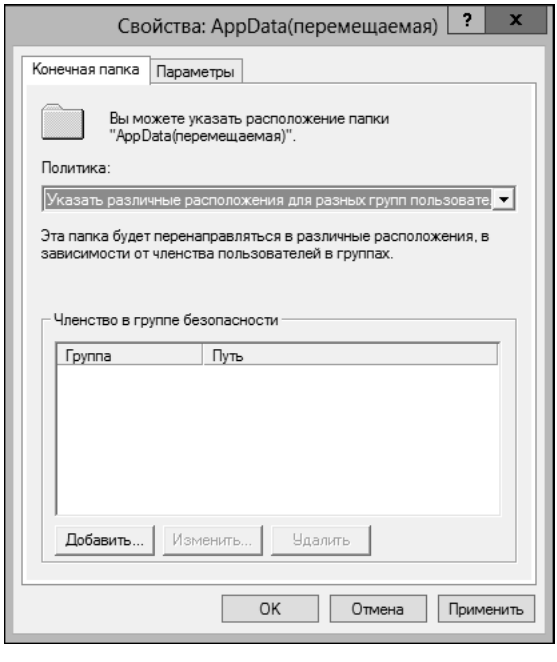


Рис. 6.2. Настройка расширенного перенаправления с использованием группы **Членство в группе безопасности**

8. Нажмите кнопку **OK**. Повторите действия 5–7 для других групп, которые нужно настроить.
9. Когда закончите создание записей групп, перейдите на вкладку **Параметры**, чтобы настроить дополнительные параметры, и нажмите кнопку **OK** для завершения процесса:
   - **Предоставить права монопольного доступа к** — предоставляет пользователям полные права доступа к своим данным в специальной папке;

- **Перенести содержимое <название папки> в новое расположение** — перемещает данные в специальные папки из отдельных систем сети в центральную папку или папки;
- **Применить политику перенаправления также к** — применяет политику перенаправления к предыдущим версиям Windows.

Удаление перенаправления

Иногда нужно удалить перенаправление определенной папки. Сделать это можно следующим образом:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которыми нужно работать. Выберите команду **Изменить**, чтобы открыть редактор GPO.
2. В редакторе политики разверните следующие узлы: **Конфигурация пользователя\Конфигурация Windows\Перенаправление папки** (User Configuration\Windows Settings\Folder Redirection).
3. В узле **Перенаправление папки** щелкните правой кнопкой мыши на специальной папке и выберите команду **Свойства**.
4. Перейдите на вкладку **Параметры** появившегося диалогового окна и убедитесь, что выбрана нужная опция в группе **Удаление политики** (Policy Removal). Доступны следующие опции.
   - **После удаления политики оставить папку в новом расположении** (Leave the folder in the new location when policy is removed). При выборе этой опции папка и все ее содержимое останутся в переадресованном местоположении, а действующим пользователям будет разрешен доступ к папке и ее содержимому в этом местоположении.
   - **После удаления политики перенаправить папку обратно в локальный профиль пользователя** (Redirect the folder back to the local userprofile location when policy is removed). При выборе этой опции папка и все ее содержимое будут скопированы обратно в оригинальное расположение. Контент не будет удален из предыдущего расположения.
5. Если вы изменили опцию **Политика удаления** (Policy Removal), нажмите кнопку **Применить** (Apply), а затем перейдите на вкладку **Целевая папка**. Если не было никаких изменений, просто перейдите на вкладку **Целевая папка**.
6. Для удаления всех определений перенаправлений для специальной папки выберите переключатель **Не задана** (Not Configured) в списке **Политика** (Setting).
7. Для удаления перенаправления определенной группы выберите группу в области **Членство в группе безопасности** (Security Group Membership) и нажмите кнопку **Удалить** (Remove). Нажмите кнопку **OK**.

Управление сценариями пользователя и компьютера

В Windows Server можно настроить четыре типа сценариев:

- Computer Startup — выполняется при запуске;
- Computer Shutdown — выполняется при завершении работы;
- User Logon — выполняется, когда пользователь входит в систему;
- User Logoff — выполняется, когда пользователь выходит из системы.

Windows 2000 и более поздние версии поддерживают сценарии, написанные на языке командной оболочки, с расширениями bat и cmd или сценарии, которые используют Windows Script Host (WSH). WSH — это компонент Windows Server, позволяющий использовать сценарии, написанные на языке сценариев вроде VBScript без необходимости вставки сценария в веб-страницу. Для предоставления доступа к многоцелевой среде WSH основывается на движках сценариев. Движок сценариев — это компонент, определяющий основной синтаксис и структуру определенного языка сценариев. Windows Server поддерживает движки сценариев для VBScript и JScript. Также доступны другие движки.

Начиная с Windows 7 и Windows Server 2008 R2, текущие версии Windows поддерживают сценарии PowerShell. Если Windows PowerShell установлен на компьютеры, которые обрабатывают определенные GPO, можно использовать сценарии Windows PowerShell так же, как и остальные сценарии. Есть возможность запуска сценариев Windows PowerShell до или после других типов сценариев.

Назначение сценариев Computer Startup и Computer Shutdown

Сценарии Computer Startup и Computer Shutdown назначаются как часть GPO. Таким образом, все компьютеры, которые являются членами сайта, домена и организационного подразделения или всех трех структур одновременно, выполняют сценарии автоматически, когда загружаются или завершают работу.

Чтобы назначить сценарий запуска или завершения работы, выполните следующие действия:

1. В Проводнике Windows откройте папку, содержащую сценарии, которые нужно использовать.
2. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которыми будете работать. Выберите команду **Изменить**, чтобы открыть редактор GPO.
3. В узле **Конфигурация компьютера** (Computer Configuration) дважды щелкните на папке **Конфигурация Windows** (Windows Settings), затем перейдите в подпапку **Сценарии (запуск/завершение)** (Scripts).
4. Для работы со сценариями запуска щелкните правой кнопкой мыши на элементе **Автозагрузка** (Startup) и выберите команду **Свойства** (Properties). Для работы со

сценариями завершения работы щелкните правой кнопкой на элементе **Завершение работы** (Shutdown) и выберите команду **Свойства**. Откроется окно, подобное изображенному на рис. 6.3.

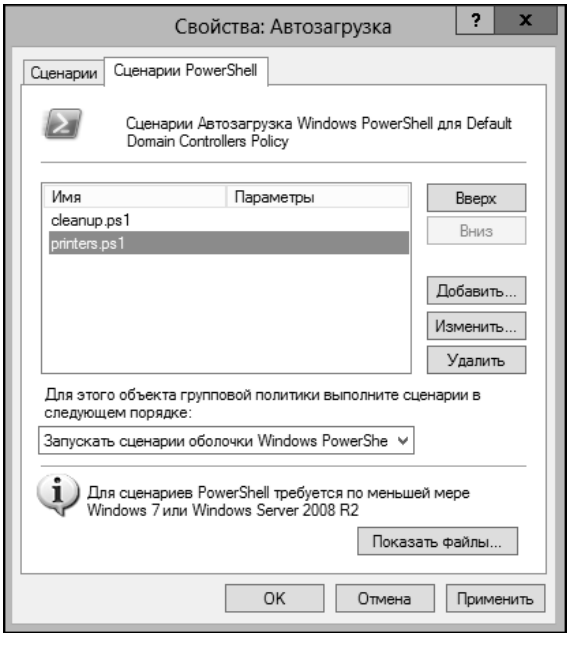


Рис. 6.3. Добавление, изменение и удаление сценариев автозагрузки

5. На вкладке **Сценарии** (Scripts) можно управлять сценариями командной строки (с расширениями bat или cmd) и сценариями Windows Scripting Host. На вкладке **Сценарии PowerShell** (PowerShell Scripts) можно управлять сценариями Windows PowerShell. Для перехода к папке, в которой находятся сценарии, нажмите кнопку **Показать файлы** (Show Files).
6. Скопируйте файлы в окне Проводника Windows и вставьте их в окно, которое будет открыто после нажатия кнопки **Показать файлы**.
7. Нажмите кнопку **Добавить** для назначения сценария. Откроется окно **Добавление сценария** (Add A Script). В поле **Имя сценария** (Script Name) введите имя сценария, который был скопирован в папку Machine\Scripts\Startup или папку Machine\Scripts\Shutdown. В поле **Параметры сценария** (Script Parameters) введите любые параметры, которые нужно передать сценарию. Повторите этот шаг для других сценариев.
8. Во время запуска и завершения работы сценарии будут выполнены в том порядке, в котором они указаны в окне **Свойства**. На вкладке **Сценарии** используйте кнопки **Вверх** (Up) и **Вниз** (Down) для изменения порядка выполнения сценариев. Такие же кнопки есть на вкладке **Сценарии PowerShell**. На вкладке **Сценарии PowerShell** есть также список, позволяющий выбрать, когда должны запускаться сценарии Windows PowerShell: до или после запуска других типов сценариев.

9. Если нужно отредактировать имя сценария или его параметры, выберите сценарий и нажмите кнопку **Изменить**. Для удаления сценария выберите его и нажмите кнопку **Удалить**.
10. Для сохранения изменений нажмите кнопку **OK**.

Назначение сценариев входа и выхода пользователя

Сценарии пользователя можно назначить с помощью одного из трех способов.

- Можно назначить сценарии входа/выхода как часть GPO. В этом случае все пользователи, являющиеся членами сайта, домена или организационного подразделения (или всех трех сразу), автоматически запустят сценарии при входе или выходе.
- Можно назначить сценарии входа индивидуально, используя консоль **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers). В этом случае можно назначить каждому пользователю или каждой группе отдельный сценарий входа. Подробно этот способ будет рассмотрен в *главе 9*.
- Также можно назначить отдельные сценарии выхода как запланированные задачи. Для создания расписаний задач используется мастер создания задачи (Scheduled Task Wizard).

Чтобы назначить сценарии входа или выхода в GPO, выполните следующие действия:

1. В Проводнике Windows откройте папку, содержащую сценарии, которые нужно использовать.
2. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которыми планируете работать. Выберите команду **Изменить**, чтобы открыть редактор GPO.
3. В узле **Конфигурация пользователя** (User Configuration) дважды щелкните на папке **Конфигурация Windows** (Windows Settings), затем перейдите в узел **Сценарии (вход/выход из системы)** (Scripts).
4. Для работы со сценариями входа щелкните правой кнопкой мыши на папке **Вход в систему** (Logon) и выберите команду **Свойства**. Для работы со сценариями выхода щелкните правой кнопкой мыши на папке **Сценарии выхода** (Logoff) и выберите команду **Свойства**. Откроется окно, подобное изображенному на рис. 6.4.
5. На вкладке **Сценарии** можно управлять сценариями командной строки (с расширениями bat или cmd) и сценариями Windows Scripting Host. На вкладке **Сценарии PowerShell** можно управлять сценариями Windows PowerShell. Для перехода к папке, в которой находятся сценарии, нажмите кнопку **Показать файлы**.
6. Скопируйте файлы в окне Проводника Windows и вставьте их в окно, которое будет открыто после нажатия кнопки **Показать файлы**.
7. Нажмите кнопку **Добавить** для назначения сценария. Откроется окно **Добавление сценария**. В поле **Имя сценария** введите имя сценария, который скопирован в папку User\Scripts\Logon или папку User\Scripts\Logoff. В поле **Параметры сценария** введите любые параметры, которые нужно передать сценарию. Повторите этот шаг для других сценариев.

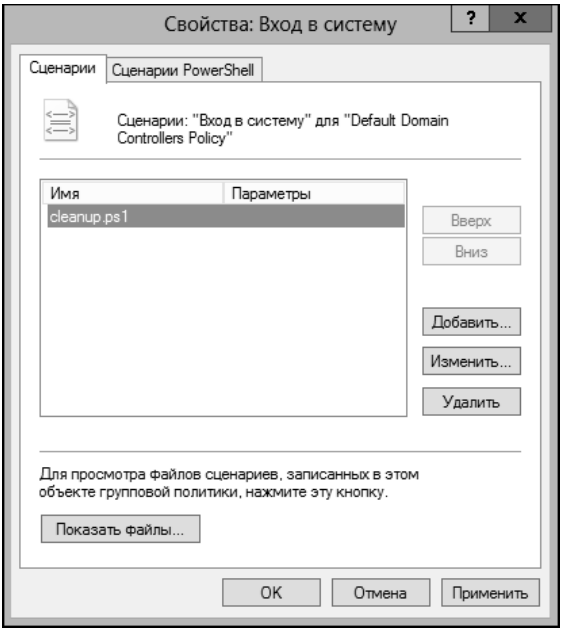


Рис. 6.4. Добавление, изменение и удаление сценариев входа/выхода пользователей

8. Во время входа в систему и выхода из нее сценарии будут выполнены в том порядке, в котором они определены в окне **Свойства**. На вкладке **Сценарии** используйте кнопки **Вверх** и **Вниз** для изменения порядка сценариев в случае необходимости. Такие же кнопки есть на вкладке **Сценарии PowerShell**. На вкладке **Сценарии PowerShell** существует также список, позволяющий выбрать, когда должны запускаться сценарии Windows PowerShell: до или после запуска других типов сценариев.
9. Если нужно отредактировать имя сценария или его параметры, выберите сценарий и нажмите кнопку **Изменить**. Для удаления сценария выберите его и нажмите кнопку **Удалить**.
10. Для сохранения изменений нажмите кнопку **OK**.

Развертывание программного обеспечения через групповую политику

Для развертывания ПО в групповой политике есть базовая функциональность, называемая *политикой установки программного обеспечения*. Хотя она не разработана для замены решений для предприятий вроде System Center 2012 R2, ее можно использовать для автоматизации развертывания и обслуживания ПО в организации практически любого размера при условии, что все компьютеры работают под управлением операционной системы Windows.

Знакомство с политикой установки программного обеспечения

В групповой политике можно развертывать ПО на основе компьютеров и пользователей. Приложения на базе компьютеров доступны всем пользователям компьютера и настраиваются в узле **Конфигурация компьютера\Конфигурация программ\Установка программ** (Computer Configuration\Software Settings\Software Installation).

Можно развернуть программы тремя основными способами.

- **Назначение компьютеру** (Computer assignment) — назначает программное обеспечение на компьютеры клиента, чтобы установка ПО выполнялась при запуске компьютера. Эта техника не требует какого-либо вмешательства со стороны пользователя, но она нуждается в перезагрузке системы для установки программ. Установленное программное обеспечение будет доступно всем пользователям компьютера.
- **Назначение пользователю** (User assignment) — назначает программное обеспечение пользователям так, что оно будет установлено при входе пользователя в систему. Эта техника не требует какого-либо вмешательства со стороны пользователя, но предполагает вход в систему для установки программы. Установленное программное обеспечение будет доступно только конкретному пользователю.
- **Публикация пользователю** (User publishing) — публикует программное обеспечение так, что пользователи могут установить его вручную с помощью утилиты **Программы и компоненты** (Programs And Features). Эта техника требует вмешательства пользователя для установки программы или активации установки. Установленное программное обеспечение будет доступно только конкретному пользователю.

При использовании назначения пользователю или публикации пользователю можно объявлять программное обеспечение так, чтобы компьютер мог установить программу при ее первом использовании. В этом случае программное обеспечение может быть установлено автоматически в следующих ситуациях:

- когда пользователь пытается открыть документ, для работы с которым нужна программа;
- когда пользователь открывает ярлык приложения;
- когда другому приложению требуется компонент программы.

При настройке политики **Установка программ** (Software Installation) не нужно использовать существующие GPO. Вместо этого следует создать объекты GPO, которые будут настраивать установку программ и затем привязать эти GPO к соответствующим контейнерам в групповой политике. При использовании этого подхода значительно проще повторно развернуть программное обеспечение и применить обновления.

После создания GPO для разворачивания программного обеспечения нужно настроить точку распространения. *Точка распространения* — это общая папка, которая доступна компьютерам и пользователям, для которых вы разворачиваете ПО. Как правило, можно подготовить точку распространения путем копирования файла пакета инсталлятора и всех необходимых приложению файлов на общий ресурс и настройкой разрешений так, чтобы все эти файлы были доступны. Для других приложений, например Microsoft

Office, можно подготовить точку восстановления путем административной установки на общий ресурс. В случае с MS Office нужно запустить программу установки с параметром `/a` и указать общий ресурс как назначение установки. Преимущество административной установки состоит в том, что программное обеспечение может быть обновлено и повторно развернуто через политику **Установка программ**.

Можно обновить приложения, развернутые через политику **Установка программ** либо с помощью обновления или сервис-пака, либо с помощью развертывания новой версии приложения. Эти задачи немного отличаются друг от друга.

Развертывание программ в организации

Политика **Установка программ** используется только с пакетами установщика Windows (msi) и пакетами приложений нижнего уровня ZAW (zap). При использовании назначения компьютера, назначения пользователя или публикации можно развернуть ПО с помощью пакетов установщика Windows. При использовании публикации можно применять как msi-пакеты, так и zap-пакеты. Необходимо установить разрешения на файле пакета установщика так, чтобы у соответствующих компьютеров и пользователей был доступ для чтения.

Поскольку политика **Установка программ** применяется во время обработки настроек политики, развертывание приложения на компьютере обрабатывается при его запуске, а развертывание приложения для пользователя осуществляется при входе в систему. Можно настроить установку с использованием файлов преобразований (mst). Эти файлы изменяют процесс установки согласно настройкам, которые заданы для определенных компьютеров и пользователей.

Развернуть программное обеспечение можно с помощью следующих действий:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO, который нужно модифицировать для распространения, и затем нажмите кнопку **Изменить**.
2. В редакторе политики разверните узел **Конфигурация компьютера\Конфигурация программ\Установка программ** (Computer Configuration\Software Settings\ Software Installation) или узел **Конфигурация пользователя\Конфигурация программ\Установка программ** (User Configuration\Software Settings\Software Installation) в зависимости от типа разворачивания ПО.
3. Щелкните правой кнопкой мыши на политике **Установка программ**. В появившемся контекстном меню выберите команду **Создать | Пакет** (New | Package).
4. В окне **Открытие** (Open) перейдите к сетевому ресурсу, в котором размещены пакеты, щелкните на пакете для его выбора и нажмите кнопку **Открыть** (Open).

   Примечание

   В списке типов файлов (в диалоговом окне открытия файла) по умолчанию выбраны пакеты установщика Windows (msi). Если нужно выполнить публикацию программного обеспечения, можно также выбрать тип файла **Пакеты приложений нижнего уровня ZAW (.zap)**.

5. В окне **Развертывание программ** (Deploy Software), показанном на рис. 6.5, выберите один из следующих методов развертывания и нажмите кнопку **OK**:

- **публичный** (Published) — публикует приложение без изменений;
- **назначенный** (Assigned) — назначает приложение без изменений;
- **особый** (Advanced) — развертывание приложения с использованием расширенных параметров настройки.

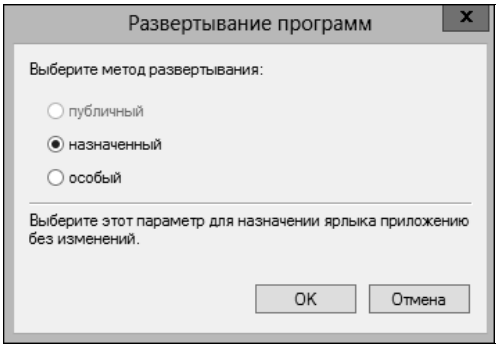


Рис. 6.5. Выберите метод развертывания

Настройка параметров развертывания программного обеспечения

Просмотреть и установить основные параметры для пакета программного обеспечения можно с использованием следующих действий:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO, который используете для развертывания, и выберите команду **Изменить**.
2. В редакторе политики разверните узел **Конфигурация компьютера\Конфигурация программ\Установка программ** или узел **Конфигурация пользователя\Конфигурация программ\Установка программ** в зависимости от типа разворачивания ПО.
3. Дважды щелкните по пакету установки ПО. В окне **Свойства** можно просмотреть или модифицировать параметры развертывания ПО.
4. На вкладке **Развертывание** (Deployment) (рис. 6.6) можно изменить тип развертывания и настроить следующие параметры развертывания и установки.
   - **Автоматически устанавливать приложение при обращении к файлу с соответствующим расширением** (Auto-install this application by file extension activation) — связывает приложение с файлами, которое оно обрабатывает. Программа будет установлена при первом обращении к файлу связанного типа. Используется по умолчанию.
   - **Удалять это приложение, если его использование выходит за рамки, допустимые политикой управления** (Uninstall this application when it falls out of the scope of management) — удаляет приложение, если оно больше не применимо к пользователю.

- **Не отображать этот пакет в окне мастера установки и удаления программ панели управления** (Do not display this package in the add/remove programs control panel) — запрещает отображение приложения в окне **Установка/удаление программ**, что предотвращает удаление приложения пользователем.

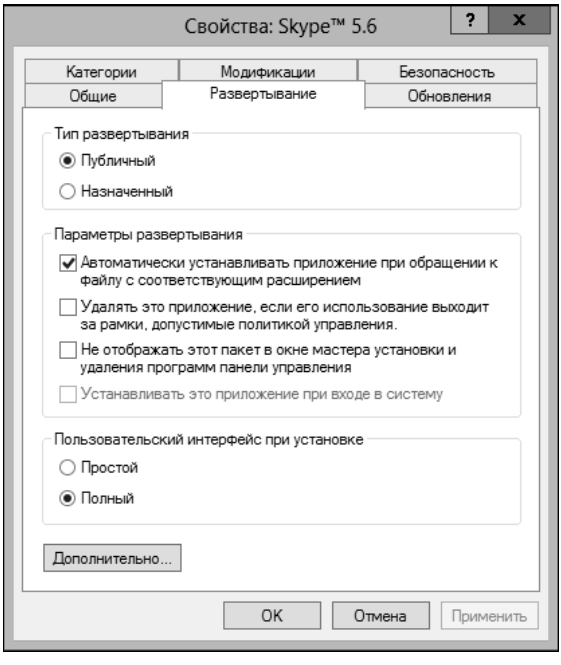


Рис. 6.6. Просмотрите и измените параметры развертывания в случае необходимости

- **Устанавливать это приложение при входе в систему** (Install this application at logon) — при входе пользователя в систему будет произведена полная установка программы, а не "объявление" приложения. Эта опция не может быть выбрана, когда приложение публикуется для пользователя.
- **Пользовательский интерфейс при установке** (Installation user interface options) — контролирует, как будет произведена установка. Значение по умолчанию — **Полный** (Maximum), при этом пользователь увидит все экраны программы установки и все сообщения. При значении **Простой** (Basic) пользователь увидит только сообщения об ошибках и сообщение о завершении установки.

5. Нажмите кнопку **OK**.

Обновление развернутого программного обеспечения

Когда приложение использует пакет установщика Windows, можно применить обновление или пакет обновлений к развернутому приложению с помощью следующих действий:

1. После получения msi- или msp-файла (патч), содержащего обновления или пакет обновлений, который будет применен, скопируйте его и любые другие установоч-

ные файлы в папку, содержащую оригинальный msi-файл. В случае необходимости перезапишите любые повторяющиеся файлы.

2. В консоли GPMC щелкните правой кнопкой мыши на GPO, который вы используете для развертывания, и выберите команду **Изменить**.
3. В редакторе политики разверните узел **Конфигурация компьютера\Конфигурация программ\Установка программ** или узел **Конфигурация пользователя\Конфигурация программ\Установка программ** в зависимости от типа разворачивания ПО.
4. Щелкните правой кнопкой мыши по пакету, затем в контекстном меню выберите команды **Все задачи | Развернуть приложение заново** (All Tasks | Redeploy Application).
5. Когда консоль попросит подтвердить действие, нажмите кнопку **Да**. Приложение будет заново развернуто для всех пользователей и компьютеров, в соответствии с выбранным GPO.

Когда приложение не использует пакеты установщика Windows, можно обновить развернутое приложение или применить пакет обновлений следующим образом:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO, который используется для развертывания, и выберите команду **Изменить**.
2. В редакторе политики разверните узел **Конфигурация компьютера\Конфигурация программ\Установка программ** или узел **Конфигурация пользователя\Конфигурация программ\Установка программ** в зависимости от типа разворачивания ПО.
3. Щелкните правой кнопкой мыши по пакету, а затем в контекстном меню выберите команды **Все задачи | Удалить** (All Task | Remove).
4. Скопируйте новый zap-файл и все дополнительные файлы на сетевой ресурс и заново разместите приложение.

Обновление развернутого приложения

Обновить ранее развернутое приложение можно до более новой версии следующим образом:

1. Получите новый файл установщика Windows, содержащий новую версию программного обеспечения, скопируйте его и все необходимые файлы на сетевой ресурс. Либо можно осуществить административную установку на сетевой ресурс.
2. В консоли GPMC щелкните правой кнопкой мыши на GPO, который используется для развертывания, и выберите команду **Изменить**.
3. В редакторе политики разверните узел **Конфигурация компьютера\Конфигурация программ\Установка программ** или **Конфигурация пользователя\ Конфигурация программ\Установка программ** в зависимости от типа разворачивания ПО.
4. Щелкните правой кнопкой мыши на политике **Установка программ**. В появившемся контекстном меню выберите команды **Создать | Пакет** (New | Package). Соз-

дайте и назначьте или опубликуйте приложение с использованием пакета установщика Windows для новой версии ПО.

5. Щелкните правой кнопкой мыши по названию пакета и выберите команду **Свойства**. На странице **Обновления** (Upgrades) нажмите кнопку **Добавить**. В окне **Добавление обновления** (Add Upgrade Package) выполните одно из следующих действий.
   - Если исходное приложение и обновление находятся в текущем GPO, выберите переключатель **из текущего объекта групповой политики (GPO)** (Current Group Policy Object), а затем выберите ранее развернутое приложение в списке **Обновляемое приложение** (Package To Upgrade).
   - Если исходное приложение и обновление находятся в разных GPO, выберите переключатель **из указанного объекта групповой политики** (A Specific GPO). Далее нажмите кнопку **Обзор** и выберите GPO в окне **Поиск объекта групповой политики** (Browse For A Group Policy Object). Затем выберите ранее развернутое приложение из списка **Обновляемое приложение** (Package to upgrade).
6. Выберите опции обновления. Если нужно заменить приложение новой версией, выберите переключатель **Удалить приложение, затем установить его обновление** (Uninstall the existing package). Если же нужно осуществить именно обновление поверх существующей инсталляции, выберите переключатель **Обновление возможно поверх имеющегося приложения** (Package can upgrade over the existing package).
7. Нажмите кнопку **OK** для закрытия окна **Добавление обновления**. Если нужно сделать это обновление обязательным, выберите переключатель **Обязательное обновление для уже установленных приложений** (Required upgrade for existing packages), а затем нажмите кнопку **OK** для закрытия окна **Свойства**.

Автоматическая настройка рабочих папок

Компьютеры, являющиеся членами рабочего места, могут получить доступ к ресурсам внутренней сети, таким как внутренние веб-сайты и бизнес-приложения. Рабочие папки позволяют пользователям синхронизировать корпоративные данные с конечными устройствами и наоборот. Данные устройства могут быть соединены с корпоративным доменом или рабочим местом. Устройства получают доступ к рабочим папкам через удаленный веб-шлюз, работающий на Microsoft Internet Information Services (IIS).

Чтобы развернуть рабочие файлы, нужно добавить роль **Файловые службы и службы хранилища** на файловый сервер, а затем настроить рабочие папки с помощью диспетчера серверов. Позже можно будет использовать параметры политики для управления связанными параметрами, например, сервером, к которому пользователи могут подключаться удаленно и получать доступ к рабочим папкам. Управлять сервером соединения можно одним из двух способов:

- указав точный URL файлового сервера, размещающего рабочие папки для пользователя, например, **https://server29.cpandl.com**;
- указав URL, используемый в организации для обнаружения рабочих папок, например, **https://workfolders.cpandl.com**.

Практический совет

Пока у серверов, размещающих рабочие папки, есть допустимые сертификаты SSL, клиенты используют безопасное зашифрованное соединение с рабочими папками. Когда устройство инициирует SSL-соединение, сервер отправляет сертификат клиенту. Клиент проверяет сертификат и продолжает работу, только если сертификату можно доверять. Если настраивается соединение с точным URL, клиент может соединиться непосредственно с указанным сервером и синхронизировать данные в рабочих папках. У сертификата сервера общее имя (Common Name, CN) и альтернативное имя (Subject Alternative Name, SAN) должны соответствовать заголовку узла в запросе. Например, если клиент выполняет запрос к **https://server18.cpandl.com**, CN и SAN должны быть **server18.cpandl.com**.

Параметр групповой политики **Указать параметры рабочих папок** (Specify Work Folders Settings) в узле **Конфигурация пользователя\Административные шаблоны\ Компоненты Windows\Рабочие папки** (User Configuration\ Administrative Templates\ Windows Components \Work Folders) применяется для указания URL, используемого внутри организации для обнаружения рабочих папок. По умолчанию любой сервер, настроенный для работы с рабочими папками, действует как сервер обнаружения. Если явно указать URL, клиенты будут подключаться к одному из нескольких серверов, а для определения, какой именно сервер содержит рабочие папки для клиента, будет использоваться адрес электронной почты пользователя. Затем клиент соединяется с этим сервером. У каждого сервера обнаружения должен быть сертификат с несколькими альтернативными именами (SAN), содержащий имя сервера и имя обнаружения. Например, если клиент делает запрос к **https://workfolders.cpandl.com** и соединяется с **fileserver11.cpandl.com**, у сертификата атрибут CN или SAN должен быть **fileserver11.cpandl.com**, а SAN — **workfolders.cpandl.com**.

Для настройки рабочих папок в групповой политике используется следующая техника:

1. Получите доступ к групповой политике для системы, сайта, домена или организационного подразделения, с которыми нужно работать. Далее получите доступ к узлу **Рабочие папки** (**Конфигурация пользователя\Административные шаблоны\ Компоненты Windows\Рабочие папки**).
2. Дважды щелкните на параметре **Указать параметры рабочих папок** (Specify Work Folders Settings) и выберите переключатель **Включено**.
3. В поле **URL-адрес рабочих папок** (Work Folders URL) введите URL файлового сервера, размещающего рабочие папки для пользователя, или URL, используемый внутри организации для обнаружения рабочих папок.
4. Если нужно запретить пользователям изменить параметры рабочих папок, включите флажок **Принудительная автоматическая настройка** (Force automatic setup).
5. Нажмите кнопку **OK**.

Автоматическая регистрация сертификатов компьютера и пользователя

Сервер, определенный как центр сертификации, отвечает за выпуск цифровых сертификатов и управление списками аннулированных сертификатов (Certificate Revocation Lists, CRL). Серверы под управлением Windows Server могут быть сконфигурированы как центры сертификации, для этого нужно установить **Службы сертификатов Active**

Directory (Active Directory Certificate Services, AD CS). Компьютеры и пользователи могут использовать сертификаты для аутентификации и шифрования.

На предприятии используются корпоративные центры сертификации для автоматической регистрации сертификатов. Это означает, что авторизированные пользователи и компьютеры могут запросить сертификат, а центр сертификации — автоматически обработать запрос сертификата так, чтобы пользователи и компьютеры могли сразу установить сертификат.

Групповая политика контролирует способ работы автоматической регистрации. При установке корпоративного центра сертификации политика автоматической регистрации для пользователей и компьютеров включается автоматически. Политика для регистрации сертификатов компьютера называется **Клиент служб сертификации: автоматическая регистрация** (Certificate Services Client — Auto-Enrollment Settings) и находится в узле **Конфигурация компьютера\Политики\Конфигурация Windows\ Параметры безопасности\ Политики открытого ключа** (Computer Configuration\ Policies\Windows Settings\Security Settings\Public Key Policies). Политика для регистрации сертификатов пользователя называется **Клиент служб сертификации: автоматическая регистрация** и находится в узле **Конфигурация пользователя\Политики\ Конфигурация Windows\Параметры безопасности\Политики открытого ключа** (User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies).

Настроить автоматическую регистрацию можно так:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO и выберите команду **Изменить**.
2. В редакторе политик разверните узел **Конфигурация компьютера\Политики\ Конфигурация Windows\Параметры безопасности \Политики открытого ключа** или узел **Конфигурация пользователя\Политики\Конфигурация Windows\ Параметры безопасности\Политики открытого ключа** в зависимости от политики, настройки которой нужно просмотреть.
3. Дважды щелкните на политике **Клиент служб сертификации: автоматическая регистрация**. Для отключения автоматической регистрации установите переключатель **Отключено** (Disabled) из списка **Модель конфигурации** (Configuration Model) и нажмите кнопку **OK**. Далее пропустите все последующие шаги этой процедуры. Для включения автоматической регистрации установите переключатель **Включено** (Enable) из списка **Модель конфигурации**.
4. Для автоматического возобновления истекших сертификатов, обновления сертификатов в состоянии ожидания и удаления отозванных сертификатов установите соответствующий флажок.
5. Чтобы убедиться, что используется последняя версия шаблонов сертификатов, отметьте флажок **Обновлять сертификаты, использующие шаблоны сертификатов** (Update certificates that use certificate templates).
6. Для уведомления пользователей о том, что срок сертификата скоро выйдет, определите, когда будут отправлены уведомления пользователям. По умолчанию уведомления отправляются, когда осталось 10% от времени жизни сертификата.
7. Нажмите кнопку **OK** для сохранения настроек.

Управление автоматическими обновлениями с помощью групповой политики

Автоматические обновления помогают поддерживать операционную систему в актуальном состоянии. Хотя можно настроить автоматические обновления на основе компьютеров, обычно необходимо настроить эту функцию для всех пользователей и компьютеров, которые обрабатывают GPO — это более эффективная техника управления.

Заметьте, что по умолчанию Windows 8.1 и Windows Server 2012 R2 используют Windows Update для загрузки компонентов Windows, а также двоичных файлов для ролей, служб ролей и компонентов. Если средства диагностики Windows определят, что компонент Windows требует ремонта, Windows использует Windows Update для загрузки компонента. Если администратор пытается установить роль, службу роли или компонент, а полезные данные отсутствуют (payloads), Windows использует Windows Update для загрузки нужных бинарных файлов.

Настройка автоматических обновлений

При управлении автоматическими обновлениями через групповую политику можно выбрать конфигурацию обновления.

- **Автоматическая загрузка и установка по расписанию** (Auto Download And Schedule The Install) — обновления будут автоматически загружены и установлены в соответствии с созданным расписанием. Когда обновления будут загружены, операционная система уведомит пользователя, что он может просмотреть запланированные обновления. Пользователь может установить обновления или подождать, пока придет время запланированной установки.
- **Автоматическая загрузка и уведомление об установке** (Auto Download And Notify For Install) — операционная система получит все обновления и, когда они станут доступны, уведомит пользователя, что они готовы к установке. Пользователь может принять или отклонить обновления. Принятые обновления будут установлены. Отклоненные обновления не будут установлены, но останутся в системе и их можно будет установить позже.
- **Уведомление о загрузке и установке** (Notify For Download And Notify For Install) — операционная система уведомляет пользователя перед получением любых обновлений. Если пользователь выберет загрузку обновлений, у него есть еще возможность принять или отклонить их. Принятые обновления будут установлены. Отклоненные обновления не будут установлены, но останутся в системе, и их можно будет установить позже.
- **Разрешить локальному администратору выбирать параметры** (Allow Local Admin To Choose Setting) — позволяет локальному администратору настраивать автоматическое обновление. Заметьте, что используются любые другие опции, локальные пользователи и администраторы не могут изменить параметры автоматического обновления.

Настроить автоматическое обновление можно так:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO, с которым нужно работать, и выберите команду **Изменить**.
2. В редакторе политик разверните узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows** (Computer Configuration\Administrative Templates\Windows Components\Windows Update).
3. Дважды щелкните на политике **Настройка автоматического обновления** (Configure Automatic Updates). В появившемся окне можно включить или отключить управление автоматическими обновлениями с помощью групповой политики. Для включения управления автоматическими обновлениями установите переключатель **Включено**, для отключения управления — переключатель **Отключено**. Нажмите кнопку **OK** и пропустите следующие шаги.
4. Из списка **Настройка автоматического обновления** (Configure Automatic Updating) выберите опцию обновления. В Windows 8 (и более поздних версиях), как и в Windows Server 2012 (и поздних версиях), обновления устанавливаются автоматически во время запланированного обслуживания, если включен флажок **Устанавливать во время автоматического обслуживания** (Install during automatic maintenance).
5. Если выбрана опция **Автоматическая загрузка и установка по расписанию** (Auto download and schedule the install), можете выбрать день и время установки обновлений. Нажмите кнопку **OK** для сохранения изменений.

По умолчанию обновление Windows запускается ежедневно в 02:00 как часть автоматического обслуживания. В случае с настольными операционными системами (Windows 8 и более поздними версиями), обновление Windows использует возможности управления питанием компьютера для пробуждения компьютера из режима гибернации или сна в запланированное время, а затем устанавливает обновления. Этот процесс пробуждения и установки произойдет независимо от того, работает ли компьютер от батареи или от сети питания.

Если для завершения обновлений, применяемых как часть автоматического обслуживания, требуется перезапуск и есть активный сеанс пользователя, Windows кэширует учетные данные пользователя, зарегистрированного в данный момент в консоли, а затем перезапустит компьютер автоматически. После перезапуска Windows использует кэшируемые учетные данные, чтобы войти в систему, как этот пользователь. Затем Windows перезапустит приложения, которые были ранее запущены, и заблокирует сеанс, используя безопасный рабочий стол (Secure Desktop). Если BitLocker включен, весь процесс будет защищен шифрованием BitLocker.

Процесс обслуживания не требует, чтобы в системе был зарегистрирован пользователь. Процесс обслуживания будет запущен, независимо от того, зарегистрирован ли в системе пользователь или нет. Если пользователь не зарегистрирован на момент начала обслуживания и требуется перезапуск, Windows перезапустит компьютер без кэширования учетных данных и хранения информации о запущенных приложениях. После перезапуска Windows не будет выполнять вход от имени какого-то пользователя.

Поскольку Windows автоматически пробуждает компьютер для осуществления автоматического обслуживания и обновления, администратору нужно внимательно отнестись к параметрам питания. Если план питания не сконфигурирован, чтобы выключить дисплей и перевести компьютер в состояние сна, компьютер может остаться включенным в течение многих часов после автоматического обслуживания и обновления.

Оптимизация автоматических обновлений

В целом, большинство автоматических обновлений устанавливается только при перезагрузке компьютера. Некоторые автоматические обновления могут быть установлены немедленно без прерывания системных служб и перезапуска системы. Чтобы убедиться, что эти обновления устанавливаются немедленно, выполните следующие шаги:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO, с которым нужно работать, и выберите команду **Изменить**.
2. В редакторе политик разверните узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows**.
3. Дважды щелкните на политике **Разрешить немедленную установку автоматических обновлений** (Allow Automatic Updates Immediate Installation). В окне **Свойства** установите переключатель **Включено** и нажмите кнопку **OK**.

По умолчанию только пользователи с привилегиями локальных администраторов получают уведомления об обновлениях. Можно разрешить любому зарегистрированному пользователю получать уведомления об обновлениях так:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO, который нужно модифицировать, и выберите команду **Изменить**.
2. В редакторе политик разверните узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows**.
3. Дважды щелкните на политике **Разрешать пользователям, не являющимися администраторами, получать уведомления об обновлениях** (Allow Non-Administrators To Receive Update Notifications). В окне **Свойства** установите переключатель **Включено** и нажмите кнопку **OK**.

Другая полезная политика — **Запретить использование любых средств Центра обновления Windows** (Remove Access To Use All Windows Update Features). Она запрещает доступ ко всем функциям Центра обновления. Если политика включена, все функции Центра обновления будут удалены и не могут быть настроены, в том числе будет недоступна вкладка **Центр обновления** (Windows Update) в утилите **Система** (System) и обновление драйверов от сайта Windows Update в диспетчере устройств. Данная политика находится в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Центр обновления Windows**.

Использование службы обновлений в интрасети

В сетях с сотнями и тысячами компьютеров процесс автоматического обновления может использовать значительную часть пропускной способности сети, в конечном итоге не целесообразно, чтобы каждый компьютер проверял обновления и загружал их по

Интернету. Вместо этого рассмотрите использование политики службы обновления Microsoft в интрасети, которая обязывает отдельные компьютеры проверять обновления на выделенном внутреннем сервере.

На выделенном сервере обновлений должны быть запущены службы Windows Server Update Services (WSUS), также он должен быть настроен как веб-сервер (на нем должен быть запущен Microsoft Internet Information Services, IIS), и он должен выдержать дополнительную нагрузку, которая будет значительной в большой сети во время пикового использования службы обновления. Дополнительно, у сервера обновлений должен быть открыт порт 80 для доступа к внешней сети. Использование брандмауэра или прокси-сервера на этом порту не должно вызвать какие-либо проблемы.

Процесс обновления также отслеживает конфигурационную информацию и статистику для каждого компьютера. Эта информация необходима для корректной работы процесса обновления и может быть сохранена на отдельном сервере статистики (сервере внутренней сети, на котором запущен IIS) или же на самом сервере обновления.

Чтобы указать внутренний сервер обновления, выполните следующие действия:

1. После установки и настройки сервера обновлений откройте GPO, который нужно отредактировать. В редакторе политик разверните узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows**.
2. Дважды щелкните на политике **Указать размещение службы обновления Майкрософт в интрасети** (Specify Intranet Microsoft Update Service Location).
3. В поле **Укажите службу обновлений в интрасети для поиска обновлений** (Set the intranet update service for detecting updates) укажите URL сервера обновления. В большинстве случаев URL выглядит так: **http://имя_сервера**, например, **http://CorpUpdateServer01**.
4. В поле **Укажите сервер статистики в интрасети** (Set the intranet statistics server) введите URL сервера статистики. Сервер статистики не обязательно должен быть отдельным сервером, в этом поле можно указать адрес сервера обновлений.

   Примечание

   Если нужно использовать один сервер и для обновлений, и для статистики, введите один и тот же URL в оба поля. В противном случае введите разные URL в соответствующие поля.

5. Нажмите кнопку **OK**. После обновления GPO системы, работающие под определенными версиями Windows, будут использовать внутренний сервер для обновлений. Необходимо контролировать серверы обновлений и статистики несколько дней или даже недель, чтобы убедиться, что они работают корректно. На сервере обновлений и сервере статистики будут созданы файлы и каталоги.

ГЛАВА 7

Управление TCP/IP-сетью

Администратор разрешает компьютерам взаимодействовать по сети, используя базовые сетевые протоколы, встроенные в Windows Server 2012 R2. Основным сетевым протоколом является TCP/IP. Протокол TCP/IP — это набор протоколов и служб, используемых для сетевого взаимодействия, и основной протокол для межсетевого взаимодействия. По сравнению с другими сетевыми протоколами настройка TCP/IP довольно сложна, зато TCP/IP — самый универсальный протокол.

> ***Примечание***
>
> Настройки групповой политики могут влиять на возможность устанавливать и управлять TCP/IP-сетью. Ключевые политики, которые необходимо исследовать, находятся в узлах **Конфигурация пользователя\Административные шаблоны\Сеть\Сетевые подключения** (User Configuration\Administrative Templates\Network\Network Connections) и **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика** (Computer Configuration\Administrative Templates\System\Group Policy).

Навигация по сетям в Windows Server 2012 R2

В Windows Server 2012 R2 имеется расширенный набор сетевых утилит:

- **Обозреватель сети** (Network Explorer) — предоставляет собой основное средство просмотра компьютеров и устройств сети;
- **Центр управления сетями и общим доступом** (Network and Sharing Center) — основная консоль для просмотра и управления конфигурацией сети и общего доступа;
- **Диагностика сети** (Network Diagnostics) — предоставляет средство автоматической диагностики для обнаружения и решения сетевых проблем.

Перед описанием этих утилит давайте сначала посмотрим на компоненты Windows Server 2012 R2, на которых и основаны эти утилиты:

- **Сетевое обнаружение** (Network Discovery) — компонент, управляющий способностью видеть другие компьютеры и устройства;
- **Служба сетевого расположения** (Network Awareness) — компонент, уведомляющий об изменениях в подключениях узлов и конфигурации сети.

Практический совет

Компьютеры под управлением Windows Vista с SP1 или более поздние версии Windows поддерживают расширения сетевого расположения. Эти расположения позволяют компьютеру подключаться к одной или нескольким сетям через два или более интерфейса (независимо от типа соединения — проводное или беспроводное) для выбора маршрута с лучшей производительностью для передачи данных. В рамках выявления оптимального маршрута Windows выбирает лучший интерфейс (проводной или беспроводной) для передачи. Этот механизм улучшает выбор беспроводного интерфейса по проводным сетям, когда оба интерфейса присутствуют.

Параметры сетевого обнаружения используемого компьютера определяют, какие компьютеры и устройства будут доступны в сетевых инструментах Windows Server 2012 R2. Параметры обнаружения работают в сочетании с Брандмауэром Windows и способны блокировать или разрешать следующие действия:

- обнаружение сетевых компьютеров и устройств;
- обнаружение компьютера другими системами.

Параметры сетевого обнаружения должны обеспечить надлежащий уровень безопасности для каждой из категорий сетей, к которым подключен компьютер. Существуют три категории сетей:

- *доменная сеть* — сеть, в которой компьютеры подключены к домену предприятия;
- *частная сеть* — сеть, компьютеры которой являются членами рабочей группы и лишены прямого выхода в Интернет;
- *публичная сеть* — сеть в общественном месте, например, в кафе или аэропорту.

Поскольку компьютер хранит настройки отдельно для каждой категории сети, различные настройки блокирования и разрешения могут использоваться для каждой категории. При первом подключении сетевого адаптера компьютера к сети Windows устанавливает категорию сети на основании конфигурации компьютера. Основываясь на категории сети, ОС Windows Server 2012 R2 автоматически настраивает параметры, которые могут включать или выключать обнаружение. Если режим обнаружения включен, то:

- компьютер может обнаруживать другие компьютеры и устройства в сети;
- другие компьютеры и устройства в сети могут обнаруживать этот компьютер.

Когда обнаружение выключено, то:

- компьютер не способен обнаруживать другие компьютеры и устройства в сети;
- другие компьютеры и устройства в сети не могут обнаруживать этот компьютер.

Обычно сетевой адаптер устанавливается как публичный, прежде чем компьютер будет подключен к домену. Обозреватель сети, показанный на рис. 7.1, отображает список обнаруженных компьютеров и устройств в сети. Для доступа к обозревателю сети запустите Проводник на экране **Пуск** (Start). В окне Проводника выберите **Сеть** (Network) на панели слева.

Какие компьютеры и устройства будут отображены в обозревателе сети, зависит от настроек сетевого обнаружения компьютера, операционной системы и от того, является ли компьютер членом домена. Если обнаружение блокируется и сервер под управлением Windows Server 2012 R2 не является членом домена, будет отображено соот-

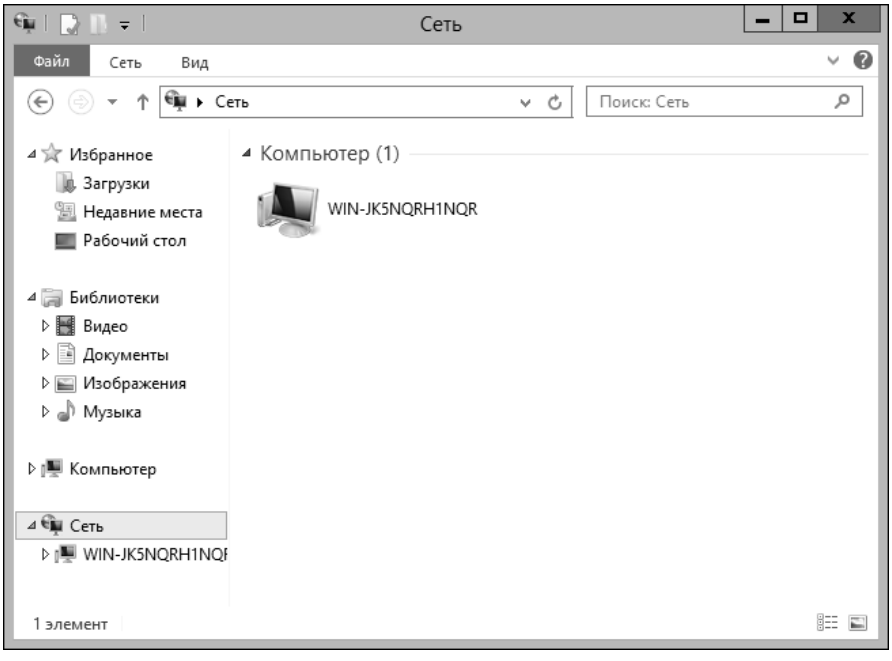


Рис. 7.1. Используйте обозреватель сети для просмотра сетевых ресурсов

ветствующее предупреждение. Щелкните на этом предупреждении и выберите команду **Включить сетевое обнаружение** (Turn On Network Discovery And File Sharing), чтобы включить сетевое обнаружение. В результате будут открыты соответствующие порты Брандмауэра Windows.

Центр управления сетями и общим доступом (Network and Sharing Center), показанный на рис. 7.2, предоставляет информацию о текущем состоянии сети, а также обзор текущей конфигурации сети. Чтобы открыть Центр управления сетями и общим доступом, в Панели управления щелкните по ссылке **Просмотр состояния сети и задач** (View network status and tasks) под заголовком **Сеть и Интернет** (Network and Internet).

Центр управления сетями и общим доступом предоставляет обзор сети. Под именем сети выводится ее категория, например **Доменная сеть** (Domain network), **Частная сеть** (Private network) или **Общедоступная сеть** (Public network). Поле **Тип доступа** (Access type) указывает, как компьютер подключен к текущей сети. Значения для этой опции могут быть следующими: **Без доступа к сети** (No network access), **Без доступа к Интернету** (No Internet access) или **Интернет** (Internet). При щелчке по имени подключения можно будет увидеть соответствующее окно состояния.

Щелкните на задаче **Изменение параметров адаптера** (Change adapter settings) для отображения страницы **Сетевые подключения** (Network Connections), которая используется для управления сетевыми подключениями. Щелчок на задаче **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) предоставляет возможность настройки параметров общего доступа и сетевого обнаружения для каждого профиля сети. Для управления профилем разверните панель профиля, нажав кнопку со стрелкой вниз напротив имени профиля, установите параметры, а затем на-

жмите кнопку **Сохранить изменения** (Save changes). Чтобы включить или выключить сетевое обнаружение, выберите, соответственно, **Включить сетевое обнаружение** (Turn on network discovery) или **Отключить сетевое обнаружение** (Turn off network discovery), а затем нажмите кнопку **Сохранить изменения**[1].

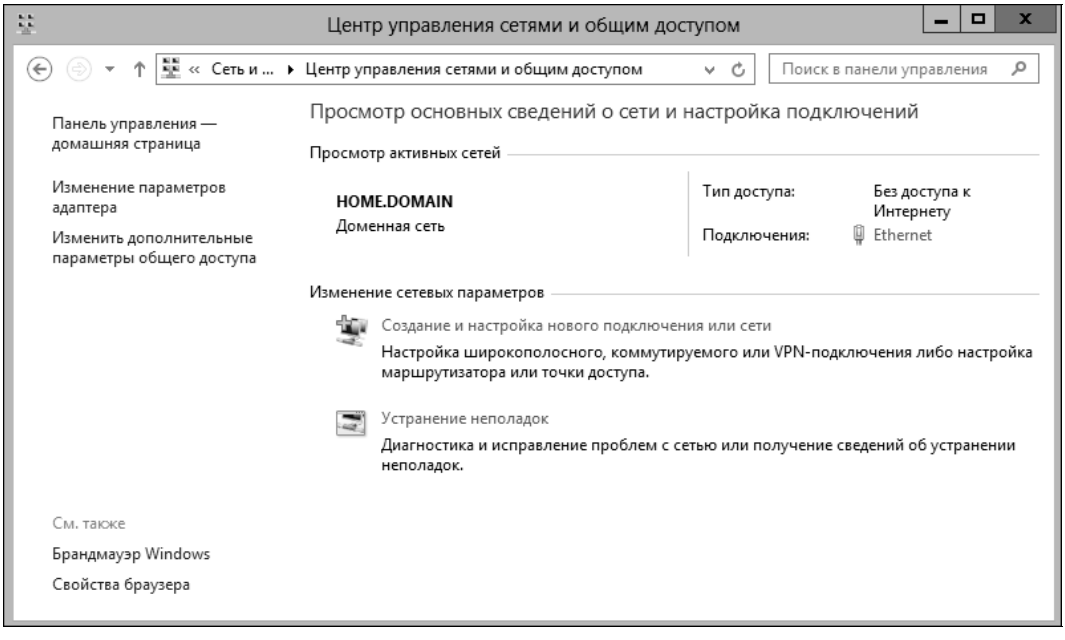


Рис. 7.2. Просмотр и управление настройками сети через Центр управления сетями и общим доступом

Средствами Центра управления сетями и общим доступом можно диагностировать проблемы с сетью. Для этого щелкните на ссылке **Устранение неполадок** (Troubleshoot problems) и выберите возникшую проблему, например **Входящие подключения** (Incoming Connections), а затем следуйте инструкциям. Диагностика сети попытается идентифицировать проблему и предложит возможное решение.

> ***Примечание***
>
> Для быстрого доступа к странице **Сетевые подключения** без открытия Центра управления сетями и общим доступом нажмите клавишу <Window> и введите команду `ncpa.cpl`. Альтернативно вы можете ввести эту команду в командной строке или командной строке Windows PowerShell.

[1] Если сетевое обнаружение не включается (нет никаких ошибок, просто при нажатии кнопки **Сохранить изменения** переключатель остается в положении **Отключить сетевое обнаружение**), убедитесь, что включены следующие службы: **Обнаружение SSDP**, **Модуль поддержки NetBIOS через TCP/IP**, **Браузер компьютеров**, **Сервер** и **Публикация ресурсов обнаружения функции**. Эти службы (или некоторые из них) по умолчанию могут быть выключены на Windows Server. Такова особенность серверной версии Windows. — *Прим. пер.*

Управление сетью в Windows 8.1 и Windows Server 2012 R2

В групповой политике находятся политики управления сетью как для проводных сетей (IEEE 802.3), так и для беспроводных сетей (IEEE 802.11). Эти политики находятся в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности** (Computer Configuration\Windows Settings\Security Settings). Только одна проводная и одна беспроводная политики могут быть созданы и применены за один раз. Это означает, что можно устанавливать как проводные, так и беспроводные политики для компьютеров под управлением Windows Vista и более новых версий Windows. Также можно создать беспроводную политику для компьютеров под управлением Windows XP.

Если щелкнуть правой кнопкой мыши на узле **Политики проводной сети (IEEE 802.3)** (Wired Network), можно создать политику для Windows Vista и более поздних версий ОС, которая определяет, будет ли использоваться служба **Wire AutoConfig** для настройки и подключения этих клиентов к проводным сетям 802.3 Ethernet. Для Windows 7 и более поздних версий Windows доступны опции, запрещающие использование общих учетных данных и включающие период блокировки, который не разрешает компьютерам производить автоподключение к сети на указанный период времени.

Если щелкнуть правой кнопкой мыши на узле **Политики беспроводной сети (IEEE 802.11)**, у вас будет возможность создать разные политики — для компьютеров под управлением Windows XP и для компьютеров с более новыми версиями Windows. Данные политики включают автонастройку WLAN, определяют, какие сети могут быть использованы, и устанавливают сетевые разрешения. Для Windows 7 и более поздних версий есть возможность запрещения использования общих учетных данных, включения периода блокировки, а также запрещения размещенных сетей.

ОС Windows Vista SP1 и более поздние версии поддерживают несколько проводных и беспроводных расширений. Эти расширения позволяют пользователям изменять свои пароли при подключении к проводной или беспроводной сети (в противовес использованию функции изменения пароля Winlogon), исправлять неправильный пароль, введенный во время входа и сброса истекшего пароля, — все это часть процесса сетевого входа.

Расширения сетевой безопасности включают следующие протоколы:

- протокол SSTP (Secure Socket Tunneling Protocol);
- безопасный удаленный доступ SRA (Secure Remote Access);
- интерфейс CryptoAPI Version 2 (CAPI2);
- расширения протокола OCSP (Online Certificate Status Protocol);
- резервирование порта для протокола Teredo;
- подпись файла по протоколу RDP (Remote Desktop Protocol).

Протокол SSTP позволяет передавать данные на канальном уровне по протоколу HTTP через подключение HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer). Технология SPA обеспечивает безопасный доступ к удаленным сетям по HTTPS. Вместе

обе технологии позволяют пользователям получать защищенный доступ к частной сети посредством интернет-соединения. Протоколы SSTP и SPA представляют собой модификации PPTP (Point-to-Point Tunneling Protocol) и L2TP/IPsec (Layer Two Tunneling Protocol/Internet Protocol). Для защищенного веб-трафика они используют стандартные порты TCP/IP, что позволяет им проходить через большинство брандмауэров, а также преобразование сетевых адресов NAT (Network Address Translation) и веб-прокси.

Протокол SSTP использует HTTP по протоколу SSL (HTTP over Secure Sockets Layer), который так же известен, как TLS (Transport Layer Security). Протокол HTTP по SSL (TCP-порт 443) обычно служит для защищенной связи с веб-сайтами. Каждый раз, когда пользователи подключаются к веб-адресу, который начинается с https://, они используют HTTP по SSL. Этот подход решает множество проблем VPN-подключений. Поскольку SSTP поддерживает и IPv4, и IPv6, то пользователи могут установить безопасные соединения, используя любую версию IP. По сути, вы получите технологию VPN, которая работает всегда и везде.

Интерфейс CAPI2 расширяет поддержку сертификатов PKI и X.509, а также реализует дополнительную функциональность для проверки пути, хранилищ сертификатов и проверку подписи. Один из этапов проверки пути сертификата — это проверка аннулирования (отзывы), включающая в себя проверку состояния сертификата, чтобы убедиться, что он не был отозван издателем. Здесь на сцене появляется протокол онлайн-проверки состояния сертификата (Online Certificate Status Protocol, OCSP).

Протокол OCSP используется для проверки состояния аннулирования сертификатов. Также CAPI2 поддерживает независимые цепочки подписей OCSP и определяет дополнительные источники загрузки OCSP для каждого издателя. Независимые цепочки подписей OCSP изменяют исходную реализацию OCSP так, что он может работать с OCSP-откликами, подписанными доверенными источниками OCSP, которые не связаны с издателем проверяемого сертификата. Дополнительные источники загрузки OCSP позволяют указать источники загрузки OCSP для выпуска CA-сертификатов в виде URL, которые добавляются как свойства к CA-сертификатам.

Чтобы гарантировать сосуществование IPv4/IPv6, Windows позволяет приложениям использовать IPv6 в сети IPv4, и это дает возможность применять соответствующие технологии, например резервирование порта для Teredo. Teredo — технология туннелирования на базе протокола UDP (User Datagram Protocol), способная пройти через NAT. Она устанавливает связь между симметричными NAT с резервированием портов и прочими типами NAT. Механизм NAT с резервированием портов использует внешний порт с тем же номером, что и внутренний.

Текущие выпуски Windows Server поддерживают технологию разгрузки процессора TCP Chimney. Эта функция позволяет перенести обработку TCP/IP-соединения с процессоров сервера на его сетевые адаптеры, если они поддерживают функцию разгрузки TCP/IP. Могут быть разгружены как TCP/IPv4-соединения, так и TCP/IPv6. По умолчанию TCP-соединения разгружаются на Ethernet-адаптерах, работающих со скоростью 10 Гбит/с, но эта функция выключена на адаптерах со скоростью 1 Гбит/с. Для изменения соответствующих настроек можно использовать Netsh.

Инфраструктура диагностики сети (Network Diagnostic Framework, NDF) упрощает поиск неполадок путем автоматизации множества этапов поиска неисправности и пре-

доставления готовых решений. При использовании утилиты **Диагностика сети Windows** (Windows Network Diagnostics) каждый сеанс диагностики генерирует отчет с ее результатами, а просмотреть эту информацию можно в Центре поддержки (Action Center), щелкнув по ссылке **Устранение неполадок** (Troubleshooting), а затем нажав кнопку **Просмотр журнала** (View History). На странице **Журнал устранения неполадок** (Troubleshooting History) каждый сеанс выводится по типу и дате запуска. Для просмотра подробной информации щелкните на сеансе, который нужно просмотреть, и нажмите кнопку **Подробности** (View details).

Диагностическая информация, показанная в Центре поддержки, приходит из файла ETL (Event Trace Log), создаваемого при диагностике. Если щелкнуть правой кнопкой мыши по сеансу диагностики, в контекстном меню будет команда **Открыть расположение файла** (Open File Location). Выбрав ее, можно увидеть все сгенерированные файлы диагностики для выбранного сеанса диагностики.

Контекст Netsh Trace может быть использован для осуществления всесторонней трассировки, а также захвата и фильтрации пакетов. Трассировки выполняются с использованием предопределенных или пользовательских сценариев и провайдеров. Сценарии трассировки — это коллекции провайдеров. Провайдеры — это фактические компоненты в стеке сетевого протокола, с которыми нужно работать, такие как TCP/IP, Платформа фильтрации Windows и брандмауэр, Службы беспроводной сети, Winsock или NDIS. Как правило, для анализа данных трассировки используется приложение **Сетевой монитор** (Network Monitor, Netmon). Если нужно собрать данные трассировки по компьютеру, где не установлен **Сетевой монитор**, можно просто скопировать файл трассировки на компьютер, где это приложение имеется, чтобы проанализировать данные.

В Windows Vista SP1 и более поздних версиях используется клиент RDP 6.1, который позволяет подписывать файлы RDP для предотвращения открытия или запуска пользователями потенциально опасных файлов из неизвестных источников. Администраторы могут подписывать файлы RDP при помощи специального инструментария Microsoft. В групповой политике или реестре могут быть настроены три связанных параметра: разделенный запятыми список хэшей сертификатов, которым доверяют администраторы *(список доверенных издателей)*, параметр, позволяющий пользователям принимать недоверенных издателей (включен по умолчанию), а также параметр, позволяющий принимать неподписанные файлы (включен по умолчанию).

Windows 8.1 и Windows Server 2012 R2 имеют ряд усовершенствований встроенного DNS-клиента, которые улучшают разрешение имен в сетях IPv4 и IPv6. Используя адаптивный тайм-аут запроса, DNS-клиент адаптирует интервал тайм-аута на основании времени, требуемого на выполнение предыдущих запросов. Таким образом, вместо того, чтобы ждать 1000 мс прежде, чем повторить запрос, время ожидания корректируется на основании предыдущих показателей для сети и варьируется от 25 до 1000 мс.

DNS-клиент для Windows 8.1 и Windows Server 2012 R2 также поддерживает слияние запросов, параллельные запросы и постоянное кэширование. Слияние запросов позволяет DNS-клиенту объединять несколько DNS-запросов для одного и того же имени. Благодаря параллельным запросам DNS-клиент выдает IPv4- и IPv6-запросы параллельно для записей A и AAAA, когда оба IP-интерфейса включены, что упрощает про-

цесс запроса и улучшает производительность. Запросы LLMNR (Link-local multicast name resolution) и NetBIOS также генерируются параллельно для IPv4 и IPv6. Постоянный кэш позволяет DNS-клиенту поддерживать кэширование DNS через изменения, которые происходят в той же сети. Например, теперь DNS-клиент сохраняет кэш после уведомлений об изменении адреса и когда компьютер возобновляет работу после сна или из режима ожидания.

Установка сети TCP/IP

Для установки сети на компьютере нужно установить поддержку TCP/IP и сетевой адаптер. В системе Windows Server 2012 R2 протокол TCP/IP используется в качестве стандартного протокола глобальных сетей. Обычно установка сети происходит одновременно с установкой Windows Server 2012 R2. Администратор также может установить протокол TCP/IP в свойствах подключения по локальной сети.

Для установки TCP/IP после установки Windows Server 2012 R2 зайдите в компьютер, используя учетную запись с привилегиями администратора, и выполните эти действия:

1. В Панели управления откройте Центр управления сетями и общим доступом, щелкнув по ссылке **Просмотр состояния сети и задач** (View network status and tasks) под заголовком **Сеть и Интернет** (Network and Internet).
2. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера** (Change adapter settings).

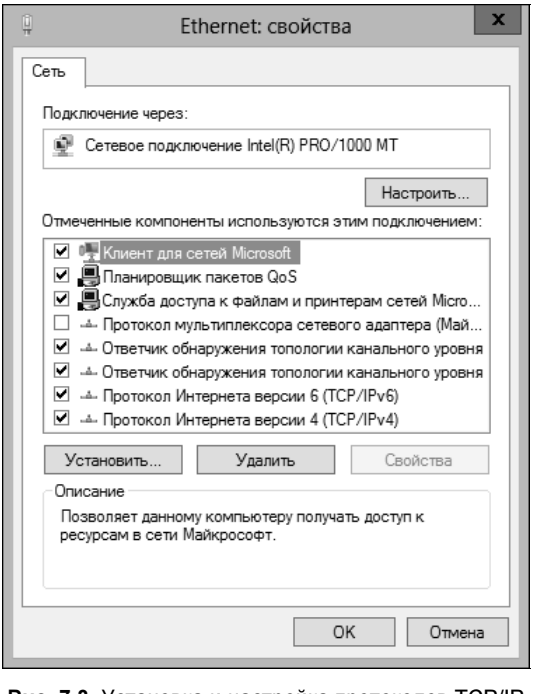


Рис. 7.3. Установка и настройка протоколов TCP/IP

3. На странице **Сетевые подключения** (Network Connections) щелкните правой кнопкой мыши по соединению, параметры которого нужно изменить, выберите команду **Свойства**. Откроется окно свойств для подключения (рис. 7.3).
4. Если в списке отсутствуют **Протокол Интернета версии 6 (TCP/IPv6)** (Internet Protocol Version 6 (TCP/IPv6)) и **Протокол Интернета версии 4 (TCP/IPv4)** (Internet Protocol Version 4 (TCP/IPv4)), нужно установить их. Нажмите кнопку **Установить** (Install), а затем выберите элемент **Протокол** (Protocol) и нажмите кнопку **Добавить** (Add). В окне **Выбор сетевого протокола** (Select Network Protocol) выберите протокол для установки и затем нажмите кнопку **OK**. Если устанавливается и TCP/IPv6, и TCP/IPv4, повторите эту процедуру для каждого протокола.
5. В окне свойств для сетевого подключения убедитесь, что оба протокола (TCP/IPv6 и TCP/IPv4) выбраны, и нажмите кнопку **OK**.
6. При необходимости следуйте инструкциям следующего раздела для настройки сетевых подключений компьютера.

Настройка TCP/IP-сети

Подключение по локальной сети создается автоматически, если в компьютере есть сетевой адаптер и он подключен к сети. Если на компьютере установлено несколько сетевых адаптеров, у каждого из них будет собственное подключение к локальной сети. Если доступных сетевых подключений не существует, следует подключить компьютер к сети или создать подключение другого типа.

Для работы по протоколу TCP/IP компьютеру необходим IP-адрес. В Windows Server 2012 R2 существует несколько способов настройки IP-адреса.

- **Вручную.** IP-адреса, назначаемые вручную, называются *статическими IP-адресами*. Такие фиксированные адреса не изменяются, пока администратор не изменит их. Как правило, статические IP-адреса назначаются серверам Windows. При этом следует настроить также ряд дополнительных параметров, чтобы помочь серверу "освоиться" в сети.
- **Динамически.** Динамические IP-адреса назначаются во время запуска компьютера DHCP-сервером (если он установлен в сети). Время от времени такие адреса могут изменяться. По умолчанию все IP-адреса компьютера считаются динамическими.
- **Альтернативный адрес (только для IPv4).** Когда компьютер настроен на использование DHCPv4, но в сети нет доступного DHCPv4-сервера, ОС Windows Server 2012 R2 автоматически назначает компьютеру частный альтернативный IP-адрес. По умолчанию альтернативный адрес IPv4 назначается из диапазона 169.254.0.1–169.254.255.254 с маской подсети 255.255.0.0. Также можно назначить пользовательский альтернативный IPv4-адрес, что особенно полезно на ноутбуке.

Настройка статического IP-адреса

При назначении статического IP-адреса кроме самого IP-адреса нужно указать маску подсети, а также, при необходимости, шлюз по умолчанию для межсетевого взаимодействия. IP-адрес — это числовой идентификатор компьютера. Схемы IP-адресации

различаются в зависимости от настройки сети, но в большинстве случаев они назначаются на основе конкретных сетевых сегментов.

Адреса IPv6 сильно отличаются от адресов IPv4. В IPv6-адресах первые 64 бита представляют идентификатор сети, а оставшиеся 64 бита — сетевой интерфейс. В IPv4-адресах переменное число первых битов обозначает идентификатор сети, а остальные биты — идентификатор хоста. Допустим, используется протокол IPv4 и компьютер в сегменте сети 10.0.10.0 с маской подсети 255.255.255.0. Первые три группы битов обозначают сетевой идентификатор, а доступные для хостов адреса находятся в диапазоне от 10.0.10.1 до 10.0.10.254. Адрес 10.0.10.255 зарезервирован для широковещательной передачи.

Если компьютер находится в частной сети, не имеющей прямого выхода в Интернет, следует использовать частные IPv4-адреса, приведенные в табл. 7.1.

Таблица 7.1. *Частные сетевые IPv4-адреса*

Идентификатор частной сети	Маска сети	Диапазон сетевых адресов
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.255

Все остальные сетевые IPv4-адреса являются публичными и должны арендоваться или приобретаться. Если сеть подключена напрямую к Интернету, получите диапазон IPv4-адресов от интернет-провайдера и назначайте их компьютерам.

Использование команды *ping* для проверки IP-адреса

Прежде чем назначить статический IP-адрес, убедитесь, что он не занят и не зарезервирован для использования с DHCP. Проверить использование адреса можно при помощи команды `ping`. Откройте командную строку и введите `ping` с IP-адресом, который хотите проверить.

Например, для проверки IPv4-адреса 10.0.10.12 нужно ввести команду:

```
ping 10.0.10.12
```

Команда для проверки IPv6-адреса FEC0::02BC:FF:BECB:FE4F:961D выглядит так:

```
ping FEC0::02BC:FF:BECB:FE4F:9610
```

Если команда `ping` даст положительный ответ, данный IP-адрес уже используется, и необходимо проверить другой адрес. Если время запроса всех четырех попыток команды `ping` истекло, а отклик от компьютера так и не получен, IP-адрес в настоящий момент не активен и, возможно, не используется. Однако запросы `ping` могут блокироваться брандмауэром. Информацию об использовании адреса также может предоставить администратор сети компании.

Настройка статического IPv4- или IPv6-адреса

Каждый установленный сетевой адаптер может быть подключен к одной локальной сети. Подключения создаются автоматически. Для настройки IP-адреса конкретного подключения выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**. На странице **Сетевые подключения** щелкните правой кнопкой мыши по соединению, с которым необходимо работать, выберите команду **Свойства**.
2. Дважды щелкните на протоколе TCP/IPv6 или TCP/IPv4 в зависимости от того, какой тип IP-адреса нужно настроить.
3. Для IPv6-адреса сделайте следующее.
   - Выберите переключатель **Использовать следующий IPv6-адрес** (Use the following IPv6 address) и затем введите IPv6-адрес в поле **IPv6-адрес** (IPv6 address). Введенный вами IPv6-адрес не должен использоваться на каком-либо другом компьютере сети.
   - Поле **Длина префикса подсети** (Subnet prefix length) обеспечивает нормальный доступ компьютера к сети. ОС Windows Server 2012 R2 вставляет в поле **Длина префикса подсети** стандартное значение префикса. Если в сети не используются подсети переменной длины, стандартное значение должно сработать. В противном случае придется привести значение в соответствие с сетью.
4. Для IPv4-адреса сделайте следующее.
   - Выберите переключатель **Использовать следующий IP-адрес** (Use the following IP address) и введите IPv4-адрес в поле **IP-адрес** (IP address). Введенный IPv4-адрес должен быть уникален в пределах сети.
   - Поле **Маска подсети** (Subnet mask) обеспечивает нормальный доступ компьютера к сети. ОС Windows Server 2012 R2 автоматически вставляет в поле значение маски по умолчанию. Если в сети не используются подсети переменной длины, стандартное значение должно сработать. В противном случае придется привести значение в соответствие с сетью предприятия.
5. Если компьютеру необходим выход в другие TCP/IP-сети, в Интернет или другие подсети, укажите IP-адрес шлюза по умолчанию в поле **Основной шлюз** (Default gateway).
6. Доменная система имен (DNS) необходима для разрешения доменных имен. Введите адреса предпочитаемого и альтернативного DNS-серверов в предоставленные поля.
7. Когда закончите, нажмите кнопку **OK** дважды. Повторите этот процесс для других сетевых адаптеров и IP-протоколов, которые необходимо настроить.
8. При использовании IPv4-адресации настройте WINS при необходимости.

Настройка динамических и альтернативных IP-адресов

Хотя у большинства серверов есть статические IP-адреса, можно настроить серверы для использования динамических и альтернативных IP-адресов или их комбинаций. Для настройки динамической и альтернативной адресации выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**. На странице **Сетевые подключения** для каждого установленного сетевого адаптера отображается одно подключение по локальной сети. Подключения создаются автоматически. Если для установленного адаптера сетевое подключение не отображается, проверьте драйвер адаптера. Возможно, он установлен неправильно. Щелкните правой кнопкой мыши по нужному подключению и выберите команду **Свойства**.
2. Дважды щелкните на TCP/IPv6 или TCP/IPv4 в зависимости от типа настраиваемого IP-адреса.
3. Выберите переключатель **Получить IPv6-адрес автоматически** (Obtain an IPv6 address automatically) или **Получить IP-адрес автоматически** (Obtain an IP address automatically) в соответствии с типом настраиваемого IP-адреса. При необходимости установите также переключатель **Получить адрес DNS-сервера автоматически** (Obtain DNS server address automatically) или **Использовать следующие адреса DNS-серверов** (Use the following DNS server addresses), а затем введите адреса основного и альтернативного DNS-серверов в предоставленные поля.
4. При использовании динамического IPv4-адреса на настольном компьютере можно либо использовать автоматический альтернативный адрес, либо вручную настроить альтернативный адрес. На вкладке **Альтернативная конфигурация** (Alternate Configuration) установите переключатель **Автоматический частный IP-адрес** (Automatic private IP address) для автоматического подключения альтернативного IP-адреса. Нажмите кнопку **OK**, а затем кнопку **Закрыть** и пропустите оставшиеся действия.
5. Для задания альтернативного адреса вручную перейдите на вкладку **Альтернативная конфигурация** и выберите переключатель **Настраиваемый пользователем** (User configured), а затем введите IP-адрес, который планируется использовать. Указанный вами IP-адрес должен быть частным IP-адресом, т. е. принадлежать одному из диапазонов, приведенных в табл. 7.1, и быть уникальным в пределах сети. Завершите альтернативную конфигурацию вводом маски сети, шлюза по умолчанию, DNS-сервера и WINS-сервера. Когда закончите, нажмите кнопку **OK**, а затем кнопку **Закрыть**.

Настройка нескольких шлюзов

Для обеспечения отказоустойчивости в случае отказа маршрутизатора можно настроить компьютеры на базе Windows Server 2012 R2 так, что они будут использовать несколько основных шлюзов. При назначении нескольких шлюзов ОС Windows Server 2012 R2 использует метрику шлюза для определения, какой шлюз задействовать и в какое время. Метрика шлюза характеризует затраты на маршрутизацию для данного

шлюза. Первым используется шлюз с наименьшей метрикой. Если компьютер не может установить связь с этим шлюзом, ОС Windows Server 2012 R2 пытается использовать шлюз, следующий по возрастанию метрики.

Выбор лучшего способа настройки нескольких шлюзов зависит от конфигурации сети. Если компьютеры в вашей организации настраиваются при помощи DHCP, вероятно, лучше задавать дополнительные шлюзы через параметры на DHCP-сервере. Если же компьютеры используют статические IP-адреса или нужно задавать IP-адреса шлюзов самостоятельно, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**. На странице **Сетевые подключения** щелкните правой кнопкой мыши по необходимому соединению и выберите команду **Свойства**.
2. Дважды щелкните на TCP/IPv6 или TCP/IPv4 в зависимости от типа настраиваемого IP-адреса.
3. Нажмите кнопку **Дополнительно** (Advanced), чтобы открыть окно **Дополнительные параметры TCP/IP** (Advanced TCP/IP Settings), показанное на рис. 7.4.

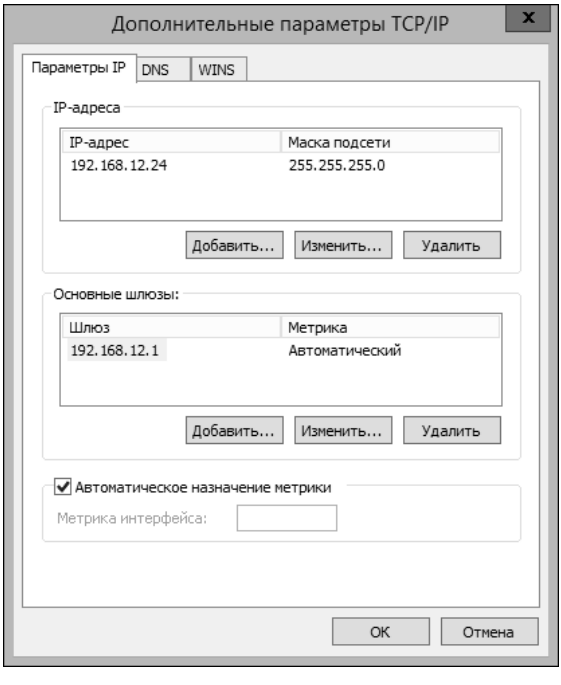


Рис. 7.4. Настройте несколько IP-адресов шлюзов в окне **Дополнительные параметры TCP/IP**

4. В группе **Основные шлюзы** (Default gateways) перечислены шлюзы, которые были настроены вручную (если таковые имеются). При необходимости введите адреса дополнительных шлюзов:
   - нажмите кнопку **Добавить** и введите адрес шлюза в поле **Шлюз** (Gateway);
   - по умолчанию Windows Server 2012 R2 назначает метрику шлюзу автоматически, но можно задать ее вручную. Сбросьте флажок **Автоматическое назначение**

метрики (Automatic metric) и введите метрику в соответствующее поле. Нажмите кнопку **Добавить**;

- повторите приведенные ранее действия для каждого шлюза, который необходимо добавить.

5. Нажмите кнопку **OK**, а затем кнопку **Закрыть**.

Настройка сети для Hyper-V

После установки Hyper-V и создания внешней виртуальной сети ваш сервер будет использовать виртуальный сетевой адаптер для подключения к физической сети. Страница **Сетевые подключения** покажет название исходного сетевого адаптера и новый виртуальный сетевой адаптер. К исходному сетевому адаптеру будет добавлен протокол **Расширяемый виртуальный коммутатор Hyper-V** (Microsoft Virtual Network Switch Protocol). У виртуального сетевого адаптера будут все стандартные протоколы и службы. Имя виртуального сетевого адаптера, отображающееся на странице **Сетевые подключения**, будет таким же, как и имя виртуального сетевого коммутатора, связанного с ним.

Примечание

Для настройки Hyper-V можно создать внутреннюю виртуальную сеть, что позволит обмениваться данными только между сервером и размещенными виртуальными машинами. В этом случае не будет необходимости связывать физический сетевой адаптер с виртуальным сетевым адаптером. Hyper-V связывает виртуальную сетевую службу с физическим адаптером, только когда создается внешняя сеть.

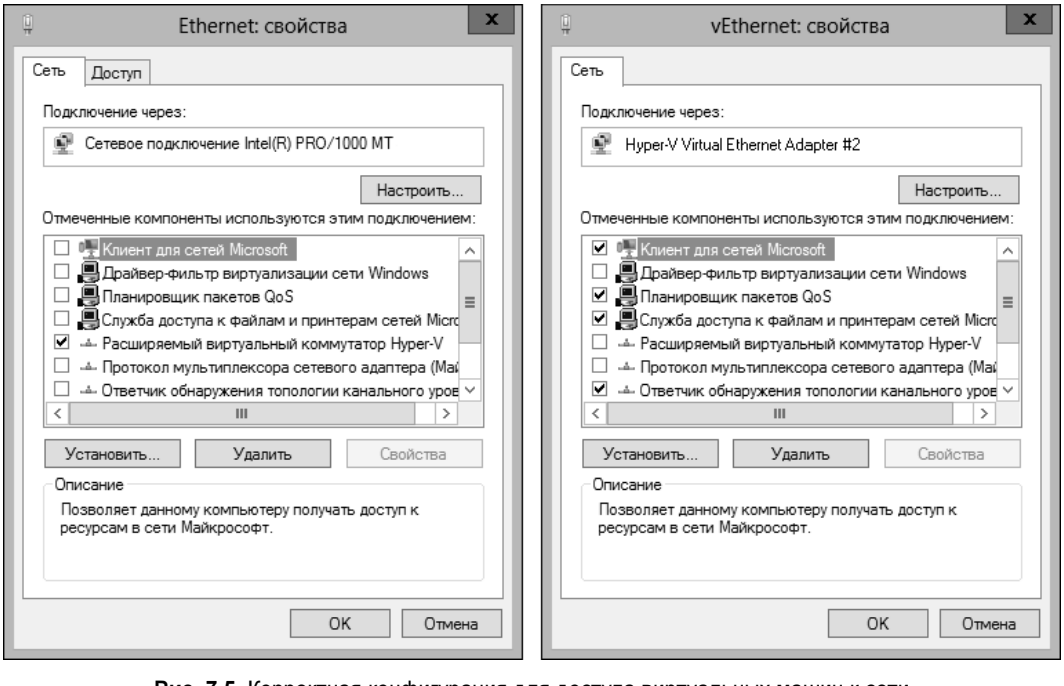


Рис. 7.5. Корректная конфигурация для доступа виртуальных машин к сети

После установки Hyper-V на сервер и включения внешней виртуальной сети будет использоваться переключение виртуальной сети. Как показано на рис. 7.5, у сервера есть сетевое подключение с включенным протоколом **Расширяемый виртуальный коммутатор Hyper-V** (Hyper-V Extensible Virtual Switch Protocol), все остальные компоненты сетевого адаптера выключены. Для виртуального сетевого адаптера основные сетевые компоненты включены, а протокол **Расширяемый виртуальный коммутатор Hyper-V** выключен. Такая конфигурация необходима для корректной коммуникации между сервером и виртуальными машинами. Если эту конфигурацию изменить, виртуальные машины не смогут подключаться к внешней сети.

Управление сетевыми подключениями

Сетевые подключения позволяют компьютерам получать доступ к ресурсам в сети и в Интернете. Для каждого установленного на компьютере сетевого адаптера автоматически устанавливается одно подключение по локальной сети. В этом разделе рассмотрены способы управления подключениями.

Проверка состояния, скорости и активности сетевого подключения

Для проверки состояния сетевого соединения выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**. На странице **Сетевые подключения** щелкните правой кнопкой мыши по соединению и выберите команду **Состояние** (Status).
2. Будет открыто окно **Состояние** (Status) для сетевого подключения. Если подключение выключено или кабель не подключен, это окно не откроется. Включите подключение или подключите сетевой кабель для решения проблемы, а затем снова попытайтесь отобразить окно **Состояние**.

Включение или отключение сетевых подключений

Сетевые подключения создаются и подключаются автоматически. Если нужно отключить соединение так, чтобы его нельзя было использовать, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**. На странице **Сетевые подключения** щелкните правой кнопкой мыши по соединению, которое нужно отключить, выберите команду **Отключить** (Disable) для отключения соединения.
2. Если необходимо включить подключение позже, щелкните правой кнопкой мыши на подключении и выберите команду **Включить** (Enable).

Если необходимо отключиться от сети, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**. На странице **Сетевые подключения** щелкните правой кнопкой мыши по соединению и выберите команду **Отключить**.

2. Если позже понадобится активировать подключение, щелкните по нему правой кнопкой мыши и выберите команду **Подключить** (Connect).

Переименование сетевых подключений

Операционная система Windows Server 2012 R2 автоматически назначает имена сетевым подключениям. На странице **Сетевые подключения** можно переименовать подключение, щелкнув по нему правой кнопкой мыши и выбрав команду **Переименовать** (Rename). После этого нужно ввести новое имя. Если у компьютера много сетевых подключений, используйте информативные имена, чтобы понимать назначение каждого соединения.

ГЛАВА 8

Запуск DCHP-клиентов и серверов

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) используется для упрощения администрирования доменов Active Directory, и в этой главе будет рассказано, как это сделать. Протокол DHCP служит для динамического назначения конфигурационной информации TCP/IP-клиентам сети. Протокол не только экономит время, необходимое на настройку клиентов сети, но и предоставляет централизованный механизм для обновления конфигурации. Для включения DHCP в сети нужно установить и настроить DHCP-сервер. Этот сервер отвечает за назначение необходимой сетевой информации.

Обзор DHCP

Протокол DHCP предоставляет централизованное управление IP-адресацией и многое другое. После установки DHCP с его помощью можно передавать клиентам сети всю необходимую для настройки TCP/IP информацию, а именно: IP-адрес, маску сети, основной шлюз, адреса основного и альтернативного DNS-серверов, адреса основного и альтернативного WINS-серверов, доменное имя компьютера. DHCP-серверы могут назначать динамические адреса IPv4 и/или IPv6 любой сетевой карте (Network Interface Card, NIC) компьютера.

Динамическая IPv4-адресация

Компьютер, использующий динамическую адресацию и настройку параметров протокола IPv4, называется *DHCPv4-клиентом*. При загрузке DHCPv4-клиента из пула IPv4-адресов, выделенного DHCP-серверу, извлекается 32-разрядный IPv4-адрес и назначается клиенту на определенный период времени, называемый *сроком аренды*. По истечении примерно половины срока аренды клиент пытается ее продлить. Если попытка не удалась, до истечения срока аренды клиент ее повторит. В случае неудачи клиент попытается связаться с другим DHCP-сервером. IPv4-адреса, аренда которых не продлена, возвращаются в пул адресов. Если клиенту удается связаться с сервером DHCP, но нет возможности продлить аренду текущего IP-адреса, DHCP-сервер назначает клиенту новый IPv4-адрес.

Доступность DHCP-сервера не влияет на запуск или вход в систему (в большинстве случаев). Даже если DHCP-сервер недоступен, DHCPv4-клиенты могут быть запущены и пользователи могут войти в локальный компьютер. Во время запуска клиент DHCPv4 производит поиск DHCP-сервера. Если DHCP-сервер доступен, клиент получает у него информацию о настройках. Если DHCP-сервер недоступен, но срок аренды еще не истек, клиент "пингует" основной шлюз, записанный в параметрах аренды. Успех операции свидетельствует, что клиент находится в той же сети, в которой он был на момент предоставления аренды. Клиент продолжает пользоваться арендой, как было описано ранее. Неудача команды `ping` говорит о том, что клиент находится в другой сети. В этом случае клиент использует автоматическую настройку IPv4. Она также применяется, если DHCP-сервер не доступен, а срок предыдущей аренды истек.

Автоматическая настройка IPv4 работает следующим образом:

1. Клиентский компьютер выбирает IP-адрес из подсети класса B 169.254.0.0 с маской подсети 255.255.0.0, зарезервированной Microsoft. Перед использованием IPv4-адреса клиент при помощи протокола ARP проверяет, что данный IPv-адрес не занят другим клиентом.
2. Если адрес занят, клиент повторяет шаг 1. После десяти неудачных попыток произойдет ошибка. Если клиент отключен от сети, результат ARP-тестирования всегда будет успешным, поэтому клиент получит первый попавшийся IPv4-адрес.
3. Если выбранный IPv4-адрес доступен, клиент соответствующим образом настраивает сетевой адаптер. Далее, клиент пытается связаться с DHCP-сервером, каждые пять минут посылая в сеть запрос. После успешной установки связи клиента с сервером клиент получает аренду и заново настраивает сетевой интерфейс.

Администратор должен определить, сколько DHCP-серверов требуется установить в сети. Обычно нужно как минимум два DHCP-сервера в физическом сегменте сети. Операционная система Windows Server 2012 R2 поддерживает отказоустойчивость DHCP для IPv4. Отказоустойчивость предполагает высокую доступность DHCP-сервисов путем синхронизации информации об аренде IPv4-адресов между двумя DHCP-серверами в одном из двух режимов.

- **Режим балансировки нагрузки (Load Balance).** В этом режиме администратор указывает процентное соотношение загрузки каждого сервера. Обычно используется соотношение 50/50, чтобы нагрузка на каждый сервер была одинаковой. Но можно использовать другие соотношения, например 60/40, при этом один сервер будет обрабатывать 60% запросов, другой — 40%.
- **Режим горячего резервирования (Hot Standby).** В этом режиме один из серверов действует как основной сервер и обрабатывает DHCP-запросы. Другой сервер является резервным и используется, когда произошел сбой основного сервера или на основном сервере закончились IP-адреса для аренды. Обычно для резервного сервера резервируется 5% IP-адресов.

Настройка отказоустойчивости DHCP предельно проста и не требует кластеризации или какой-либо другой расширенной настройки. Для настройки отказоустойчивости DHCP нужно выполнить следующие действия:

1. Установите и настройте два DHCP-сервера. Серверы должны находиться в одной и той же физической сети.

2. Создайте область DHCPv4 на одном из серверов. Область — это пул IPv4- или IPv6-адресов, которые можно назначить клиентам с помощью аренды.
3. Как только укажете, что другой сервер является партнером отказоустойчивости для области DHCPv4, область будет реплицирована партнеру.

Динамическая IPv6-адресация

Если в процессе установки системы на компьютере обнаружено сетевое оборудование, по умолчанию включаются оба протокола (IPv4 и IPv6). Как было сказано в *главе 7*, IPv4 — основная версия протокола IP, используемая в большинстве сетей, а IPv6 — это следующая версия протокола IP. В протоколе IPv6 используются 128-разрядные адреса. В стандартной конфигурации первые 64 бита — это идентификатор сети, а последние 64 бита — сетевой интерфейс на клиентском компьютере.

Существуют два режима настройки IPv6-адресации средствами DHCP.

- **Режим с отслеживанием состояния (DHCPv6 stateful mode).** В этом режиме DHCPv6-клиенты получают IPv6-адреса и параметры настройки сети от DHCPv6-сервера.
- **Режим без отслеживания состояния (DHCPv6 stateless mode).** В этом режиме DHCPv6-клиенты получают IP-адреса при помощи автоматической настройки, а параметры сетевой конфигурации — при помощи DHCPv6.

Компьютер, получающий от DHCPv6-сервера IPv6-адрес и/или сетевые настройки, называется *DHCPv6-клиентом*. Как и в случае DHCPv4, инфраструктура DHCPv6 состоит из DHCPv6-клиентов, запрашивающих параметры, DHCPv6-серверов, предоставляющих параметры, и агентов-ретрансляторов DHCPv6, которые обеспечивают обмен данными между клиентами и серверами, когда клиенты находятся в подсетях, не имеющих DHCPv6-сервера.

В отличие от DHCPv4, для поддержки DHCPv6 придется настроить IPv6-маршрутизаторы. В основе автоматической настройки DHCPv6 лежат следующие флаги в сообщении, посылаемом ближайшим маршрутизатором:

- флаг Managed Address Configuration (флаг M) — если этот флаг установлен в 1, он предписывает клиенту использовать протокол для получения адресов с отслеживанием состояния;
- флаг Other Stateful Configuration (флаг O) — если этот флаг установлен в 1, он предписывает клиенту использовать протокол для получения других параметров.

Клиент DHCPv6 имеется в любой современной версии Windows (начиная с Vista). Он выстраивает конфигурацию DHCPv6 в зависимости от значений флагов M и O в полученных им объявлениях маршрутизатора. Если в данной сети несколько объявляющих маршрутизаторов, их следует настроить так, чтобы для флагов M и O объявлялись одинаковые значения и префиксы адреса без отслеживания состояния. Все современные[1] настольные и серверные версии Windows содержат IPv6-клиенты и поэтому принимают значения флагов M и O в объявлениях маршрутизаторов.

[1] У клиентов IPv6 под управлением Windows XP или Windows Server 2003 нет DHCPv6-клиента, поэтому они игнорируют флаги M и O в объявлениях маршрутизаторов. — *Прим. пер.*

Можно настроить маршрутизатор IPv6 на установку в объявлениях значения 1 для флага M. Для этого в командной строке с повышенными полномочиями нужно ввести команду:

```
netsh interface ipv6 set interface InterfaceName managedaddress=enabled
```

Здесь *InterfaceName* — фактическое имя интерфейса.

Аналогичным способом можно установить значение 1 для флага O в объявлениях, введя в командной строке с повышенными полномочиями команду:

```
netsh interface ipv6 set interface InterfaceName otherstateful=enabled
```

Если в имени интерфейса присутствуют пробелы, его следует заключить в кавычки, как в следующем примере:

```
netsh interface ipv6 set interface "Wired Ethernet Connection 2" managedaddress=enabled
```

Работая с флагами M и O, помните о следующем.

- Если оба флага имеют значение 0, считается, что в сети нет инфраструктуры DHCPv6. Клиенты используют объявления маршрутизатора для настройки нелокальных адресов и ручную настройку других параметров.
- Если оба флага имеют значение 1, DHCPv6 используется для назначения как IP-адресов, так и других параметров конфигурации. Эта комбинация известна как *режим с отслеживанием состояния*, при котором DHCPv6 назначает IPv6-клиентам адреса.
- Если значение флага M равно 0, а значение флага O — 1, DHCPv6 используется только для назначения прочих параметров конфигурации. Соседние маршрутизаторы настроены на объявление префиксов нелокальных адресов, из которых клиенты IPv6 получают адреса без отслеживания состояния. Эта комбинация известна как *режим без отслеживания состояния*.
- Если значение флага M равно 1, а значение флага O — 0, DHCPv6 используется для настройки IP-адресов, но не других параметров. Поскольку IPv6-адреса следует, как правило, настраивать вместе с другими параметрами, например IPv6-адресами DNS-серверов, данная комбинация применяется редко.

ОС Windows получает динамические IPv6-адреса примерно так же, как и адреса IPv4. Обычно автоматическая настройка IPv6 для клиентов DHCPv6 в режиме с отслеживанием состояния происходит так:

1. Клиентский компьютер получает индивидуальный локальный IPv6-адрес с отслеживанием состояния. Перед использованием IPv6-адреса клиент при помощи ARP проверяет, что данный IPv6-адрес не используется другим клиентом.
2. Если адрес занят, клиент повторяет шаг 1. Помните, что если клиент отключен от сети, результат ARP-тестирования всегда успешный. Поэтому клиент получает первый попавшийся IPv6-адрес.
3. Если выбранный IPv6-адрес доступен, клиент соответствующим образом настраивает сетевой адаптер. Далее клиент пытается связаться с DHCP-сервером, каждые пять минут посылая запрос в сеть. После успешной установки связи клиента с сервером клиент получает аренду и заново настраивает сетевой интерфейс.

Иначе работает автоматическая настройка параметров IPv6 на клиентах DHCPv6 в режиме без отслеживания состояния. В этом случае клиенты DHCPv6 настраивают как локальные адреса, так и дополнительные нелокальные адреса, обмениваясь запросами и объявлениями с соседними маршрутизаторами.

Как и в случае DHCPv4, в протоколе DHCPv6 используются сообщения UDP. Клиенты DHCPv6 принимают сообщения на UDP-порт 546. Серверы и агенты-ретрансляторы DHCPv6 принимают сообщения на UDP-порт 547. Структура сообщений DHCPv6 намного проще, чем структура сообщений DHCPv4 — наследника протокола BOOTP, который служит для поддержки бездисковых рабочих станций.

Сообщения DHCPv6 начинаются с 1-байтового поля Msg-Type (тип сообщения). За ним следует 3-байтовое поле Transaction-ID, определяемое клиентом и служащее для группирования сообщений DHCPv6. За полем Transaction-ID следуют параметры DHCPv6 — идентификаторы сервера и клиента, адреса и прочие параметры.

С каждым параметром DHCPv6 связаны три поля. Поле Option-Code (2 байта) идентифицирует параметр. Поле Option-Len (2 байта) указывает на длину поля Option-Data в байтах. Поле Option-Data содержит данные соответствующего параметра.

У сообщений, пересылаемых между агентами-ретрансляторами и серверами, иная структура. Поле Hop-Count (1 байт) указывает на количество агентов-ретрансляторов, получивших сообщение. Агент, получивший сообщение, может отбросить его, если значение счетчика переходов превысило заданный предел. Поле Link-Address длиной 15 байт содержит нелокальный адрес интерфейса, подключенного к подсети, в которой расположен клиент. На основе информации из поля Link-Address сервер устанавливает корректный диапазон, из которого следует извлекать адрес. Поле Peer-Address длиной 15 байт содержит IPv6-адрес клиента, пославшего сообщение, или агента, ретранслировавшего это сообщение. За полем Peer-Address следуют параметры DHCPv6. Основной параметр Relay Message обеспечивает инкапсуляцию сообщений, передаваемых между клиентом и сервером.

У протокола IPv6 нет широковещательных адресов. Вместо них в DHCPv6 пришел адрес All_DHCP_Relay_Agents_and_Servers, значение которого равно FF02::1:2. Чтобы обнаружить расположение DHCPv6-сервера в сети, клиент DHCPv6 отправляет Solicit-запрос со своего локального адреса. Если в подсети клиента есть DHCPv6-сервер, он получает Solicit-запрос и отправляет соответствующий ответ. Если клиент и сервер находятся в различных подсетях, агент-ретранслятор DHCPv6 в подсети клиента, который получает Solicit-запрос, перешлет его на DHCPv6-сервер.

Проверка назначения IP-адреса

Утилиту Ipconfig можно использовать для проверки назначенного в данный момент IP-адреса и другой конфигурационной информации. Чтобы получить информацию обо всех сетевых адаптерах компьютера, введите команду `ipconfig /all`. Если IP-адрес был назначен автоматически, будет выведено поле **IP-адрес автонастройки** (Autoconfiguration IP Address). В следующем примере автоматически настроен адрес 169.254.98.59:

```
Настройка протокола IP для Windows
  Имя компьютера ..............: DELTA
```

```
  Основной DNS-суффикс.....: microsoft.com
  Тип узла  ...............: Смешанный
  IP-маршрутизация включена ...: Нет
  WINS-прокси включен . . . ...: Нет
  Список поиска суффиксов DNS..: microsoft.com
Ethernet adapter Ethernet:
  DNS-суффикс подключения .....:
  Описание ................: Intel Pro/1000 Network Connection
  Физический адрес.........: 23-15-C6-F8-FD-67
  DHCP включен.............: Да
  Автонастройка включена.....: Да
  IP-адрес автонастройки.....: 169.254.98.59
  Маска подсети ...........: 255.255.0.0
  Основной шлюз ...........:
  DNS-серверы .............:
```

Области адресов

Области адресов — это пулы IPv4- и IPv6-адресов, которые могут арендовать клиенты. Протокол DHCP также позволяет предоставлять адреса в бессрочную аренду. Чтобы зарезервировать конкретный IPv4-адрес, свяжите его с MAC-адресом компьютера, которому должен назначаться этот IPv4-адрес. В результате клиентский компьютер с указанным MAC-адресом будет всегда получать заданный IPv4-адрес. В протоколе IPv6 резервирование осуществляется посредством указания бессрочной аренды.

Администратором создаются области для определения диапазонов IP-адресов, доступных DHCP-клиентам. Например, можно назначить диапазон IP-адресов от 192.168.12.2 до 192.168.12.250 для области Предприятие. В областях допускается использование открытых или частных IPv4-адресов в следующих сетях:

- сети класса A — IP-адреса в диапазоне от 1.0.0.0 до 126.255.255.255;
- сети класса B — IP-адреса в диапазоне от 128.0.0.0 до 191.255.255.255;
- сети класса C — IP-адреса в диапазоне от 192.0.0.0 до 223.255.255.255;
- сети класса D — IP-адреса в диапазоне от 224.0.0.0 до 239.255.255.255.

> ***Примечание***
> IP-адрес 127.0.01 используется для локальной петли (loopback).

В областях можно также использовать локальные одноадресные IPv6-адреса, глобальные одноадресные и многоадресные IPv6-адреса. Локальные одноадресные адреса начинаются с FE80. Многоадресные адреса начинаются с FF00. Глобальные (в пределах сайта) индивидуальные адреса включают все остальные адреса, кроме :: (unspecified) и ::1 (loopback).

Один DHCP-сервер может управлять несколькими областями. Для IPv4-адресов доступны четыре типа областей:

- *обычные области* — используются для назначения адресов в сетях классов A, B и C;

- *многоадресные области* — используются для назначения IP-адресов в сетях IPv4 класса D. Многоадресные IP-адреса применяются в качестве второстепенных, в дополнение к стандартным IP-адресам;
- *суперобласти* — это контейнеры для других областей, которые упрощают управление несколькими областями;
- *области отказоустойчивости* — области между двумя DHCP-серверами для повышения отказоустойчивости, предоставления избыточности и включения балансировки нагрузки.

В IPv6 доступны только обычные области. Хотя можно создавать области, охватывающие несколько сегментов сети, обычно эти сегменты принадлежат к одному классу сети, например, к классу C.

> **Совет**
>
> Не забудьте, что необходимо настроить DHCPv4- и DHCPv6-ретрансляцию для ретрансляции широковещательных DHCPv4- и DHCPv6-запросов между сетевыми сегментами. Настроить агенты ретрансляции можно с помощью протокола RRAS (Routing and Remote Access Service) и агента DHCP-ретрансляции (DHCP Relay Agent Service). Также можно настроить некоторые маршрутизации как агенты ретрансляции.

Установка DHCP-сервера

Динамическая IP-адресация возможна, только если в сети установлен DHCP-сервер. Используя мастер добавления ролей и компонентов (Add Roles and Features Wizard), администратор может установить DHCP-сервер в качестве службы роли, задать ее начальные настройки и авторизовать сервер в Active Directory. Предоставлять клиентам динамические IP-адреса могут только авторизованные DHCP-серверы.

Установка компонентов DHCP

Чтобы сервер под управлением ОС Windows Server 2012 R2 функционировал как DHCP-сервер, выполните следующие действия:

1. Серверу DHCP должны быть назначены статические IPv4- или IPv6-адреса в каждой обслуживаемой ими подсети. Убедитесь, что у сервера есть статические IPv4- или IPv6-адреса.
2. В диспетчере серверов выберите команду меню **Управление | Добавить роли и компоненты** или щелкните по ссылке **Добавить роли и компоненты** (Add Roles and Features) на панели приветствия. Будет запущен мастер добавления ролей и компонентов. Если мастер отобразит страницу **Перед началом работы**, прочитайте приветствие и нажмите кнопку **Далее**.
3. На странице **Выбор типа установки** по умолчанию отмечен переключатель **Установка ролей или компонентов**. Нажмите кнопку **Далее**.
4. На странице **Выбор целевого сервера** можно выбрать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите либо сервер из пула серверов, либо сервер, на котором можно смонтировать виртуальный жест-

кий диск (VHD). Если добавляете роли и компоненты на VHD, нажмите кнопку **Обзор**, а затем используйте окно **Обзор виртуальных жестких дисков** для выбора VHD. Как только будете готовы продолжить, нажмите кнопку **Далее**.

Примечание

В списке серверов будут только серверы под управлением Windows Server 2012 R2 и те, которые были добавлены в диспетчере серверов.

5. На странице **Выбор ролей сервера** выберите роль **DHCP-сервер** (DHCP Server). Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, вы увидите соответствующее диалоговое окно. Нажмите кнопку **Добавить компоненты** для закрытия этого окна и установки требуемых компонентов на сервер. Как только будете готовы продолжить, нажмите кнопку **Далее**.
6. Если на сервере, на который устанавливается роль **DHCP-сервер**, нет необходимых двоичных исходных файлов, сервер получит файлы через службу Windows Update (по умолчанию) или из расположения, указанного в групповой политике.

Примечание

Также можно указать альтернативный источник для исходных файлов. Для этого щелкните по ссылке **Указать альтернативный исходный путь** (Specify An Alternate Source Path), в появившемся окне задайте альтернативный путь и нажмите кнопку **ОК**. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer2012\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2-12\install.wim:4.

7. После просмотра опций установки сохраните их при необходимости, нажмите кнопку **Установить** для начала процесса установки. Страница **Ход установки** позволяет отслеживать процесс инсталляции. Если мастер был закрыт, нажмите значок **Уведомления** (Notifications) в диспетчере серверов, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.
8. Когда мастер закончит установку выбранных ролей и компонентов, страница **Ход установки** сообщит об этом. Просмотрите подробности установки и убедитесь, что все фазы инсталляции завершены успешно.
9. Для завершения установки DHCP-сервера нужна дополнительная конфигурация. Щелкните по ссылке **Завершение настройки DHCP** (Complete DHCP Configuration). Будет запущен мастер настройки DHCP после установки (DHCP Post-Install Configuration Wizard).
10. Панель **Описание** (Description) говорит о том, что для делегирования DHCP-сервера будут созданы группы **Администратор DHCP** (DHCP Administrators) и **Пользователи DHCP** (DHCP Users). Дополнительно, если DHCP-сервер присоединен к домену, его нужно авторизовать в Active Directory. Нажмите кнопку **Далее**.
11. На странице **Авторизация** (Authorization) укажите учетные данные, которые будут использоваться для авторизации этого DHCP-сервера доменными службами Active Directory.

- Текущее имя пользователя отображено в поле **Имя пользователя** (User name). Если у вас имеются привилегии администратора в домене, к которому присоединен DHCP-сервер, и нужно использовать текущие учетные данные, нажмите кнопку **Фиксировать** (Commit) для авторизации сервера с использованием этих учетных данных.
- Если нужно использовать альтернативные учетные данные или нельзя авторизовать сервер с помощью текущих учетных данных, установите флажок **Использовать другие учетные данные** (Use alternate credentials), а затем нажмите кнопку **Указать** (Specify). В окне **Безопасность Windows** (Windows Security) введите имя пользователя и пароль для авторизированной учетной записи и нажмите кнопку **OK**. Нажмите кнопку **Фиксировать** для попытки авторизации сервера с использованием этих учетных данных.
- Если нужно авторизовать DHCP-сервер позже, установите флажок **Пропустить авторизацию AD** (Skip AD Authorization) и нажмите кнопку **Фиксировать**. Помните, что в домене только авторизованные DHCP-серверы могут предоставлять клиентам динамические IP-адреса.

12. Когда мастер закончит постинсталляционную настройку, просмотрите сводку, убедитесь, что все задачи были выполнены успешно, и нажмите кнопку **Закрыть**.
13. Далее нужно перезагрузить службу **DHCP-сервер** на сервере, чтобы группы **Администраторы DHCP** и **Пользователи DHCP** могли использоваться. Для этого на левой панели консоли **Диспетчер серверов** выберите узел **DHCP**. Далее на главной панели, на панели **СЕРВЕРЫ**, выберите DHCP-сервер. На панели **СЛУЖБЫ** щелкните правой кнопкой мыши на службе **DHCP-сервер** и выберите команду **Перезапустить службы** (Restart service).
14. Для завершения инсталляции нужно сделать следующее.
    - Если у сервера есть несколько сетевых карт, пересмотрите привязку сервера и укажите соединения, которые DHCP-сервер будет использовать для обслуживания клиентов *(см. разд. "Настройка привязок сервера" далее в этой главе)*.
    - Настройте параметры, которые будут передаваться DHCPv4- и DHCPv6-клиентам, в том числе 003 Router, 006 DNS Servers, 015 DNS Domain Name и 044 WINS/NBNS Servers *(см. разд. "Установка параметров области" далее в этой главе)*.
    - Создайте и активируйте любые DHCP-области, которые будет использовать сервер *(см. разд. "Создание областей и управление ими" далее в этой главе)*.

Запуск и использование консоли DHCP

После установки DHCP-сервера нужно использовать консоль DHCP для настройки и управления динамической IP-адресацией. В диспетчере серверов в меню **Средства** выберите команду **DHCP**. Основное окно консоли DHCP показано на рис. 8.1. Оно разделено на три панели. Левая панель содержит список DHCP-серверов в домене (выводятся полные доменные имена серверов). Можно развернуть сервер, чтобы увидеть подузлы **IPv4** и **IPv6**. Если развернуть IP-узлы, будут видны области и параметры,

определенные для соответствующей версии IP. Центральная панель показывает расширенное представление выбранного элемента. Правая панель — панель действий, на ней представлены действия, которые можно выполнить над выделенными объектами.

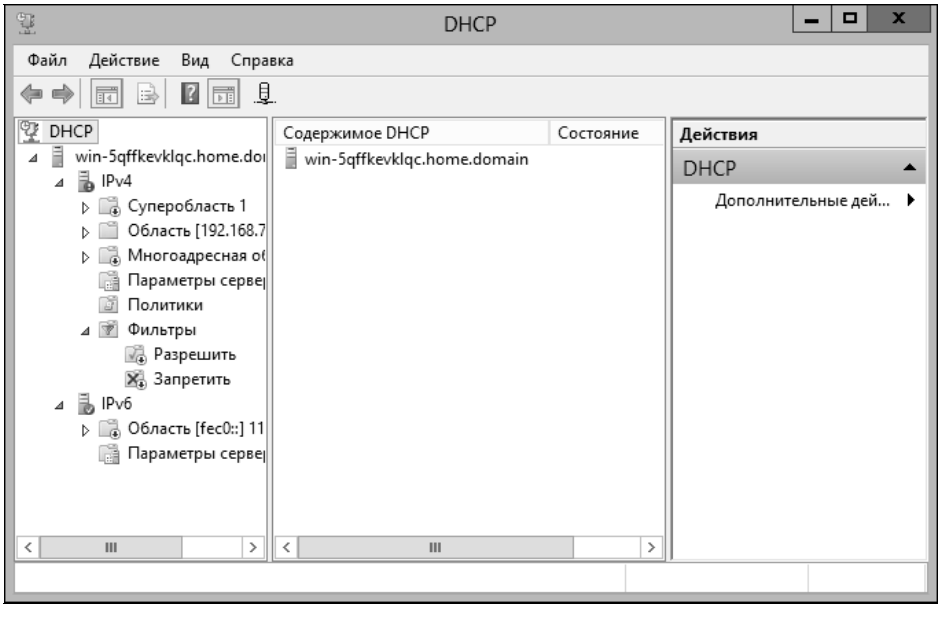


Рис. 8.1. Используйте консоль DHCP для создания и управления конфигурациями DHCP-сервера

Пиктограммы показывают текущее состояние узлов. Для серверов и IP-узлов можно увидеть следующие значки:

- галочка внутри зеленого кружочка указывает, что служба DHCP запущена и сервер активен;
- крестик в красном кружочке указывает, что консоль не может подключиться к серверу. Служба DHCP остановлена или сервер недоступен;
- красная стрелка вниз указывает, что DHCP-сервер не был авторизован;
- синий значок предупреждения указывает, что состояние сервера изменилось.

Для областей можно увидеть такие значки:

- красная стрелка вниз говорит о том, что область не была активирована;
- синий значок предупреждения указывает, что состояние области изменилось.

Подключение к удаленным DHCP-серверам

При запуске консоли DHCP она подключится к локальному DHCP-серверу, но в ней не будет записей удаленных DHCP-серверов. Подключиться к удаленным серверам можно с помощью следующих действий:

1. Щелкните правой кнопкой мыши на узле **DHCP** в дереве консоли и выберите команду **Добавить сервер** (Add Server). Откроется окно, показанное на рис. 8.2.

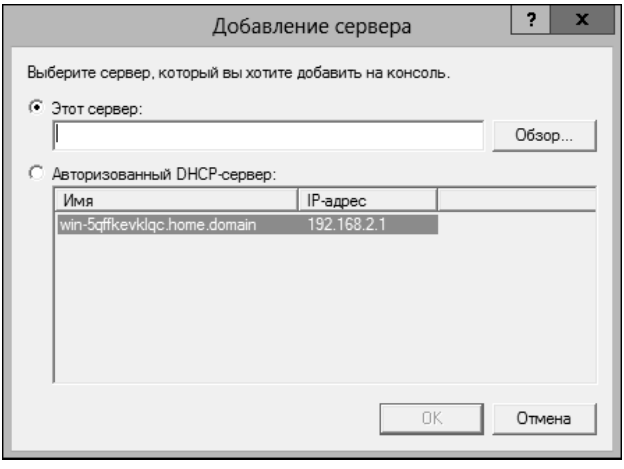


Рис. 8.2. Если нужного DHCP-сервера нет в списке, добавьте его с помощью команды **Добавить сервер**

2. Выберите переключатель **Этот сервер** (This server), а затем введите IP-адрес или имя компьютера DHCP-сервера, к которому нужно подключиться.
3. Нажмите кнопку **OK**. Запись для DHCP-сервера будет добавлена в дерево консоли.

Совет

При работе с удаленными серверами некоторые определенные опции недоступны для выбора. Для решения этой проблемы нужно просто обновить информацию о сервере. Для этого щелкните правой кнопкой мыши на узле сервера и выберите команду **Обновить** (Refresh).

Запуск и остановка DHCP-сервера

Управление DHCP-серверами осуществляется при помощи службы **DHCP-сервер** (DHCP Server). Как и любую другую службу, ее можно запустить, остановить, приостановить и перезапустить в узле **Службы** оснастки **Управления компьютером** или из командной строки. Кроме того, службой **DHCP-сервер** можно управлять в консоли DHCP. Щелкните правой кнопкой мыши на сервере, которым хотите управлять, разверните подменю **Все задачи** (All Tasks) и выберите нужную команду: **Запустить** (Start), **Остановить** (Stop), **Приостановить** (Pause), **Продолжить** (Resume) или **Перезапустить** (Restart).

Примечание

Можно также использовать консоль **Диспетчер серверов** для запуска и останова DHCP-сервера. Выберите **DHCP** на панели слева, далее на панели **СЕРВЕРЫ** выберите DHCP-сервер. Затем на панели **СЛУЖБЫ** щелкните правой кнопкой мыши по записи **DHCP-сервер** и выберите команду **Запустить службы** (Start Service), **Остановить службы** (Stop Service), **Приостановить службы** (Pause Service), **Возобновить работу служб** (Resume Service) или **Перезапустить службы** (Restart Service).

Авторизация DHCP-сервера в Active Directory

Прежде чем использовать DHCP-сервер в домене, его необходимо авторизовать в Active Directory. Авторизация сервера означает, что серверу разрешено назначать динамические IP-адреса в домене. В Windows Server 2012 R2 авторизация требуется для предотвращения обслуживания клиентов неавторизованными DHCP-серверами.

Авторизовать сервер могут только **Администраторы предприятия** (Enterprise Admins). Чтобы авторизовать DHCP-сервер, щелкните правой кнопкой мыши по элементу сервера в дереве консоли DHCP и выберите команду **Авторизовать** (Authorize). Чтобы лишить сервер авторизации, щелкните на нем правой кнопкой мыши и выберите команду **Запретить** (Unauthorize).

В командной строке Windows PowerShell, запущенной с полномочиями администратора, можно использовать команду `Add-DhcpServerInDC` для авторизации DHCP-сервера. Параметр `-DnsName` используется для указания имени сервера, который нужно авторизовать. Также указать сервер можно и по IP-адресу, используя параметр `-IpAddress`. Примеры использования команды `Add-DhcpServerInDC`:

```
Add-DhcpServerInDC -DnsName CorpSvr03.cpandl.com
Add-DhcpServerInDC -IpAddress 192.168.1.1
```

Для удаления авторизации используется команда `Remove-DhcpServerInDC`. Основной ее синтаксис такой же.

Настройка DHCP-серверов

После установки нового DHCP-сервера необходимо его настроить и оптимизировать для сетевого окружения. Для IPv4 и IPv6 предоставляются разные настройки.

Настройка привязок сервера

На сервере с несколькими сетевыми адаптерами имеется несколько подключений по локальной сети, по каждому из которых он может предоставлять параметры DHCP. Иногда работа DHCP на всех доступных подключениях не требуется. Допустим, на сервере имеются два подключения — 100 Мбит/с и 1 Гбит/с, и нужно пропускать трафик DHCP через подключение со скоростью 1 Гбит/с.

Чтобы связать DHCP с конкретным подключением, выполните следующие действия:

1. В консоли DHCP разверните узел сервера, с которым хотите работать. Щелкните правой кнопкой мыши на узле **IPv4** или **IPv6** и выберите команду **Свойства**.
2. В диалоговом окне свойств IPv4 или IPv6 перейдите на вкладку **Дополнительно** (Advanced) и нажмите кнопку **Привязки** (Add/Remove Bindings).
3. В диалоговом окне **Привязки** (Bindings) отображен список доступных сетевых подключений DHCP-сервера. Чтобы DHCP-сервер использовал подключение, установите соответствующий флажок. Чтобы подключение не использовалось, сбросьте соответствующий флажок. Если в этом окне не отображаются сетевые соединения

для протокола, с которым осуществляется работа, убедитесь, что серверу назначен статический адрес для того протокола.

4. Два раза нажмите кнопку **OK**, когда закончите.

Обновление DHCP-статистики

В консоли DHCP представлена статистика доступности и использования адресов IPv4 и IPv6. В консоли DHCP можно просмотреть эту статистику, развернув узел сервера, с которым нужно работать. Для этого щелкните правой кнопкой мыши на узле **IPv4** или **IPv6** (в зависимости от того, статистику по какому протоколу нужно просмотреть) и выберите команду **Отобразить статистику** (Display Statistics).

По умолчанию обновление статистики происходит только при запуске консоли DHCP, а также если выбрать сервер и нажать кнопку **Обновление** на панели инструментов. Если нет желания постоянно следить за DHCP, потребуется автоматическое обновление статистики. Для его настройки выполните следующие действия:

1. В консоли DHCP разверните узел сервера, щелкните правой кнопкой мыши на узле **IPv4** или **IPv6** и выберите команду **Свойства**.
2. На вкладке **Общие** установите флажок **Автоматически обновлять статистику каждые** (Automatically Update Statistics Every) и введите интервал обновления в часах и минутах. Нажмите кнопку **OK**.

Аудит и устранение неисправностей DHCP

По умолчанию Windows Server 2012 R2 настроен на аудит процессов DHCP. Аудит отслеживает процессы и запросы DHCP и ведет журналы аудита.

Журналы аудита помогут в устранении неисправностей DHCP-сервера. По умолчанию оба протокола — IPv4 и IPv6 — производят запись в разные журналы. Стандартное расположение журналов DHCP — *%SystemRoot%*\System32\DHCP. В этой папке находятся журналы для каждого дня недели. Файл журнала для протокола IPv4 понедельника называется DhcpSrvLog-Mon.log, файл журнала вторника — Dhcp-SrvLog-Tue.log, и т. д. Для протокола IPv6 файлы называются DhcpV6SrvLog-Mon.log (для понедельника), DhcpV6SrvLog-Tue.log (для вторника) и т. д.

При запуске DHCP-сервера или наступлении нового дня в файл журнала записывается заголовок. В заголовке содержится сводка событий DHCP и значение событий. При остановке и запуске службы **DHCP-сервер** очистка файла журнала может не произойти. Она обязательно выполняется по прошествии 24 часов с момента последней записи в журнал. Не нужно отслеживать использование дискового пространства службой **DHCP-сервер**. Она по умолчанию настроена на ограничение используемого пространства.

Включить или отключить аудит DHCP можно с помощью следующих действий:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, щелкните правой кнопкой мыши на узле **IPv4** или **IPv6** и выберите команду **Свойства**.
2. На вкладке **Общие** установите флажок **Вести журнал аудита DHCP** (Enable DHCP audit logging), а затем нажмите кнопку **OK**.

По умолчанию журналы DHCP хранятся в папке *%SystemRoot%*\System32\DHCP. Можно изменить расположение журналов, выполнив следующие действия:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, щелкните правой кнопкой мыши на узле **IPv4** или **IPv6** и выберите команду **Свойства**.
2. Перейдите на вкладку **Дополнительно**. Поле **Журнал аудита** (Audit log file path) показывает текущее расположение журналов аудита. Введите имя новой папки или нажмите кнопку **Обзор** для ее выбора.
3. Нажмите кнопку **OK**. Операционной системе Windows Server 2012 R2 понадобится перезапустить службу **DHCP-сервер**. Когда система попросит разрешения это сделать, нажмите кнопку **Да**. Служба будет остановлена и запущена снова.

В службе **DHCP-сервер** есть система самоконтроля, проверяющая использование дискового пространства. По умолчанию максимальный размер всех журналов DHCP-сервера составляет 70 Мбайт. Размер каждого журнала составляет одну седьмую часть от этого пространства. При достижении сервером предела в 70 Мбайт или при превышении отдельным журналом выделенного для него пространства регистрация деятельности DHCP прекращается, пока не будут очищены файлы журналов или место не освободится каким-либо иным способом. Обычно это происходит в начале нового дня, когда сервер очищает файл журнала прошлой недели.

Ключи реестра, контролирующие объем журнала и другие параметры, находятся в разделе `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters`.

Следующие параметры управляют регистрацией событий:

- `DhcpLogFilesMaxSize` — максимальный размер всех журналов. Стандартное значение — 70 Мбайт;
- `DhcpLogDiskSpaceCleanupInterval` — частота проверки использования диска и очистки журнала. Стандартный интервал — 60 минут;
- `DhcpLogMinSpaceOnDisk` — порог свободного пространства, необходимый для записи в журнал. Если свободное пространство на диске меньше установленного значения, запись в журнал временно прекращается. Стандартное значение — 20 Мбайт.

Параметр `DhcpLogMinSpaceOnDisk` не создается автоматически. Необходимо создать его самостоятельно и задать подходящее для сети значение.

Интеграция DHCP и DNS

Служба DNS используется для разрешения имен компьютеров в доменах Active Directory и Интернете. Благодаря протоколу динамического обновления DNS, администратор избавлен от необходимости регистрировать DHCP-клиентов в DNS вручную. Протокол позволяет клиенту или DHCP-серверу при необходимости регистрировать в DNS записи прямого и обратного просмотра. При работе DHCP по умолчанию DHCP-клиенты автоматически обновляют соответствующие DNS-записи после получения IP-адреса в аренду. Записи клиентов, работающих в предыдущих версиях Windows, после предоставления аренды обновляются DHCP-сервером. Можно изменить этот порядок для DHCP-сервера в целом или для конкретной области.

Защита имен — дополнительная функция в Windows Server 2012 R2. Благодаря защите имен, DHCP-сервер регистрирует записи от имени клиента, только если никакой другой клиент с этой DNS-информацией не зарегистрирован. Можно настроить защиту имени для IPv4 и IPv6 на уровне сетевого адаптера или на уровне области. Параметры защиты имен, настроенные на уровне области, имеют приоритет над параметрами на уровне IPv4 или IPv6.

Защита имени предназначена для предотвращения занятия имен. Занятие имен происходит, когда компьютер с ОС, отличной от Windows, регистрирует в DNS имя, которое уже используется на компьютере под управлением Windows. Включив защиту имен, можно предотвратить занятие имени не-Windows-компьютерами. Хотя занятие имени не представляет собой проблему при использовании Active Directory, лучше все-таки включить защиту имен во всех Windows-сетях.

Защита имени основана на идентификаторе конфигурации динамического узла (Dynamic Host Configuration Identifier, DHCID) и поддержке записи ресурса DHCID (DHCID RR) в DNS. Запись DHCID RR — это запись ресурса, хранимая в DNS и сопоставляющая имена для предотвращения дублированной регистрации. Запись ресурса используется службой DHCP для хранения идентификатора компьютера и других сведений об имени, например записи A/AAAA компьютера. Сервер DHCP может запросить сравнение и отклонить регистрацию компьютера с другим адресом, пытающегося зарегистрировать имя с существующей записью DHCID.

Можно просмотреть и изменить параметры глобальной DNS-интеграции так:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, щелкните правой кнопкой мыши на узле **IPv4** или **IPv6** и выберите команду **Свойства**.
2. Перейдите на вкладку **Служба DNS** (DNS). На рис. 8.3 показаны значения DNS-интеграции по умолчанию для IPv4 и IPv6. Поскольку параметры настроены по умолчанию, обычно их не нужно модифицировать.

> ***Внимание!***
>
> Конфигурация по умолчанию, регистрирующая и обслуживающая записи обоих типов — A и PTR, подразумевает, что администратор настроил зоны обратного просмотра (reverse lookup) для предприятия. Если это не так, зарегистрировать или обновить PTR-записи не получится. Чтобы предотвратить сбой при регистрации или обновлении PTR-записей, нужно отключить динамическое обновление PTR-записей. Если это сделать в свойствах IPv4, тогда динамическое обновление будет отключено сразу для всех IPv4-областей. Альтернативно, можно отключить динамическое обновление выборочно — только для определенных областей.

3. При желании можно включить или выключить функцию защиты имен. При включенной защите имен DHCP-сервер регистрирует записи о клиенте, если никакой другой клиент с этой DNS-информацией не зарегистрирован. Для включения или отключения защиты имен нажмите кнопку **Настроить** (Configure). В окне **Защита имен** (Name Protection) установите или сбросьте флажок **Включить защиту имен** (Enable name protection) и нажмите кнопку **OK**.

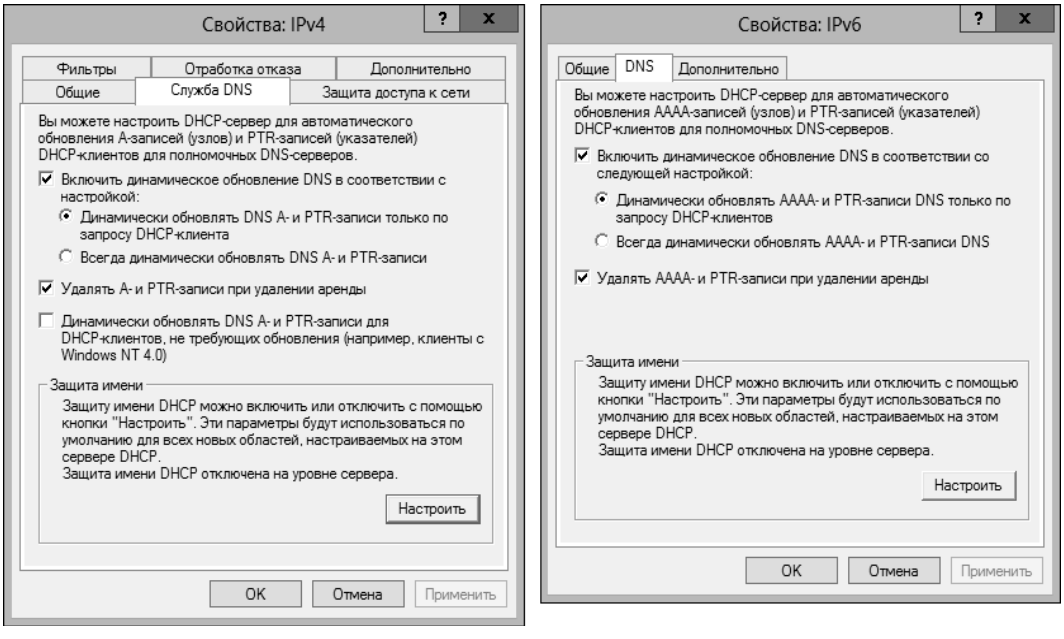


Рис. 8.3. Параметры DNS-интеграции для IPv4 и IPv6

Интеграция DHCP и NAP

Протокол защиты сетевого адреса (Network Address Protection, NAP) разработан для защиты сети от клиентов, не имеющих достаточных собственных средств защиты. Простейший способ включить NAP на DHCP — настроить DHCP-сервер как сервер политики сети (Network Policy Server, NPS). Для этого нужно установить роль **Сервер политики сети** (Network Policy Server), настроить политику объединения DHCP и NAP и включить NAP на DHCP. При этом на сетевых компьютерах осуществляется включение NAP, но не его настройка.

Интегрировать NAP и DHCP можно так:

1. На сервере, который будет функционировать как сервер политики сети, используя мастер добавления ролей и компонентов, нужно установить как минимум роль **Сервер политики сети**.
2. В консоли сервера политики (nps.msc), доступной в меню **Средства** диспетчера серверов (команда **Сервер политики сети** (Network Policy Server)), выберите узел **NPS (локально)** (NPS (Local)), нажмите кнопку **Настройка (NAP)** (Configure NAP) на главной панели. Будет запущен мастер **Настройка NAP** (Configure NAP Wizard).
3. Из списка **Способ сетевого подключения** (Network connection method) выберите **Протокол DHCP** (Dynamic Host Configuration Protocol (DHCP)). Как показано на рис. 8.4, имя политики по умолчанию будет **NAP DHCP**. Нажмите кнопку **Далее**.
4. На странице **Укажите серверы принудительной защиты доступа к сети под управлением DHCP-сервера** (Specify NAP Enforcement Servers Running DHCP Server) нужно указать все DHCP-серверы в сети.

- Нажмите кнопку **Добавить**. В окне **Новый RADIUS-клиент** (New RADIUS Client) введите имя удаленного сервера в поле **Понятное имя** (Friendly name). Затем введите DNS-имя удаленного DHCP-сервера в поле **Адрес** (Address). Нажмите кнопку **Проверить** (Verify), чтобы проверить адрес.
- На панели **Общий секрет** (Shared Secret) выберите переключатель **Создать** (Generate), чтобы создать длинный пароль с общим секретом. Нужно будет ввести эту фразу в политику **NAP DHCP** на всех удаленных DHCP-серверах. Поэтому обязательно запишите ее или сохраните в файле, в безопасном месте. Можно также скопировать эту фразу в Блокнот и сохранить в безопасном расположении. Нажмите кнопку **OK**.

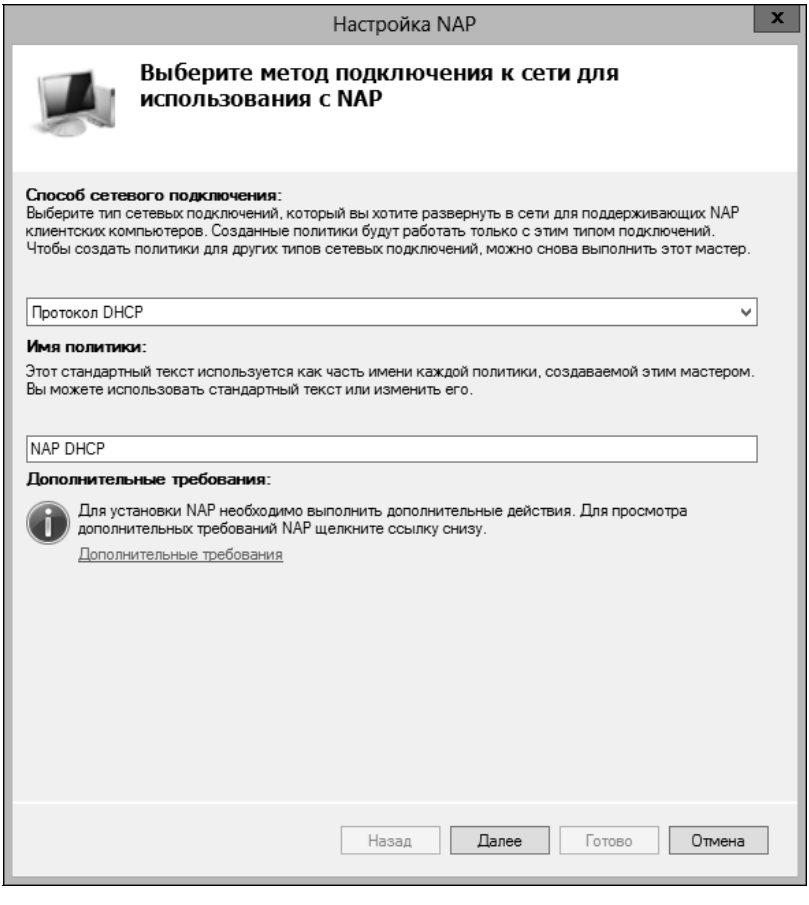


Рис. 8.4. Настройка политики NAP для локального DHCP-сервера

5. Нажмите кнопку **Далее**. На странице **Укажите DHCP-области** (Specify DHCP Scopes) можно задать DHCP-области, к которым будет применена политика. Если области не указаны, политика применяется ко всем областям на выбранных DHCP-серверах, на которых включена NAP. Нажмите кнопку **Далее** дважды для пропуска страницы **Группы компьютеров** (Configure Machine Groups).

6. На странице **Задайте группу сервера исправлений NAP и URL-адрес** (Specify A NAP Remediation Server Group And URL) нажмите кнопку **Создать группу** (New Group) для определения группы серверов исправлений. На этих серверах хранятся обновления программного обеспечения для NAP-клиентов. В предоставленное текстовое поле введите URL веб-страницы с инструкцией, как привести компьютер в соответствие с политикой NAP. Убедитесь, что клиенты DHCP могут открыть эту страницу. Нажмите кнопку **Далее**.
7. На странице **Определите политику работоспособности NAP** (Define NAP Health Policy) укажите, как будет работать политика работоспособности NAP. В большинстве случаев можно оставить параметры по умолчанию, запрещающие вход в сеть клиентам, которые не совместимы с NAP. Для NAP-совместимых клиентов будет проводиться проверка работоспособности и автоматическое исправление, что позволяет им получать необходимые обновления программного обеспечения. Нажмите кнопку **Далее**, а затем кнопку **Готово**.

Можно настроить параметры NAP для всего сервера или для отдельных областей. Для просмотра или изменения глобальных параметров NAP выполните следующие действия:

1. В консоли DHCP разверните узел необходимого DHCP-сервера. Щелкните правой кнопкой мыши по узлу **IPv4** и выберите команду **Свойства**.
2. На вкладке **Защита доступа к сети** (Network Access Protection) (рис. 8.5) нажмите кнопку **Включить во всех областях** (Enable on all scopes) или кнопку **Отключить во всех областях** (Disable on all scopes), чтобы включить или выключить NAP для всех областей сервера.

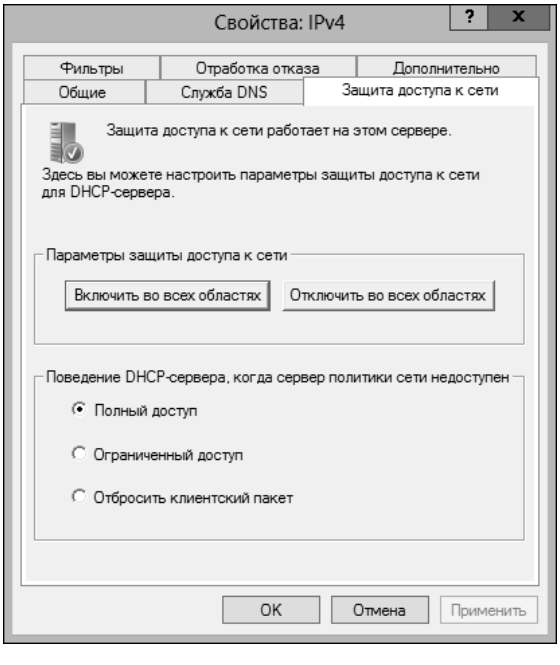


Рис. 8.5. Вкладка **Защита доступа к сети** контролирует параметры защиты для DHCP

Примечание

Когда локальный DHCP-сервер также является сервером NAP, NAP-сервер всегда должен быть доступен. Если сервер не настроен, как сервер сетевой политики, или сервер DHCP неспособен связаться с заданным NAP-сервером, на вкладке **Защита доступа к сети** будет отображено сообщение об ошибке.

3. Выберите следующие опции, чтобы указать, как должен действовать DHCP-сервер, если NPS-сервер недоступен. Затем нажмите кнопку **OK** для сохранения параметров.
   - **Полный доступ** (Full Access) — предоставляет DHCP-клиентам полный (неограниченный) доступ к сети. Клиентам позволено выполнять любые разрешенные действия.
   - **Ограниченный доступ** (Restricted Access) — предоставляет DHCP-клиентам ограниченный доступ к сети. Клиенты могут работать только с тем сервером, к которому они подключены.
   - **Отбросить клиентский пакет** (Drop Client Packet) — блокирует запросы клиентов и запрещает выход клиентов в сеть. У клиентов нет доступа к ресурсам сети.

Для просмотра и изменения параметров NAP для отдельных областей выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Затем разверните узел **IPv4**.
2. Щелкните правой кнопкой мыши по нужной области и выберите команду **Свойства**.
3. На вкладке **Защита доступа к сети** установите переключатель **Включить для этой области** (Enable For This Scope) или **Отключить для этой области** (Disable For This Scope), чтобы включить или отключить NAP для данной области.
4. Если NAP включен и нужно использовать профиль NAP, отличный от стандартного, установите переключатель **Использовать особый профиль** (Use Custom Profile) и введите имя профиля, например Alternate NAP DHCP.
5. Нажмите кнопку **OK** для сохранения параметров.

Как избежать конфликтов IP-адресов

Часто причиной проблем с DHCP становятся конфликты IPv4-адресов. Двум компьютерам в сети нельзя иметь один IP-адрес. Если компьютеру назначен уже использованный IPv4-адрес, один или оба компьютера могут быть отключены от сети. Точнее, компьютер, уже использующий IPv4-адрес, будет и дальше его применять, а любой другой компьютер, который пытается использовать этот же адрес, будет блокирован от его применения.

Чтобы своевременно обнаруживать конфликты, а еще лучше, избежать их, включите обнаружение конфликтов IPv4-адресов, выполнив следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой мыши по узлу **IPv4** и выберите команду **Свойства**.
2. На вкладке **Дополнительно** присвойте параметру **Число попыток определения конфликтов** (Conflict Detection Attempts) отличное от нуля значение. Оно опреде-

ляет количество проверок IP-адреса, которые DHCP-сервер проводит перед предоставлением адреса клиенту. Сервер DHCP проверяет IP-адреса, отправляя по сети запросы PING.

Практический совет

Одиночный (unicast) IP-адрес — это стандартный IP-адрес для сетей классов A, B и C. Когда DHCP-клиент запрашивает аренду, DHCP-сервер проверяет свой пул на наличие свободных адресов и назначает клиенту аренду на доступном IPv4-адресе. По умолчанию сервер проверяет список текущих аренд для определения, свободен ли адрес. Он не опрашивает физически сеть, чтобы узнать, используется ли адрес. К сожалению, в больших загруженных сетевых окружениях администраторы могут назначить этот IPv4-адрес другому компьютеру или оффлайн-компьютер может появиться в сети с арендой, которая еще не просрочена, даже если DHCP-сервер считает, что ее срок уже истек. Чтобы уменьшить конфликты этих типов, установите значение для параметра **Число попыток определения конфликтов** больше 0.

Сохранение и восстановление конфигурации DHCP

После того как будут установлены все необходимые DHCP-параметры, нужно сохранить конфигурацию DHCP так, чтобы можно было впоследствии ее восстановить на DHCP-сервере. Для сохранения конфигурации введите следующую команду в командной строке:

```
netsh dump DHCP > dhcpconfig.dmp
```

В этом примере dhcpconfig.dmp — имя сценария конфигурации. После создания этого сценария восстановить конфигурацию можно с помощью следующей команды, введенной в командной строке:

```
netsh exec dhcpconfig.dmp
```

Совет

Также можно использовать эту технику для настройки другого DHCP-сервера с такой же конфигурацией. Просто скопируйте сценарий конфигурации в папку на другом сервере и выполните его.

Можно сохранить и восстановить конфигурацию DHCP и с помощью консоли DHCP. Для сохранения конфигурации щелкните правой кнопкой мыши на записи DHCP-сервера, выберите команду **Архивировать** (Backup), а в открывшемся окне выберите папку для архива и нажмите кнопку **OK**. Для восстановления конфигурации щелкните правой кнопкой мыши на записи сервера и выберите команду **Восстановить** (Restore). Используя открывшееся окно, выберите архивную папку и нажмите кнопку **OK**. Нажмите кнопку **Да** для подтверждения своих намерений.

В командной строке Windows PowerShell для сохранения конфигурации используется команда `Export-DhcpServer`. Ее базовый синтаксис следующий:

```
Export-DhcpServer -ComputerName ServerID -File SavePath
```

Здесь *`ServerID`* — DNS-имя или IP-адрес DHCP-сервера, а *`SavePath`* — это путь и имя файла, в который будет записана конфигурация. Если не указать сервер, тогда будет использован локальный сервер. Если не указать путь, то конфигурация будет записана

в текущий рабочий каталог. В следующем примере конфигурация локального DHCP-сервера сохраняется в файл dhcpconfig.dmp, находящийся в каталоге d:\dhcp\scripts:

```
Export-DhcpServer-File d:\dhcp\scripts\dhcpconfig.dmp
```

Для восстановления конфигурации используется команда `Import-DhcpServer`. Синтаксис этой команды следующий:

```
Import-DhcpServer -ComputerName ServerID -BackupPath CurrentConfigSavePath -File SavePath
```

Здесь *`SavePath`* — это путь и имя файла, в котором сохранена конфигурация, а *`CurrentConfigSavePath`* задает путь, куда будет сохранена текущая конфигурация перед импортом и перезаписью существующих настроек. В следующем примере текущие настройки будут сохранены в d:\dhcp\backup\origconfig.dmp, после чего будет восстановлена конфигурация из d:\dhcp\scripts\dhcpconfig.dmp:

```
Import-DhcpServer-BackupPath d:\dhcp\backup\origconfig.dmp
-File d:\dhcp\scripts\dhcpconfig.dmp
```

Управление областями DHCP

После установки DHCP-сервера нужно настроить области, которые сервер DHCP будет использовать. Области — это пул IP-адресов, которые могут быть переданы в аренду клиентам. Как было рассказано в *разд. "Области адресов" ранее в этой главе*, для IPv4 можно создать суперобласти, обычные, многоадресные и отказоустойчивые области, для IPv6 можно создать только обычные области.

Суперобласти: создание и управление

Суперобласть служит контейнером для областей IPv4 так же, как и организационное подразделение является контейнером для объектов Active Directory. Суперобласти помогают управлять имеющимися в сети областями и также обеспечивают поддержку DHCP-клиентов в одной физической сети, где используются множественные логические IP-сети или же когда создаете суперобласти для распространения IP-адресов из разных логических сетей в один сегмент физической сети. С помощью суперобласти можно активировать или деактивировать сразу несколько областей. Также в суперобласти можно просматривать статистику для всех областей сразу, вместо того чтобы проверять статистику для каждой области отдельно.

Создание суперобластей

После создания как минимум одной обычной или многоадресной IPv4-области можно создать суперобласть так:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, а затем щелкните правой кнопкой мыши по узлу **IPv4**, выберите команду **Создать суперобласть** (New Superscope) (эта команда появится, если есть хотя бы одна обычная или многоадресная область). Будет запущен мастер создания суперобласти (New Superscope Wizard). Нажмите кнопку **Далее**.
2. Выберите имя суперобласти и нажмите кнопку **Далее**.

3. Выберите области, которые нужно добавить в суперобласть. Для выбора области просто щелкните на ней в списке **Доступные области** (Available Scopes). Чтобы выбрать несколько областей, щелкните по ним при нажатых клавишах <Shift> или <Ctrl>.
4. Нажмите кнопку **Далее**, а затем кнопку **Готово**.

Добавление областей в суперобласть

Добавлять области в суперобласть можно как в процессе ее создания, так и позже. Чтобы добавить область в существующую суперобласть, выполните следующие действия:

1. Правой кнопкой мыши щелкните на области, которую хотите добавить в существующую суперобласть, и выберите команду **Добавить в суперобласть** (Add To Superscope).
2. В диалоговом окне **Добавление области к суперобласти** (Add Scope To A Superscope) выберите суперобласть.
3. Нажмите кнопку **OK**.

Удаление областей из суперобласти

Для удаления области из суперобласти выполните следующие действия:

1. Щелкните правой кнопкой мыши на области, которую нужно удалить из суперобласти, и выберите команду **Удалить из суперобласти** (Remove From Superscope).
2. Нажмите кнопку **Да**, чтобы подтвердить действие. Если это была последняя область, суперобласть будет автоматически удалена.

Включение и отключение суперобласти

При включении или отключении суперобласти также включаются или отключаются сразу все входящие в нее области. Для включения области щелкните на ней правой кнопкой мыши и выберите команду **Активировать** (Activate). Для отключения суперобласти щелкните на ней правой кнопкой мыши и выберите команду **Деактивировать** (Deactivate).

Удаление суперобласти

При удалении суперобласти удаляется только ее контейнер, но не сами области. Если необходимо удалить области, которые входят в состав суперобласти, нужно сделать это отдельно. Для удаления суперобласти щелкните на ней правой кнопкой мыши и выберите команду **Удалить** (Delete). Нажмите кнопку **Да** для подтверждения своих намерений.

Создание областей и управление ими

Область предоставляет пул адресов для DHCP-клиентов. Обычная область — это область с адресами сетей классов A, B или C. Многоадресная область — это область с адресами сетей класса D. Хотя обычные и многоадресные области создаются по-

разному, в управлении они мало чем отличаются друг от друга. Основное отличие состоит в том, что многоадресные области не позволяют резервировать адреса, а также задавать дополнительные параметры WINS, DNS, маршрутизации и т. д.

Создание обычной области для IPv4-адресов

Создать обычную область для IPv4-адресов можно с помощью следующих действий:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, далее щелкните правой кнопкой мыши на узле **IPv4**. Если необходимо автоматически добавить новую область в суперобласть, выделите ее, а затем щелкните правой кнопкой мыши на нужной суперобласти.
2. В контекстном меню выберите команду **Создать область** (New Scope). Будет запущен мастер создания области (New Scope Wizard). Нажмите кнопку **Далее**.
3. Введите имя и описание области, а затем нажмите кнопку **Далее**.
4. Введите начальный и конечный адреса области в поля **Начальный IP-адрес** (Start IP address) и **Конечный IP-адрес** (End IP address) на странице **Диапазон адресов** (IP Address Range).

   Примечание

   Как правило, не нужно включать в область адреса x.x.x.0 и x.x.x.255, которые обычно зарезервированы для сетевых адресов и широковещательных сообщений соответственно. Поэтому необходимо использовать адреса от 192.168.10.1 до 192.168.10.254 вместо 192.168.10.0–192.168.10.255.

5. После указания диапазона IP-адресов поля **Длина** (Length) и **Маска подсети** (Subnet mask) будут заполнены автоматически (рис. 8.6). Если подсети не используются, оставьте стандартные значения.

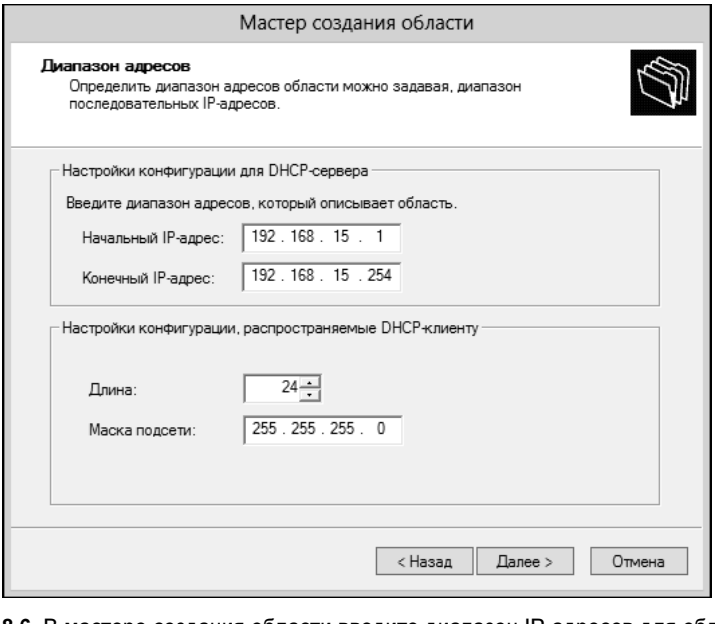


Рис. 8.6. В мастере создания области введите диапазон IP-адресов для области

6. Нажмите кнопку **Далее**. Если введенный диапазон IP-адресов охватывает разные сети, будет предоставлена возможность создать суперобласть, содержащую различные области для каждой сети. Нажмите кнопку **Да**, чтобы принять это предложение, и перейдите к шагу 8. Если была допущена ошибка, нажмите кнопку **Назад** (Back), чтобы исправить введенный диапазон IP-адресов.
7. Используйте поля **Начальный IP-адрес** (Start IP address) и **Конечный IP-адрес** (End IP address) на странице **Добавление исключений и задержка** (Add Exclusions and Delay), чтобы определить диапазоны IP-адресов, которые будут исключены из области. Можно исключить диапазоны адресов так.
   - Для определения диапазона введите начальный и конечный адреса в поля **Начальный IP-адрес** (Start IP address) и **Конечный IP-адрес** (End IP address) и нажмите кнопку **Добавить**. Чтобы исключить один IP-адрес, введите его и как начальный, и как конечный IP-адрес.
   - Исключенные диапазоны адресов отображаются в списке **Исключаемый диапазон адресов** (Excluded address range).
   - Для удаления диапазона исключения выберите его в списке **Исключаемый диапазон адресов** (Excluded address range) и затем нажмите кнопку **Удалить**.
8. Нажмите кнопку **Далее**. Укажите продолжительность аренды для диапазона адресов, используя поля **Дней** (Day(s)), **часов** (Hour(s)), **минут** (Minutes). Продолжительность аренды по умолчанию составляет 8 дней. Нажмите кнопку **Далее**.

   Примечание

   Слишком длительный срок аренды IP-адреса может снизить эффективность DHCP и стать причиной преждевременного исчерпания диапазона доступных IP-адресов, особенно в сетях с мобильными пользователями и другими типами компьютеров, которые не являются постоянными членами сети. Достаточная продолжительность аренды для большинства сетей — до трех дней.

9. У администратора есть возможность настроить общие параметры DHCP для DNS, WINS, шлюзов и т. д. Если нужно настроить эти параметры сейчас, выберите переключатель **Да, настроить эти параметры сейчас** (Yes, I want to configure these options now). В противном случае выберите **Нет, настроить эти параметры позже** (No, I will configure these options later) и пропустите шаги 10–15.
10. Нажмите кнопку **Далее**. Первым делом необходимо указать основной шлюз. В поле **IP-адрес** введите IP-адрес основного шлюза и нажмите кнопку **Добавить**. Повторите этот процесс для других шлюзов по умолчанию.
11. Сначала клиенты будут использовать первый шлюз в списке. Если он недоступен, клиенты попытаются получить доступ к следующему шлюзу и т. д. С помощью кнопок **Вверх** (Up) и **Вниз** (Down) можно изменять порядок шлюзов.
12. Нажмите кнопку **Далее**. Настройте параметры DNS для DHCP-клиентов, как показано на рис. 8.7. Введите имя родительского домена, который следует использовать для разрешения не полностью определенных имен компьютеров.
13. В поле **IP-адрес** введите IP-адрес основного DNS-сервера, а затем нажмите кнопку **Добавить**. Повторите этот процесс, чтобы указать дополнительные серверы. Здесь

опять же порядок записей определяет, какой из IP-адресов будет использован в первую очередь. При необходимости, измените порядок с помощью кнопок **Вверх** и **Вниз**. Нажмите кнопку **Далее**.

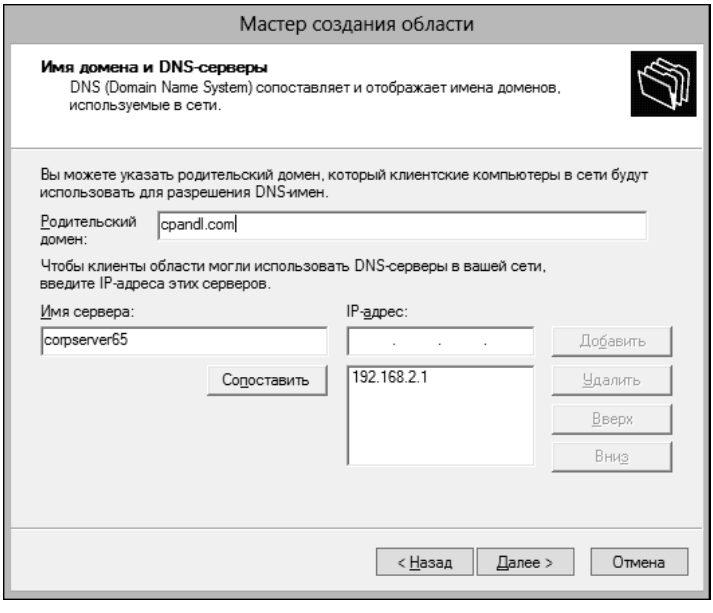


Рис. 8.7. Используйте страницу **Имя домена и DNS-серверы** для настройки параметров DNS по умолчанию для DNS-клиентов

Совет

Если знаете имя сервера, вместо IP-адреса можно ввести его в поле **Имя сервера** (Server name), а затем нажмите кнопку **Сопоставить** (Resolve). После этого добавьте IP-адрес сервера, нажав кнопку **Добавить**.

14. Параметры WINS задаются аналогично. Нажмите кнопку **Далее**.
15. Если нужно активировать область, установите переключатель **Да, я хочу активировать эту область сейчас** (Yes, I want to activate this scope now). В противном случае установите переключатель **Нет, я активирую эту область позже** (No, I will activate this scope later).
16. Нажмите кнопку **Готово** для завершения процесса.

Создание обычной области для IPv6-адресов

Создать обычную область для IPv6-адресов можно с помощью мастера создания области. При настройке DHCP для IPv6 нужно ввести идентификатор сети и предпочтительное значение. Обычно первые 64 бита IPv6-адреса идентифицируют сеть, и это 64-битное значение нужно ввести в окне мастера создания области. Предпочитаемое значение устанавливает приоритет этой области относительно других областей. Область с наименьшим предпочитаемым значением будет использована первой. Далее будет использована область со вторым наименьшим значением и т. д.

Создать обычную область для IPv6-адресов можно с помощью следующих действий:

1. В консоли DHCP разверните узел сервера, с которым нужно работать.
2. Щелкните правой кнопкой мыши на узле **IPv6**. Из появившегося контекстного меню выберите команду **Создать область**. Будет запущен мастер создания области. Нажмите кнопку **Далее**.
3. Введите имя и описание области, а затем нажмите кнопку **Далее**.
4. На странице **Префикс области** (Scope Prefix) (рис. 8.8) введите 64-битный префикс сети и затем установите предпочтение. Нажмите кнопку **Далее**.

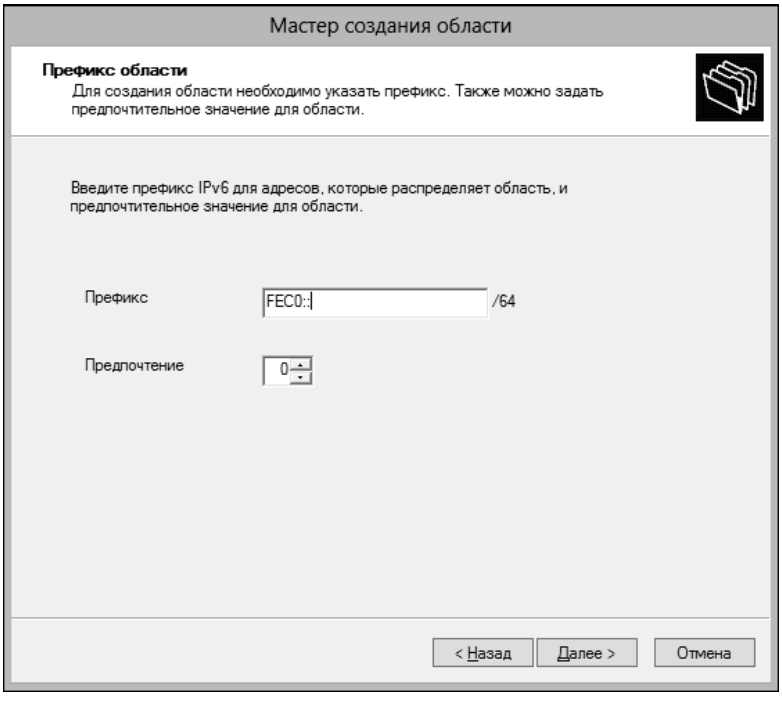


Рис. 8.8. В окне мастера создания области введите префикс сети и предпочтение

5. Используйте поля **Начальный IPv6-адрес** и **Конечный IPv6-адрес** на странице **Добавление исключений** (Add Exclusions) для определения диапазонов IPv6-адресов, которые должны быть исключены из диапазона. Исключить несколько диапазонов можно так.
   - Чтобы определить диапазон исключения, в разделе **Исключенный диапазон адресов** (Exclusion Range) введите начальный и конечный адреса в поля **Начальный IPv6-адрес** и **Конечный IPv6-адрес** и нажмите кнопку **Добавить**. Чтобы исключить один IPv6-адрес, введите его как начальный IPv6-адрес и нажмите кнопку **Добавить**.
   - Отследить исключенные диапазоны адресов можно в списке **Исключенный диапазон адресов** (Excluded Address Range).

- Чтобы удалить исключение, выделите диапазон в списке **Исключенный диапазон адресов** (Excluded Address Range) и нажмите кнопку **Удалить**.

6. Нажмите кнопку **Далее**. Динамические IPv6-адреса могут быть временными и постоянными. Постоянный адрес похож на зарезервированный адрес. На странице **Аренда области** (Scope Lease) (рис. 8.9) укажите сроки аренды для временных и постоянных адресов в разделах **Основное время жизни** (Preferred Life Time) и **Допустимое время жизни** (Valid Life Time). Основное время жизни — это типичный интервал, в течение которого будет действительна аренда. Допустимое время жизни — это максимальный интервал, в течение которого будет действительна аренда. Нажмите кнопку **Далее**.

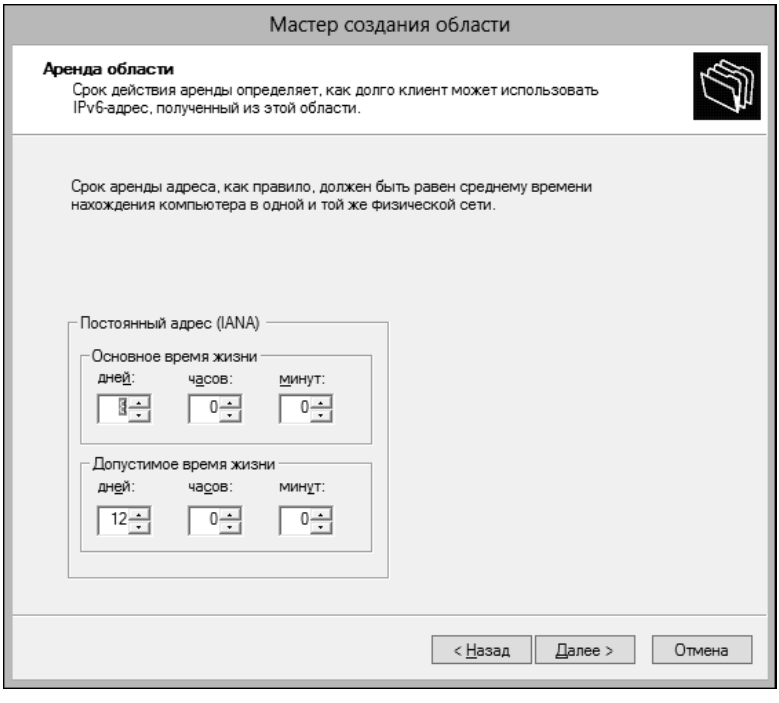


Рис. 8.9. Укажите продолжительность постоянной аренды

Примечание

Слишком длительный срок аренды IP-адреса может снизить эффективность DHCP. Достаточная продолжительность постоянной аренды — от 8 до 30 дней.

7. Если нужно активировать область, выберите переключатель **Да** на панели **Активировать область сейчас** (Activate Scope Now), а затем нажмите кнопку **Готово**. В противном случае выберите переключатель **Нет** и нажмите кнопку **Готово**.

Создание многоадресных областей

Для создания многоадресной области выполните следующие действия:

1. В консоли DHCP разверните узел сервера, с которым нужно работать. Выберите и затем щелкните правой кнопкой мыши на узле **IPv4**. Если необходимо добавить но-

вую область в суперобласть, вместо этого выберите и щелкните правой кнопкой мыши на суперобласти.

2. Из контекстного меню выберите команду **Создать многоадресную область** (New Multicast Scope). Будет запущен мастер создания многоадресной области (New Multicast Scope Wizard). Нажмите кнопку **Далее**.
3. Введите имя и описание области, а затем нажмите кнопку **Далее**.
4. Поля **Начальный IP-адрес** и **Конечный IP-адрес** определяют допустимый диапазон IP-адресов для области. Введите начальный и конечный адреса в эти поля. Необходимо определить многоадресную область, используя IP-адреса класса D. Это означает, что допустимый диапазон IP-адресов — от 224.0.0.0 до 239.255.255.255.
5. Сообщения, посылаемые компьютерами при помощи многоадресных IP-адресов, имеют конкретное время жизни (Time to Live, TTL). Им определяется максимальное количество маршрутизаторов, через которые может пройти сообщение. Стандартное значение TTL равно 32. В большинстве сетей этого достаточно. Если имеется большая сеть, увеличьте это значение, чтобы оно соответствовало реальному количеству маршрутизаторов.
6. Нажмите кнопку **Далее**. Если была допущена ошибка, нажмите кнопку **Назад** и измените указанный диапазон IP-адресов.
7. На странице **Добавление исключений** (Add Exclusions) задайте диапазоны IP-адресов, которые следует исключить из области. Можно исключить несколько диапазонов.
   - Чтобы определить исключаемый диапазон, введите начальный и конечный адреса в поля **Начальный IP-адрес** и **Конечный IP-адрес** и нажмите кнопку **Добавить**.
   - Отследить исключенные диапазоны адресов можно в списке **Исключаемые адреса**.
   - Чтобы удалить исключенный диапазон, выделите диапазон в списке **Исключаемые адреса** и нажмите кнопку **Удалить**.
8. Нажмите кнопку **Далее**. Укажите продолжительность аренды для области в днях, часах и минутах. По умолчанию продолжительность аренды составляет 30 дней. Нажмите кнопку **Далее**.

   Примечание

   Если нет богатого опыта работы с многоадресной передачей, не нужно изменять стандартное значение продолжительности аренды. Способ использования многоадресной аренды отличается от обычной аренды. Многие компьютеры могут использовать многоадресные IP-адреса, и все эти компьютеры могут арендовать IP-адрес. Хорошая продолжительность многоадресной аренды для большинства сетей — от 30 до 60 дней.

9. Если нужно активировать область, выберите переключатель **Да**, а затем нажмите кнопку **Далее**. В противном случае выберите переключатель **Нет** и нажмите кнопку **Далее**.
10. Нажмите кнопку **Готово** для завершения процесса.

Установка параметров области

Параметры области позволяют точно контролировать функционирование области и установить настройки TCP/IP по умолчанию для клиентов, которые используют область. Например, можно использовать параметры области для автоматической установки адресов DNS-серверов на клиентах сети. Также можно определить основные шлюзы, WINS и многое другое. Параметры области применяются только к обычным областям, но не к многоадресным.

Установить параметры области можно следующими способами:

- глобально для всех областей, задав параметры по умолчанию DHCP-сервера;
- отдельно для каждой области путем установки ее параметров;
- отдельно для каждого клиента путем установки параметров резервирования;
- для класса клиентов путем настройки класса пользователей.

У областей IPv4 и IPv6 разные параметры. Параметры области используют иерархию для определения применения тех или иных параметров. Предыдущий список показывает эту иерархию. В общем, она объясняет следующее:

- параметры, заданные для конкретной области, перезаписывают глобальные параметры;
- параметры клиента перезаписывают параметры области и глобальные параметры;
- параметры класса клиента перезаписывают все другие параметры.

Просмотр и назначение параметров сервера

Параметры сервера применяются ко всем настроенным областям на определенном DHCP-сервере. Можно просмотреть и задать эти параметры так:

1. В консоли DHCP дважды щелкните на сервере, параметры которого нужно изменить, а затем разверните его узлы **IPv4** и **IPv6** в дереве консоли.
2. Чтобы просмотреть его текущие параметры, выберите узел **Параметры сервера** (Server Options), который находится или в узле **IPv4**, или в узле **IPv6** в зависимости от того, с каким типом адреса нужно работать. Текущие параметры будут отображены на правой панели.
3. Чтобы назначить новые параметры сервера, щелкните правой кнопкой мыши по узлу **Параметры сервера** и из контекстного меню выберите команду **Настроить параметры** (Configure Options). Откроется окно **Параметры: сервер** (Server Options). В области **Доступный параметр** (Available Options) отметьте флажком первую опцию, которую нужно настроить. Затем, когда она будет выбрана, введите требуемую информацию на панели **Ввод данных** (Data Entry). Повторите этот процесс для настройки всех остальных параметров.
4. Нажмите кнопку **OK** для сохранения изменений.

Просмотр и назначение параметров области

Параметры области применяются к отдельной области и переопределяют параметры сервера по умолчанию. Просмотреть и изменить параметры области можно так:

1. В консоли DHCP разверните запись области.
2. Для просмотра текущих параметров выберите узел **Параметры области** (Scope Options). На панели справа будут отображены заданные параметры.
3. Для назначения новых параметров щелкните правой кнопкой мыши на узле **Параметры области** и выберите команду **Настроить параметры**. В области **Доступный параметр** отметьте флажком первую опцию, которую нужно настроить. Затем, когда она будет выбрана, введите требуемую информацию на панели **Ввод данных** (рис. 8.10). Повторите этот процесс для настройки всех остальных параметров.
4. Нажмите кнопку **OK**.

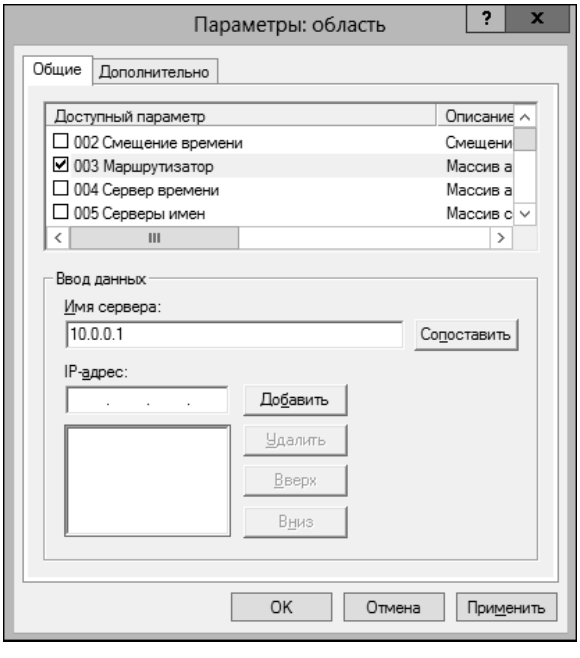


Рис. 8.10. Выберите параметр, который нужно настроить в окне **Параметры: область**, и введите требуемую информацию в область **Ввод данных**

Просмотр и назначение параметров резервирования

Администратор может назначить параметры резервирования клиенту, у которого есть зарезервированные IPv6- или IPv4-адреса. Эти параметры закрепляются за конкретным клиентом и перекрывают параметры сервера и области. Чтобы просмотреть и изменить параметры резервирования, выполните следующие действия:

1. В консоли DHCP разверните запись области, с которой нужно работать.
2. Дважды щелкните на папке **Резервирование** (Reservations) для области.
3. Чтобы просмотреть текущие параметры, щелкните на нужном резервировании. Настроенные параметры будут отображены в правой панели.
4. Чтобы назначить новые параметры, щелкните правой кнопкой мыши на резервировании и выберите команду **Настроить параметры**. Откроется диалоговое окно **Па-**

раметры: резервирование (Reservation Options). В разделе **Доступный параметр** установите флажок первого настраиваемого параметра и введите нужную информацию в поля раздела **Ввод данных**. Повторите этот шаг для настройки других параметров.

Изменение областей

Изменить существующую область можно с помощью следующих действий:

1. В консоли DHCP дважды щелкните на сервере, с которым нужно работать, а затем разверните его узлы **IPv4** или **IPv6**. Будут отображены области, настроенные для сервера.
2. Щелкните правой кнопкой мыши на области, которую нужно изменить, и выберите команду **Свойства**.
3. Теперь можно изменить параметры области. Имейте в виду следующее.
   - При изменении обычной области IPv4 у администратора есть возможность задать неограниченный срок аренды. Это негативно сказывается на эффективности выделения IP-адресов DHCP-сервером. Постоянная аренда не заканчивается, пока она не будет отключена физически или не будет отключена область. В результате возникает риск постепенно исчерпать все адреса, в особенности при расширении сети. Лучшей альтернативой неограниченному сроку аренды является использование резервирований, причем только для тех клиентов, которые действительно нуждаются в постоянном IP-адресе.
   - При изменении многоадресных областей у администратора есть возможность задать время жизни области. Оно определяет количество времени, в течение которого будет действительна область. По умолчанию многоадресные области действительны, пока они включены. Чтобы изменить этот параметр, перейдите на вкладку **Время жизни многоадресной области** (Lifetime), установите переключатель **Срок действия многоадресной области истекает** (Multicast scope expires on) и задайте срок действия.

Активация и деактивация областей

В консоли DHCP неактивная область помечается белым кружком с красной стрелкой вниз. У активной области значок, как у обычной папки.

Чтобы активировать неактивную область, щелкните на ней правой кнопкой мыши в консоли DHCP и выберите команду **Активировать**. Чтобы деактивировать активную область, щелкните на ней правой кнопкой мыши в консоли DHCP и выберите команду **Деактивировать**.

> ***Внимание!***
>
> Деактивация выключает область, но не прекращает текущие аренды клиентов. Если нужно завершить аренды, следуйте инструкциям из *разд. "Освобождение адресов и аренды" далее в этой главе*.

Включение протокола BOOTP

Протокол BOOTP (Bootstrap Protocol) — протокол для динамической IPv4-адресации, который является предшественником DHCP. Нормальные области не поддерживают BOOTP.

Чтобы включить поддержку BOOTP, выполните следующие действия:

1. Щелкните на обычной области для IPv4-адресов правой кнопкой мыши, а затем выберите команду **Свойства**.
2. На вкладке **Дополнительно** выберите переключатель **обоих типов серверов** (Both) для поддержки и DHCP-клиентов, и BOOTP-клиентов.
3. При необходимости установите продолжительность аренды для BOOT-клиентов и нажмите кнопку **OK**.

> ***Примечание***
>
> Типичное время аренды для BOOTP-адреса гораздо больше, чем для DHCP-адреса. Для BOOTP-адреса срок в 30 дней является хорошим компромиссом, однако некоторые сценарии могут потребовать неограниченного срока аренды.

Удаление области

Удаление области удаляет область из DHCP-сервера без возможности восстановления. Для удаления области выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши на области, которую нужно удалить, а затем выберите команду **Удалить**.
2. Для подтверждения действия нажмите кнопку **Да**.

Настройка нескольких областей в сети

Можно настроить несколько областей в одной сети. Один DHCP-сервер или несколько DHCP-серверов могут обслуживать эти области. Однако при работе с несколькими областями важно помнить, что диапазоны этих областей не должны накладываться. У каждой области должен быть уникальный диапазон адресов. Если это не так, одинаковые IP-адреса могут быть назначены разным DHCP-клиентам, что может вызвать серьезные проблемы в сети.

Чтобы понять, как можно использовать несколько областей, рассмотрим следующий сценарий, в котором каждый сервер имеет свою DHCP-область и обслуживает свой диапазон в одной и той же сети:

- сервер A — 192.168.10.1–192.168.10.99;
- сервер B — 192.168.10.100–192.168.10.199;
- сервер C — 192.168.10.200–192.168.10.254.

Каждый из этих серверов отвечает на сообщения обнаружения DHCP и любой из них может назначить IP-адреса клиентам. Если один из серверов откажет, другие серверы могут продолжить предоставлять DHCP-услуги сети. Чтобы предоставить отказоустойчивость и избыточность, можно использовать области, как будет показано в следующем разделе.

Создание и управление отказоустойчивыми областями

Отказоустойчивые области разбиваются между двумя DHCP-серверами и повышают отказоустойчивость, предоставляют избыточность, а также обеспечивают балансиров-

ку нагрузки. Используя отказоустойчивую область, можно идентифицировать два DHCP-сервера, которые разделят область. Если один из серверов откажет или станет перегруженным, другой сервер может занять его место, продолжая назначать IP-адреса и возобновлять уже существующие аренды. Отказоустойчивая область помогает также и при балансировке нагрузки серверов.

Создание отказоустойчивой области

Отказоустойчивые области применяются только к IPv4-адресам. Можно разбить одну обычную область или суперобласть, содержащую несколько областей.

Создавать отказоустойчивую область нужно на DHCP-сервере, который должен действовать как основной сервер. Такая область создается путем разделения существующей области или суперобласти. При создании отказоустойчивой области нужно определить сервер-партнер, с которым будет разделена область основного сервера. Этот дополнительный сервер действует как вторичный сервер для области. Поскольку отказоустойчивые области — это улучшение со стороны серверов, никакая дополнительная настройка DHCP-клиентов не требуется.

Способ разделения области зависит от настроек отказоустойчивой области.

- **Оптимизация для балансировки нагрузки.** Для отказоустойчивой области, оптимизированной для балансировки нагрузки, установлена минимальная задержка (или вообще нет задержки) в ее свойствах. Без задержки и основной, и вторичный серверы могут ответить на запросы DHCP DISCOVER от DHCP-клиентов. Это позволяет самому быстрому серверу отвечать на запрос и принимать DHCPOFFER первому. Если один из серверов станет недоступен или будет перегружен и не сможет ответить на запросы, другой сервер обработает запросы и продолжит назначение адресов, пока обычный процесс не будет восстановлен. Для балансировки нагрузки нужно установить *режим балансировки нагрузки.*
- **Оптимизация для отказоустойчивости.** Отказоустойчивая область, оптимизированная для отказоустойчивости, имеет довольно большую задержку в настройках области. Задержка на вторичных серверах позволяет серверу отвечать с задержкой на запросы DHCP DISCOVER от DHCP-клиентов. Задержка на вторичном сервере позволяет первичному серверу отвечать и принимать DHCPOFFER первому. Однако если основной сервер недоступен или перегружен и не может ответить на запрос, вторичный сервер обрабатывает запросы и продолжает распределять адреса, пока основной сервер снова не станет доступным. Для отказоустойчивости выберите *режим горячей замены*.

Создать отказоустойчивую область[1] можно так:

1. В консоли DHCP подсоединитесь к основному DHCP-серверу отказоустойчивой области. Дважды щелкните на записи основного сервера, а затем разверните узел **IPv4**.

[1] В дополнение к книге настоятельно рекомендую ознакомиться с пошаговым процессом, позволяющим настроить отказоустойчивость DHCP с нуля*:* **http://technet.microsoft.com/ru-ru/library/hh831385.aspx**. — *Прим. пер.*

2. Область, с которой нужно работать, уже должна быть определена. Щелкните на обычной области или на суперобласти правой кнопкой мыши и выберите команду **Настройка отработки отказа** (Configure Failover). Откроется окно **Настройка отработки отказа** (Configure Failover Wizard). Нажмите кнопку **Далее**.
3. Затем нужно указать сервер-партнер. Нажмите кнопку **Добавить сервер** (Add Server). Используйте параметры окна **Добавление сервера** (Add Server), чтобы выбрать вторичный сервер для отказоустойчивой области, а затем нажмите кнопку **OK**. Сбросьте флажок **Повторно использовать отношения отработки отказа, настроенные для этого сервера** (Reuse existing failover relationships), а затем нажмите кнопку **Далее** для продолжения.
4. На странице **Создайте новое отношение отработки отказа** (Create A New Failover Relationship) (рис. 8.11) используйте раскрывающийся список **Режим** (Mode) для установки режима отказоустойчивости (**Балансировка нагрузки** (Load balance) или **Горячая замена** (Hot standby)).
5. Если выбран режим **Балансировка нагрузки**, используйте предоставленные параметры для установки того, как IP-адреса будут распределяться между каждым из серверов. Несколько примеров:
   - 80/20 — лучше всего работает, когда нужно, чтобы один из серверов обрабатывал большую часть нагрузки, а второй сервер заменял бы его в случае необходимости;

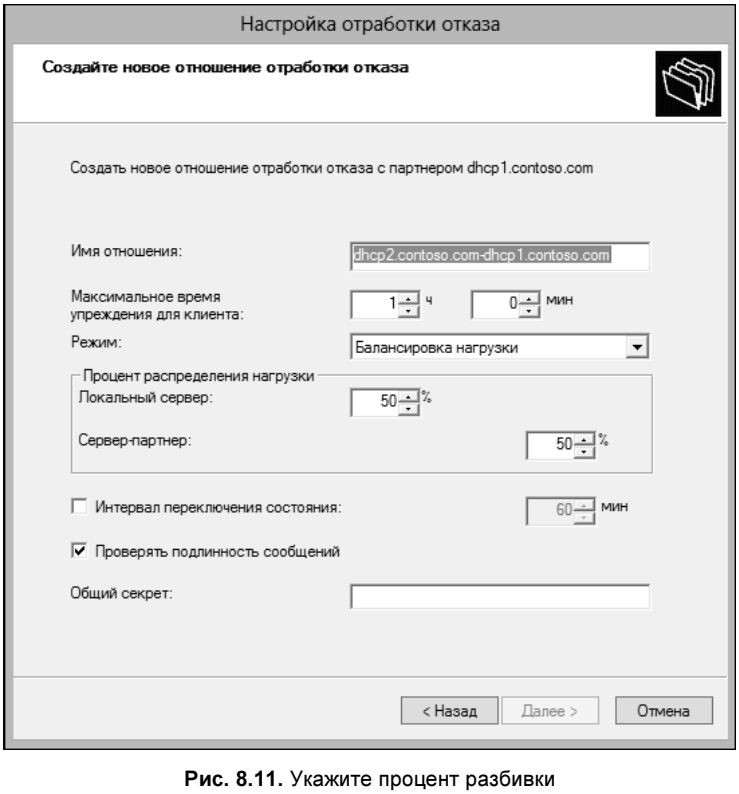


Рис. 8.11. Укажите процент разбивки

- 60/40 — лучше, когда один из серверов обрабатывает немного больше нагрузки, но нужно, чтобы у обоих серверов была постоянная загрузка;
- 50/50 — когда нужно одинаково распределить нагрузку между двумя серверами.

6. Если выбран режим **Горячая замена**, установите роль партнера — **Активный** (Active) или **Резервный** (Standby), а также укажите, сколько процентов адресов нужно зарезервировать. По умолчанию для сервера горячей замены резервируется 5% из диапазона адресов.
7. Заполните поле **Общий секрет** (Shared secret) для партнеров. Это специальный пароль, который партнеры используют при синхронизации DHCP-базы данных и осуществления других задач по обслуживанию отношений отработки отказа. Когда будете готовы продолжить, нажмите кнопку **Далее**.
8. Нажмите кнопку **Готово**. Просмотрите конфигурацию отказоустойчивой области. Если будут обнаружены какие-то ошибки, нужно внести соответствующие изменения. Нажмите кнопку **Закрыть**.

Модификация или удаление отказоустойчивых областей

Отказоустойчивые области не идентифицируются как таковые в консоли DHCP. Можно идентифицировать отказоустойчивую область по ее идентификатору сети и пулу IP-адресов. Как правило, найти отказоустойчивую область очень просто: такая область будет на двух DHCP-серверах, а свойства области будут содержать информацию об обеспечении отказоустойчивости. Чтобы просмотреть эту информацию, щелкните правой кнопкой мыши на области и выберите команду **Свойства**. В диалоговом окне **Свойства** перейдите на вкладку **Отработка отказа** (Failover).

Можно управлять отношения отработки отказа несколькими способами.

- Если есть подозрения, что конфигурация, относящаяся к отношениям отработки, отказала, рассинхронизировалась, щелкните правой кнопкой мыши на области и выберите команду **Репликация отношения** (Replicate Partnership).
- Если есть подозрения, что база данных DHCP, которую совместно используют партнерские серверы, рассинхронизировалась, щелкните правой кнопкой мыши на области и выберите команду **Репликация области** (Replicate Scope).
- Если больше не нужно использовать отказоустойчивую область, щелкните правой кнопкой мыши по ней и выберите команду **Удаление конфигурации отработки отказа** (Deconfigure Failover).

Нельзя изменить параметры отношений отработки отказа. Однако можно сначала деконфигурировать отказоустойчивую область, а затем настроить ее заново.

Управление пулом адресов, арендами и резервированием

У областей есть отдельные папки для пула адресов, арендованных адресов и резервирования. В этих папках можно просмотреть текущую статистику для соответствующих данных и управлять существующими записями.

Просмотр статистики области

Статистика области предоставляет информацию о пуле адресов для текущей области или суперобласти. Чтобы просмотреть статистику, щелкните правой кнопкой мыши по области или суперобласти, а затем выберите команду **Отобразить статистику** (Display Statistics).

Рассмотрим основные столбцы окна **Статистика области** (Scope Statistics):

- **Всего областей** (Total Scopes) — показывает, сколько областей в суперобласти;
- **Всего адресов** (Total Addresses) — сколько IP-адресов в области;
- **Используется** (In Use) — показывает (точное число и процентное соотношение используемых адресов по отношению к общему числу адресов), сколько адресов используется в данный момент. Если это значение достигает 85%, нужно задуматься о добавлении дополнительных адресов или освобождении уже используемых адресов;
- **Доступен** (Available) — общее число доступных адресов.

Включение и настройка фильтрации MAC-адресов

Фильтрация MAC-адресов — функция IPv4-адресов, которая позволяет включать или исключать компьютеры и устройства на основании их MAC-адресов. При настройке фильтрации MAC-адресов можно указать типы оборудования, которые освобождены от фильтрации. По умолчанию все типы оборудования, определенные в RFC 1700, освобождены от фильтрации. Чтобы изменить льготы типа, выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши на узле **IPv4**, а затем выберите команду **Свойства**.
2. На вкладке **Фильтры** (Filters) нажмите кнопку **Дополнительно**. В окне **Дополнительные свойства фильтра** (Advanced Filter Properties) с помощью флажков выберите типы оборудования, которые будут освобождены от фильтрации. Установите флажки типов оборудования, которые нужно фильтровать.
3. Нажмите кнопку **OK** для сохранения изменений.

Перед настройкой фильтрации MAC-адресов нужно сделать следующее.

- Включите и определите список адресов, которым разрешен доступ — *список разрешенных*. Сервер DHCP будет предоставлять доступ только тем DHCP-клиентам, MAC-адреса которых есть в этом списке. Любому клиенту, который ранее получил IP-адрес, будет отказано в возобновлении адреса, если его MAC-адреса нет в списке разрешенных.
- Определите *список запрещенных* узлов. Сервер DHCP отказывает в обслуживании DHCP-клиентам, чьи MAC-адреса есть в списке запрещенных. Любому клиенту, который ранее получил IP-адрес, будет отказано в возобновлении адреса, если MAC-адрес есть в списке запрещенных узлов.
- Список запрещенных имеет приоритет над списком разрешенных. Это означает, что DHCP-сервер предоставляет обслуживание только клиентам, MAC-адреса которых

находятся в списке разрешенных, при условии, что нет никаких соответствий в списке запрещенных. Если MAC-адрес был запрещен, он будет заблокирован, даже если он находится в списке разрешенных.

Чтобы включить список разрешенных и запрещенных (или оба списка), выполните эти действия:

1. В консоли DHCP щелкните по узлу **IPv4**, а затем выберите команду **Свойства**.
2. На странице показана текущая конфигурация фильтра. Чтобы использовать список разрешенных, установите флажок **Включить список разрешенных** (Enable allow list). Чтобы включить список запрещенных, установите флажок **Включить список запрещенных** (Enable deny list).
3. Нажмите кнопку **OK** для сохранения изменений.

> ***Примечание***
>
> В качестве альтернативы можно просто щелкнуть правой кнопкой мыши по узлу **Разрешить** (Allow) или **Запретить** (Deny) в узле **Фильтры** (Filters) и выбрать команду **Включить** (Enable) для включения списка разрешенных или запрещенных. Если нужно отключить какой-то из этих список, щелкните по списку правой кнопкой мыши и выберите команду **Отключить** (Disable).

После включения фильтрации нужно определить фильтры, используя MAC-адреса клиентских компьютеров или сетевых устройств. На клиентском компьютере можно получить его MAC-адрес с помощью команды `ipconfig /all` в командной строке. Запись **Физический адрес** (Physical Address) показывает MAC-адрес клиента. Необходимо точно ввести это значение, чтобы фильтр работал.

MAC-адрес определяется как восемь двухзначных шестнадцатеричных чисел, разделенных дефисом, как показано здесь:

```
FE-01-56-23-18-94-EB-F2
```

При определении фильтра нужно указать MAC-адрес (с дефисами или без них). Это означает, что можно ввести FE-01-56-23-18-94-EB-F2 или FE0156231894EBF2.

Также можно использовать звездочку (*) в качестве маски. Чтобы указать, что любое значение может соответствовать определенной части MAC-адреса, используйте вместо нее *, например:

```
FE-01-56-23-18-94-*-F2
FE-*-56-23-18-94-*-*
FE-01-56-23-18-*-*-*
FE01*
```

Чтобы настроить фильтр MAC-адреса, выполните следующие действия:

1. В консоли DHCP дважды щелкните по узлу **IPv4** и перейдите в раздел **Фильтры** (Filters).
2. Щелкните правой кнопкой мыши по узлу **Разрешить** или **Запретить**, в зависимости от того, какой тип фильтра нужно создать, а затем выберите команду **Новый фильтр** (New Filter).

3. Введите MAC-адрес в фильтр, а затем прокомментируйте его в поле **Описание** (при особом желании). Нажмите кнопку **Добавить**. Повторите шаг для других фильтров.
4. Нажмите кнопку **Закрыть**, когда закончите.

Установка нового диапазона исключений

Можно исключить IPv4- или IPv6-адреса из области, определив диапазон исключений. В областях может быть несколько диапазонов исключений.

Для определения исключений в области IPv4-адресов выполните следующие действия:

1. В консоли DHCP разверните нужную область, щелкните правой кнопкой мыши на узле **Пул адресов** (Address Pool) и выберите команду **Диапазон исключения** (New Exclusion Range).
2. Введите начальный и конечный адреса в поля **Начальный IP-адрес** и **Конечный IP-адрес** и нажмите кнопку **Добавить**. Указанный диапазон должен быть подмножеством диапазона текущей области и в данный момент не должен использоваться. Повторите этот шаг для добавления других диапазонов исключений.
3. Завершив настройку, нажмите кнопку **Закрыть**.

> ***Совет***
>
> Чтобы исключить один IP-адрес, укажите его в поле **Начальный IP-адрес**, а поле **Конечный IP-адрес** не заполняйте.

Чтобы определить диапазон исключений в области IPv6-адресов, выполните следующие действия:

1. В консоли DHCP разверните нужную область, щелкните правой кнопкой мыши на папке **Исключения** (Exclusions), а затем выберите команду **Диапазон исключения** (New Exclusion Range).
2. Введите начальный и конечный адреса в поля **Начальный IPv6-адрес** и **Конечный IPv6-адрес** и нажмите кнопку **Добавить**. Указанный диапазон должен быть подмножеством диапазона текущей области и в данный момент не должен использоваться. Повторите этот шаг для добавления других диапазонов исключений.
3. Завершив настройку, нажмите кнопку **Закрыть**.

Если исключение больше не нужно, его можно удалить. Выберите папку **Пул адресов (IPv4)** или **Исключения (IPv6)**, щелкните правой кнопкой мыши на исключении и выберите команду **Удалить**. В окне подтверждения нажмите кнопку **Да**.

Резервирование DHCP-адресов

Протокол DHCP позволяет назначать постоянные адреса клиентам несколькими способами. Первый способ заключается в использовании переключателя **Без ограничений** (Unlimited), в диалоговом окне свойств области можно назначить постоянный адрес всем клиентам, использующим данную область. Второй способ заключается в резервировании DHCP-адреса для конкретного клиента. В результате резервирования сервер DHCP всегда назначает клиенту один и тот же IP-адрес, сохраняя возможность централизованного управления, в чем и состоит преимущество DHCP.

Если клиент в сети и ему уже выделен IPv4/IPv6-адрес, создать резервирование можно так:

1. В консоли DHCP разверните область, с которой нужно работать, и выберите папку **Арендованные адреса** (Address Leases).
2. Щелкните правой кнопкой на аренде, с которой нужно работать, а из контекстного меню выберите команду **Добавить к резервации** (Add To Reservation).

Чтобы зарезервировать IP-адрес для клиента, выполните следующие действия:

1. В консоли DHCP разверните область, с которой нужно работать, а затем щелкните правой кнопкой мыши на папке **Резервирование** (Reservations) и в контекстном меню выберите команду **Создать резервирование** (New Reservation).
2. В поле **Имя клиента** (Reservation name) введите короткое, но описательное имя клиента. Данное поле используется только для идентификации.
3. В поле **IP-адрес** (IP address) введите IPv4-адрес, который нужно зарезервировать для клиента.

> ***Примечание***
> Этот IP-адрес должен принадлежать допустимому диапазону выбранной области.

4. Поле **MAC-адрес** (MAC address) содержит аппаратный адрес сетевого адаптера клиентского компьютера. Чтобы получить MAC-адрес, введите команду `ipconfig /all` в командной строке клиентского компьютера. В пункте **Физический адрес** содержится MAC-адрес клиента. Нужно ввести это значение без ошибок, иначе резервирование не будет работать.
5. Введите необязательный комментарий в поле **Описание** (Description).
6. По умолчанию поддерживаются и DHCP-клиенты, и BOOTP-клиенты. Это очень удобно, и отказываться от этой возможности следует, только если нужно исключить определенный тип клиента.
7. Нажмите кнопку **Добавить** для создания резервирования. Повторите этот шаг для добавления других резервирований.
8. Нажмите кнопку **Закрыть**.

Чтобы вручную зарезервировать IPv6-адрес для клиента, выполните следующие действия:

1. В консоли DHCP разверните нужную область и щелкните правой кнопкой мыши на папке **Резервирование**. В появившемся меню выберите команду **Создать резервирование**.
2. В поле **Имя клиента** введите короткое и понятное имя. Данное поле используется только для идентификации.
3. В поле **IPv6-адрес** (IPv6 address) введите IPv6-адрес, который хотите закрепить за клиентом.

> ***Примечание***
> Этот IP-адрес должен принадлежать допустимому диапазону выбранной области.

4. В поле уникального идентификатора устройства DUID (Device Unique Identifier) нужно ввести MAC-адрес сетевого адаптера клиентского компьютера. Чтобы узнать MAC-адрес, введите команду `ipconfig /all` в командной строке клиентского компьютера. В пункте **Физический адрес** хранится MAC-адрес клиента. Необходимо ввести это значение без ошибок, иначе резервирование не будет работать.
5. Идентификатор IAID (Identity Association Identifier) устанавливает уникальный префикс идентификатора клиента. Как правило, это значение состоит из 9 цифр.
6. При желании в поле **Описание** введите комментарий.
7. Нажмите кнопку **Добавить**, чтобы создать резервирование. Повторите этот процесс, чтобы добавить другие резервирования.
8. Когда закончите, нажмите кнопку **Закрыть**.

Освобождение адресов и аренды

При работе с зарезервированными адресами помните о двух нюансах.

- Зарезервированные адреса не переназначаются автоматически. Чтобы передать используемый адрес другому клиенту, адрес придется освободить. Для освобождения адреса аннулируйте аренду или введите на клиентском компьютере команду `ipconfig /release`.
- Клиенты не переходят на зарезервированные адреса автоматически. Если клиент уже использует некий IP-адрес, нужно заставить его освободить текущую аренду и запросить новую. Чтобы освободить адрес, аннулируйте аренду или введите на клиентском компьютере команду `ipconfig /renew`.

Изменение свойств резервирования

Изменить свойства резервирования можно с помощью следующих действий:

1. В консоли DHCP разверните область, с которой нужно работать, а затем перейдите в папку **Резервирование** (Reservations).
2. Щелкните правой кнопкой мыши на резервировании и выберите команду **Свойства**. После этого можно изменить параметры резервирования. Нельзя изменять неактивные параметры, зато можно изменить все остальные параметры. Эти параметры такие же, как были описаны в предыдущем разделе.

Удаление аренды и резервирования

Удалить активные аренды и резервирования можно так:

1. В консоли DHCP разверните область, с которой нужно работать, а затем перейдите в папку **Арендованные адреса** (Address Leases) или **Резервирование**.
2. Щелкните правой кнопкой мыши на аренде или резервировании и выберите команду **Удалить**.
3. Нажмите кнопку **Да** для подтверждения своих намерений.

4. После этого аренда или резервирование будут удалены из DHCP. Однако клиент после этого еще не освободит IP-адрес. Чтобы клиент освободил полученный IP-адрес, зарегистрируйтесь в его системе и введите команду `ipconfig /release` в командной строке.

Резервное копирование и восстановление базы данных DHCP

Серверы DHCP хранят DHCP-аренды и информацию резервирования в файлах базы данных. По умолчанию эти файлы находятся в каталоге *%SystemRoot%*\System32\DHCP. Основные файлы, находящиеся в этом каталоге:

- Dhcp.mdb — основной файл базы данных DHCP-сервера;
- J50.log — журнал транзакции, используемый для восстановления незавершенных транзакций в случае сбоя сервера;
- J50.chk — файл контрольной точки, используемый при усечении журнала регистрации транзакций DHCP-сервера;
- J500000NN.log — журналы резервирования для DHCP-сервера;
- Tmp.edb — временный рабочий файл DHCP-сервера.

Резервное копирование базы данных DHCP

Папка *%SystemRoot%*\System32\DHCP\Backup содержит резервные копии конфигурации и базы данных DHCP. По умолчанию база данных DHCP архивируется каждые 60 минут автоматически. Чтобы вручную сделать резервную копию базы данных DHCP, выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши на сервере, который нужно заархивировать, и выберите команду **Архивировать** (Backup).
2. В окне **Обзор папок** (Browse for folder) выберите папку, в которую нужно поместить резервную копию DHCP, а затем нажмите кнопку **OK**.

Параметры реестра, управляющие расположением архива, расписанием архивации, а также другими параметрами архивации DHCP, хранятся в разделе:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters`

Следующие параметры управляют базой данных DHCP и параметрами архивации:

- `BackupDatabasePath` — расположение базы данных DHCP. Этот параметр задается в окне свойств сервера DHCP. Перейдите на вкладку **Дополнительно** и установите нужное значение в поле **Путь к базе данных** (Database path);
- `DatabaseName` — имя основного файла базы данных DHCP. Значение по умолчанию — DHCP.mdb;
- `BackupInterval` — интервал архивации в минутах. Значение по умолчанию — 60 минут;
- `DatabaseCleanupInterval` — интервал очистки записей в базе данных. Значение по умолчанию — 4 часа.

Восстановление базы данных DHCP из резервной копии

В случае отказа сервера нужно восстановить и затем согласовать базу данных DHCP. Для восстановления базы данных DHCP из резервной копии выполните следующие действия:

1. Если нужно, восстановите из архива копию папки *%SystemRoot%*\System32\DHCP\backup. Откройте консоль DHCP, щелкните правой кнопкой мыши на сервере, который нужно восстановить, и выберите команду **Восстановить** (Restore).
2. В окне **Обзор папок** выберите папку, содержащую резервную копию, которую нужно восстановить, а затем нажмите кнопку **OK**.
3. Во время восстановления базы данных служба **DHCP-сервер** будет остановлена. В результате DHCP-клиенты временно не смогут получать IP-адреса.

Архивация и восстановление для перемещения базы данных DHCP на новый сервер

Если нужно перестроить сервер, предоставляющий службы DHCP, следует переместить DHCP-службы на другой сервер. Чтобы сделать это, нужно выполнить несколько действий на исходном и конечном серверах. На конечном сервере выполните следующее:

1. Установите службу **DHCP-сервер** на конечном сервере и перезагрузите сервер.
2. Остановите службу **DHCP-сервер** в консоли **Службы**.
3. Удалите содержимое папки *%SystemRoot%*\System32\DHCP.

На исходном сервере выполните следующие действия:

1. Остановите службу **DHCP-сервер** в консоли **Службы**.
2. После того как служба **DHCP-сервер** будет остановлена, отключите службу так, чтобы она больше не могла быть запущена.
3. Скопируйте содержимое папки *%SystemRoot%*\System32\DHCP исходного сервера в папку *%SystemRoot%*\System32\DHCP конечного сервера.

Теперь все необходимые папки находятся на конечном сервере. Запустите службу **DHCP-сервер** на конечном сервере, чтобы завершить перенос.

Принудительное регенерирование базы данных DHCP

Если база данных DHCP повреждена и Windows не в состоянии ее "починить" при перезапуске службы **DHCP-сервер**, можно попытаться восстановить ее, как описано в *разд. "Восстановление базы данных DHCP из резервной копии" ранее в этой главе*. Если это не сработало, можно запуститься с новой копией базы данных DHCP так:

1. Остановите службу **DHCP-сервер** в консоли **Службы**.
2. Удалите содержимое папки *%SystemRoot%*\System32\DHCP, если нужно принудительно завершить регенерирование базы данных и запретить серверу восстановление из предыдущего архива. Также нужно удалить содержимое папки Backup.

Осторожно!

Не удаляйте DHCP-файлы, если ключи реестра DHCPServer повреждены. Эти ключи должны быть доступны для восстановления базы данных DHCP.

3. Перезапустите службу **DHCP-сервер**.
4. В консоли DHCP не будут отображены аренды или другая информация для областей. Чтобы вернуть активные аренды для каждой области, нужно согласовать области сервера, как будет показано в следующем разделе.
5. Чтобы предотвратить конфликты с ранее присвоенными арендами, нужно включить обнаружение конфликта адреса в течение следующих нескольких дней, как было показано ранее в этой главе.

Согласование аренд и резервирования

Согласование проверяет аренды клиентов и резервирования. Если будут найдены несогласованности между тем, что зарегистрировано в реестре Windows, и тем, что записано в базу данных DHCP-сервера, можно выбрать и согласовать любые противоречивые записи. Как только записи будут согласованы, DHCP восстановит IP-адрес для первоначального владельца или создаст временное резервирование для IP-адреса. Когда время аренды истечет, адрес будет восстановлен для будущего использования.

Можно согласовать области отдельно или же согласовать сразу все области на сервере. Для согласования отдельной области выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши по области, с которой нужно работать, а затем выберите команду **Согласование** (Reconcile).
2. В окне **Согласование** (Reconcile) нажмите кнопку **Проверить** (Verify).
3. Если будут найдены противоречия, об этом сообщат. Выберите выведенные на экран адреса и нажмите кнопку **Согласовать** (Reconcile), чтобы избавиться от противоречий.
4. Если противоречий не будет, нажмите кнопку **OK**.

Чтобы согласовать все области на сервере, выполните следующие действия:

1. В консоли DHCP разверните запись сервера, затем щелкните правой кнопкой мыши на узле **IPv4**, выберите команду **Согласовать все области** (Reconcile All Scopes).
2. В окне **Согласование всех областей** (Reconcile All Scopes) нажмите кнопку **Проверить**.
3. Если будут найдены противоречия, об этом сообщат. Выберите выведенные на экран адреса и нажмите кнопку **Согласовать**, чтобы избавиться от противоречий.
4. Если противоречий не будет, нажмите кнопку **OK**.

ГЛАВА 9

Оптимизация DNS

В этой главе рассмотрены методы установки и управления системой доменных имен (DNS) в сети. DNS (Domain Name System) — это служба разрешения имен, преобразующая имена компьютеров в IP-адреса, позволяющие компьютерам находить друг друга. При использовании DNS полное имя узла, например omega.microsoft.com, может быть разрешено в IP-адрес, позволяющий компьютерам находить друг друга. Система DNS работает через стек протоколов TCP/IP и может интегрироваться с WINS, DHCP и Active Directory. Полная интеграция DNS с сетевыми возможностями Microsoft Windows позволяет оптимизировать работу DNS в доменах Microsoft Windows Server.

Общие сведения о DNS

Система DNS объединяет группы компьютеров в домены. Домены организованы в иерархическую структуру, которая для публичных сетей определяется в Интернете, а для частных (также известных как *интрасети* или *экстрасети*) — на уровне предприятия. Различные уровни иерархии соответствуют отдельным компьютерам, доменам организаций и доменам верхнего уровня. В полностью определенном имени хоста **omega.microsoft.com**: **omega** — имя отдельного компьютера, **microsoft** — домен организации, **com** — домен верхнего уровня.

Домены верхнего уровня (Top Level Domains, TLD) лежат в основе иерархии DNS, поэтому их часто называют *корневыми*. Эти домены упорядочены географически, по типу организации и по назначению. Обычные домены, например **microsoft.com**, также называются *родительскими доменами*, поскольку являются родителями для групп или подразделений в организации. Можно разделить родительские домены на поддомены, предназначенные для групп или отделов внутри организации.

Поддомены часто называют *дочерними доменами*. Например, полное доменное имя (Fully Qualified Domain Name, FQDN) для компьютера из отдела кадров может называться **jacob.hr.microsoft.com**. Здесь **jacob** — имя узла, **hr** — дочерний домен, а **microsoft.com** — родительский домен.

Интеграция Active Directory и DNS

Домены Active Directory используют DNS для реализации своей структуры имен и иерархии. Служба каталогов Active Directory и DNS настолько тесно взаимосвязаны, что перед установкой доменных служб Active Directory (AD DS) необходимо установить DNS в сети.

Во время установки первого контроллера домена в сети есть возможность автоматически установить DNS, если DNS-сервер не найден. Также можно указать, должны ли DNS и Active Directory полностью интегрироваться. В большинстве случаев на оба вопроса следует дать утвердительный ответ. При полной интеграции информация DNS хранится в Active Directory, что позволяет воспользоваться всеми преимуществами Active Directory.

Очень важно понимать различия между частичной и полной интеграцией.

- **Частичная интеграция.** При частичной интеграции для хранения информации DNS используется стандартное хранилище. Информация DNS хранится в текстовых файлах с расширением dns в заданной по умолчанию папке *%SystemRoot%*\System32\Dns. Обновления DNS проводятся через единственный полномочный DNS-сервер. Этот сервер задан как основной DNS-сервер конкретного домена или области внутри домена, которая называется *зоной* (zone). Клиенты, использующие динамическое обновление DNS через DHCP, должны быть настроены на работу с основным DNS-сервером зоны. В противном случае DNS-информация на них обновляться не будет. Если в сети отсутствует основной DNS-сервер, проводить динамические обновления через DHCP нельзя.
- **Полная интеграция.** При полной интеграции информация DNS хранится в Active Directory, в контейнере dnsZone. Поскольку DNS-информация — это часть Active Directory, любой контроллер домена может получить доступ к данным, и динамические обновления через DHCP можно проводить по модели с несколькими хозяевами. А это позволяет любому контроллеру домена, на котором запущена служба **DNS-сервер**, обрабатывать динамические обновления. Клиенты, использующие динамические обновления DNS через DHCP, могут работать с любым DNS-сервером внутри зоны. Еще одно преимущество интеграции с каталогом заключается в возможности управлять доступом к DNS-информации при помощи системы безопасности каталога.

Если внимательно посмотреть на способ репликации информации DNS по сети, найдутся и другие преимущества полной интеграции с Active Directory. При частичной интеграции информация DNS хранится и реплицируется отдельно от Active Directory. Если есть две отдельные структуры, снижается эффективность как DNS, так и Active Directory, а также усложняется репликация. С точки зрения репликации изменений система DNS менее эффективна, чем Active Directory, поэтому репликация изменений DNS займет больше времени и ресурсов.

В предыдущих версиях DNS-сервера для Windows Server перезапуск DNS-сервера в больших организациях с большим числом зон, интегрированных в AD DS, мог длиться часами. Это происходило потому, что данные зон загружались не в фоновом

режиме одновременно с запуском службы DNS. В целях повышения эффективности DNS-серверов в Windows Server 2008 R2 и более поздних версиях они существенно доработаны. Теперь перезагрузки данных зон из AD DS осуществляются в фоновом режиме. Это гарантирует способность DNS-сервера отвечать на запросы, в том числе и из других зон.

При запуске DNS-сервер под управлением Windows Server 2008 R2 и более поздних версий выполняет следующие задачи:

- перечисляет все загружаемые зоны;
- загружает корневые ссылки из файлов или хранилища AD DS;
- загружает все зоны, хранящиеся в файлах, а не в AD DS;
- начинает отвечать на запросы и вызовы RPC (Remote Procedure Call);
- создает один или несколько потоков для загрузки зон, которые хранятся в AD DS.

Поскольку отдельные потоки загружают данные зоны, DNS-сервер способен во время загрузки зон отвечать на запросы. Если DNS-клиент посылает запрос относительно узла в уже загруженной зоне, DNS-сервер отвечает ему. Если это запрос относительно компьютера, который еще не загружен в память, сервер считывает данные узла из AD DS и соответствующим образом обновляет список записей.

Включение DNS в сети

Для включения DNS в сети нужно настроить DNS-клиенты и серверы. При настройке DNS-клиентов на них указываются IP-адреса DNS-серверов сети. Используя эти адреса, клиенты могут взаимодействовать с DNS-серверами по всей сети, даже если серверы находятся в разных подсетях.

> ***Примечание***
>
> Настройка DNS-клиентов описана в *главе 7*, а настройка DNS-сервера объясняется в следующем разделе этой главы.

Клиент DNS, встроенный в Windows 7 и Windows Server 2008 R2 и более поздние версии, поддерживает DNS-трафик по протоколам IPv4 и IPv6. По умолчанию при использовании протокола IPv6 серверам DNS назначаются хорошо известные локальные адреса[1]. Чтобы добавить IPv6-адреса DNS-серверов, используйте окно свойств протокола TCP/IPv6 или следующую команду:

```
netsh interface IPV6 ADD DNSSERVERS
```

В Windows PowerShell вы также можете использовать команду `Get-NetIPInterface` для вывода доступных интерфейсов, а также команду `Set-DNSClientServerAddress` для установки IPv6-адреса на определенном интерфейсе.

Серверы DNS, работающие под управлением Windows Server 2008 R2 или более поздних версий, в равной мере поддерживают протоколы IPv4 и IPv6. В консоли **Диспетчер DNS** (DNS Manager) адреса хостов отображаются как IPv4- или IPv6-адреса, соот-

[1] FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2 и FEC0:0:0:FFFF::3. — *Прим. пер.*

ветственно. Утилита командной строки Dnscmd также поддерживает оба формата. Теперь DNS-серверы способны посылать рекурсивные запросы на серверы с поддержкой только протокола IPv6, тогда как список пересылки сервера может содержать и IPv4-, и IPv6-адреса. И наконец, DNS-серверы поддерживают доменное пространство имен для обратного просмотра.

Если сеть использует DHCP, его нужно настроить для работы с DNS. DCHP-клиенты могут регистрировать IPv6-адреса как вместе с IPv4-адресами, так и вместо них. Чтобы обеспечить надлежащую интеграцию DHCP и DNS, задайте параметры области DHCP, как было описано в *главе 8*. Для IPv4 нужно установить параметры области **006 DNS-серверы** (006 DNS Servers) и **015 DNS-имя домена** (015 DNS Domain Name). Для IPv6 следует установить параметры области **00023 Список адресов IPv6 рекурсивных серверов имен DNS** (00023 DNS Recursive Name Server IPV6 Address) и **00024 Список поиска доменов** (00024 Domain Search List). Также, если нужно организовать доступ к компьютерам сети из других доменов Active Directory, создайте для них записи в DNS. DNS-записи упорядочены по зонам — областям внутри домена.

DNS-клиенты под управлением Windows 7 (или более поздних версий), так же как и Windows Server 2008 R2, могут использовать протокол LLMNR (Link-Local Multicast Name Resolution) для разрешения имен в сегменте локальной сети, когда DNS-сервер недоступен. Они также периодически производят поиск контроллера домена в домене, к которому они принадлежат. Такое поведение позволяет избежать проблем производительности, которые могут произойти, если отказ сети или сервера заставляет DNS-клиента связываться с удаленным контроллером домена, доступным по медленному соединению, а не с локальным контроллером домена. Ранее клиент использовал этот контроллер домена до тех пор, пока он не был вынужден искать новый контроллер, например, когда клиентский компьютер был долгое время отключен от сети. Периодически обновляя его связь с контроллером домена, DNS-клиент может уменьшить вероятность того, что он будет связан с несоответствующим контроллером домена.

У службы **DNS-клиент** (DNS client) для Windows 8 и более поздних версий есть несколько расширений безопасности относительно LLMNR и NetBIOS. Чтобы повысить безопасность для мобильных сетей, служба:

- не отправляет исходящие LLMNR-запросы по мобильной широкополосной (3G, EDGE) сети или по VPN-интерфейсам;
- не отправляет исходящие NetBIOS-запросы по мобильной широкополосной (3G, EDGE) сети.

Для лучшей совместимости с устройствами в энергосберегающем режиме тайм-аут LLMNR-запроса увеличен до 410 мс для первой попытки и 410 мс для второй попытки, что в сумме равно 820 мс вместо 300 мс. Чтобы улучшить время ответа для всех запросов, служба **DNS-клиент** делает следующее:

- параллельно отправляет LLNMR- и NetBIOS-запросы, оптимизируя их для IPv4 и IPv6;
- делит интерфейсы на сети для отправки параллельных DNS-запросов;
- использует асинхронный DNS-кэш с оптимизированным временем ответа.

Примечание

Можно настроить DNS-клиент на компьютере под управлением Windows 7 или более поздней версии (или Windows Server 2008 R2 или более поздней версии) для нахождения ближайшего контроллера домена вместо случайного поиска. В результате повысится производительность в сетях, содержащих домены, которые существуют по медленным соединениям. Однако поскольку этот процесс генерирует сетевой трафик, поиск ближайшего контроллера домена может отрицательно влиять на производительность сети.

В Windows Server 2008 и более поздних версиях поддерживаются основные зоны только для чтения и зона GlobalNames. Основная зона только для чтения автоматически создается для поддержки контроллера домена RODC. Когда компьютер становится RODC-контроллером, он реплицирует с доступом только для чтения полную копию всех разделов каталога приложений, используемых DNS, включая раздел домена, а также зоны DNS-леса (ForestDNSZones) и домена (DomainDNSZones). Это гарантирует наличие на DNS-сервере RODC полной копии всех зон DNS. Администратор RODC может просматривать содержимое основной зоны, но не может изменять его. Администратор может редактировать содержимое зоны только на стандартном контроллере домена.

Для поддержки всех сред DNS и разрешения однокомпонентных имен создается зона GlobalNames. Для оптимальной производительности и поддержки в различных лесах интегрируйте эту зону с AD DS и настройте каждый полномочный DNS-сервер при помощи локальной копии. Если публикуется расположение зоны GlobalNames посредством записи ресурса **Расположение службы** (Service Location, SRV), зона предоставляет уникальные однокомпонентные имена по всему лесу. В отличие от WINS, зона GlobalNames предназначена для разрешения однокомпонентных имен для подмножества имен хостов, обычно записей ресурса CNAME для корпоративных серверов. Зона GlobalNames не предназначена для разрешения одноранговых имен, например разрешения имен рабочих станций. Для этого существует LLMNR.

Если зона GlobalNames настроена правильно, разрешение однокомпонентных имен работает следующим образом:

1. К однокомпонентному имени, которое запрашивает клиент, добавляется основной DNS-суффикс клиента. Затем запрос передается DNS-серверу.
2. Если полное имя компьютера не получается разрешить, клиент запрашивает разрешение при помощи списков поиска DNS-суффикса, если они имеются.
3. Если ни один из вариантов имени не удается разрешить, клиент запрашивает разрешение посредством однокомпонентного имени.
4. Если однокомпонентное имя имеется в зоне GlobalNames, имя разрешает DNS-сервер, на котором размещена зона. В противном случае, запрос передастся в WINS.

Зона GlobalNames обеспечивает разрешение однокомпонентных имен только при условии, что все уполномоченные DNS-серверы работают под управлением Windows Server 2008 R2 и более поздних версий. Впрочем, иные DNS-серверы, которые не являются уполномоченными ни в одной зоне, могут работать под управлением других операционных систем (например, под управлением UNIX). Динамические обновления в зоне GlobalNames не поддерживаются.

Настройка разрешения имен на DNS-клиентах

Лучший способ настроить разрешение имен на DNS-клиентах зависит от конфигурации сети. Если компьютеры используют DHCP, возможно, лучше настроить DNS через параметры на DHCP-сервере. Если компьютеры используют статические IP-адреса или необходимо указать отдельные параметры DNS на отдельных системах, нужно настроить DNS вручную.

Настроить параметры DNS можно на вкладке **DNS** окна **Дополнительные параметры TCP/IP** (Advanced TCP/IP Settings). Чтобы открыть это окно, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
2. В окне **Сетевые подключения** щелкните правой кнопкой мыши по нужному подключению и выберите команду **Свойства**.
3. Дважды щелкните по протоколу, который хотите настроить, — **TCP/IPv6** или **TCP/IPv4**.
4. Если используете DHCP и нужно, чтобы адрес DNS-сервера был задан по DHCP, установите переключатель **Получить адрес DNS-сервера автоматически** (Obtain DNS Server Address Automatically). В противном случае установите переключатель **Использовать следующие адреса DNS-серверов** (Use The Following DNS Server Addresses), а затем введите адреса основного и дополнительного DNS-серверов в соответствующих полях.
5. Нажмите кнопку **Дополнительно**, чтобы открыть диалоговое окно **Дополнительные параметры TCP/IP**. Перейдите на вкладку **DNS** и настройте необходимые параметры.

   - **Адреса DNS-серверов, в порядке использования** (DNS server addresses, in order of use) — укажите IP-адрес каждого DNS-сервера, который используется для разрешения доменных имен. Чтобы добавить IP-адрес сервера в список, нажмите кнопку **Добавить**. Нажмите кнопку **Удалить**, чтобы удалить адрес выделенного сервера из списка. Чтобы изменить выделенную запись, нажмите кнопку **Изменить**. Если указано несколько серверов DNS, их приоритет определяется очередностью в списке. Если первый сервер не может ответить на запрос о разрешении имени хоста, запрос посылается на следующий DNS-сервер, и т. д. Чтобы изменить позицию сервера в списке, выделите его и воспользуйтесь кнопками со стрелками вверх и вниз.
   - **Дописывать основной DNS-суффикс и суффикс подключения** (Append primary and connection specific DNS suffixes) — обычно по умолчанию этот переключатель установлен. Включите этот параметр для разрешения неполных имен компьютеров в основном домене. Допустим, происходит обращение к компьютеру Glandolf в родительском домене **microsoft.com**. Для разрешения имя компьютера будет автоматически дополнено суффиксом DNS — **glandolf.microsoft.com**. Если в основном домене компьютера с таким именем нет, запрос не выполняет-

ся. Основной домен задается на вкладке **Имя компьютера** (Computer Name) диалогового окна **Свойства системы** (System Properties).

- **Добавлять родительские суффиксы основного DNS-суффикса** (Append parent suffixes of the primary DNS suffix) — по умолчанию этот переключатель установлен. Включите его для разрешения неполных имен компьютеров в иерархии родительских/дочерних доменов. В случае неудачного запроса в ближайшем родительском домене, для попытки разрешения запроса используется суффикс родительского домена более высокого уровня. Этот процесс продолжается, пока не будет достигнута вершина иерархии доменов DNS. Допустим, в запросе указано имя компьютера Glandolf в родительском домене **dev.microsoft.com**. Сначала DNS пытается разрешить имя компьютера **glandolf.dev.microsoft.com**, а потом, в случае неудачи, пытается разрешить имя **glandolf.microsoft.com**.
- **Дописывать следующие DNS-суффиксы (по порядку)** (Append these DNS suffixes (in order)) — установите этот переключатель, чтобы задать использование особых DNS-суффиксов вместо имени родительского домена. Нажмите кнопку **Добавить**, чтобы добавить суффикс домена в список. Нажмите кнопку **Удалить**, чтобы удалить выделенный суффикс домена из списка. Для редактирования выделенной записи нажмите кнопку **Изменить**. Разрешается указать несколько суффиксов домена. Если первый суффикс не позволяет разрешить имя, DNS применяет следующий суффикс из списка. Если первый суффикс не был разрешен, берется следующий суффикс, и т. д. Чтобы изменить очередность суффиксов домена, выберите нужный суффикс и измените его положение кнопками со стрелками вверх и вниз.
- **DNS-суффикс подключения** (DNS suffix for this connection) — в этом поле задается DNS-суффикс подключения, переопределяющий DNS-имена, уже настроенные на использование с данным подключением. Обычно имя домена DNS указывается на вкладке **Имя компьютера** диалогового окна **Свойства системы**.
- **Зарегистрировать адреса этого подключения в DNS** (Register this connection's addresses in DNS) — включите этот параметр, если нужно зарегистрировать все IP-адреса для этого соединения в DNS с FQDN-именами компьютеров. Этот параметр включен по умолчанию.

Примечание

Динамические обновления DNS используются в сочетании с DHCP, чтобы позволить клиенту обновить его запись A (адрес узла), если его IP-адрес изменяется и позволяет DHCP-серверу обновить запись PTR (указатель) для клиента на DNS-сервере. Также можно настроить DHCP-серверы, чтобы они обновляли обе записи (A и PTR) от имени клиента. Динамические обновления поддерживаются DNS-серверами BIND 8.2.1 и более поздними версиями, Windows Server 2000, Windows Server 2003 и более поздними версиями Windows Server.

- **Использовать DNS-суффикс подключения при регистрации в DNS** (Use this connection's DNS suffix in dns registration) — установите этот флажок, если нужно, чтобы все IP-адреса для данного подключения регистрировались в DNS родительского домена.

Установка DNS-серверов

Любую систему Windows Server 2012 R2 можно настроить как DNS-сервер. Доступны четыре типа DNS-серверов.

- *Основной сервер, интегрированный с Active Directory* — DNS-сервер полностью интегрированный с Active Directory. Все данные DNS хранятся непосредственно в Active Directory.
- *Основной сервер* — основной DNS-сервер домена с частичной интеграцией с Active Directory. В этом случае основная копия DNS-записей и конфигурация домена хранятся в текстовых файлах с расширением dns.
- *Вторичный (дополнительный) сервер* — резервный DNS-сервер. Хранит копию DNS-записей, полученную с основного сервера и передачи зон для обновлений. Вторичный сервер при запуске получает всю необходимую информацию с DNS-сервера.
- *Сервер пересылки (forward-сервер)* — сервер, кэширующий DNS-информацию после lookup-запросов и всегда передающий запросы на другие серверы. Сервер пересылки хранит DNS-информацию до обновления, до истечения срока действия или до перезапуска сервера. В отличие от вторичных серверов forward-сервер не запрашивает полную копию файлов базы данных зоны. Это означает, что при запуске сервера пересылки его база данных пуста.

Перед настройкой DNS-сервера требуется установить службу **DNS-сервер**. Затем можно будет настроить сервер для предоставления ним интегрированного, основного, вторичного DNS-сервиса или DNS-сервиса пересылки.

Установка и настройка службы *DNS-сервер*

Все контроллеры домена могут работать как DNS-серверы, и при установке контроллера домена предлагается установить и настроить DNS в ходе установки контроллера домена. Если администратор согласился на установку DNS, то служба **DNS-сервер** будет установлена с автоматически заданной стандартной конфигурацией. Переустановка не требуется.

Если настраивается рядовой сервер и служба **DNS-сервер** еще не установлена, выполните следующие действия:

1. В диспетчере серверов выберите команду меню **Управление | Добавить роли и компоненты** или щелкните по ссылке **Добавить роли и компоненты** на панели приветствия. Будет запущен мастер добавления ролей и компонентов. Если мастер отобразит страницу **Перед началом работы**, прочитайте приветствие и нажмите кнопку **Далее**.
2. На странице **Выбор типа установки** по умолчанию выбран переключатель **Установка ролей или компонентов**. Нажмите кнопку **Далее**.
3. На странице **Выбор целевого сервера** можно указать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите либо сервер

из пула серверов, либо сервер, на котором можно смонтировать виртуальный жесткий диск (VHD). Если роли и компоненты добавляются на VHD, нажмите кнопку **Обзор**, а затем используйте окно **Обзор виртуальных жестких дисков** для выбора VHD. Когда будете готовы продолжить, нажмите кнопку **Далее**.

Примечание

В списке серверов будут только серверы под управлением Windows Server 2012 R2 и добавленные администратором в диспетчере серверов.

4. На странице **Выбор ролей сервера** выберите роль **DNS-сервер**. Если нужно установить дополнительные компоненты, от которых зависит данный компонент, будет отображено соответствующее диалоговое окно. Нажмите кнопку **Добавить компоненты** для закрытия этого окна и установки требуемых компонентов на сервер. Для продолжения нажмите кнопку **Далее** трижды.
5. Если на сервере, на который устанавливается роль **DNS-сервер**, нет необходимых двоичных исходных файлов, сервер получит файлы через службу Windows Update (по умолчанию) или из расположения, указанного в групповой политике.

Примечание

Можно также указать альтернативный источник для исходных файлов. Чтобы сделать это, щелкните по ссылке **Указать альтернативный исходный путь** (Specify An Alternate Source Path), в появившемся окне укажите альтернативный путь и нажмите кнопку **OK**. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer2012\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2012\install.wim:4.

6. Нажмите кнопку **Установить** для начала процесса установки. Страница **Ход установки** позволяет отслеживать процесс инсталляции. Если окно мастера закрыто, нажмите значок **Уведомления** в консоли **Диспетчер серверов**, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.
7. Когда мастер закончит установку роли **DNS-сервер**, страница **Ход установки** сообщит об этом. Просмотрите подробности установки, чтобы убедиться, что все фазы инсталляции завершены успешно.
8. Начиная с этого момента, служба **DNS-сервер** должна запускаться автоматически при каждой перезагрузке сервера. Если она не запустится, нужно запустить ее вручную *(см. разд. "Запуск и остановка DNS-сервера" далее в этой главе)*.
9. После установки DNS-сервера можно использовать консоль **Диспетчер DNS** (DNS Manager) для настройки и управления DNS-сервером. Для вызова консоли **Диспетчер DNS** (рис. 9.1) выберите команду **DNS** из меню **Средства** в диспетчере серверов.
10. Если настраиваемый сервер не отображается в представлении дерева, нужно подключиться к нему. Щелкните правой кнопкой мыши по узлу **DNS** в представлении дерева и выберите команду **Подключение к DNS-серверу** (Connect To DNS Server). Теперь выполните одно из действий:
    - для подключения к локальному компьютеру установите переключатель **этот компьютер** и нажмите кнопку **OK**;

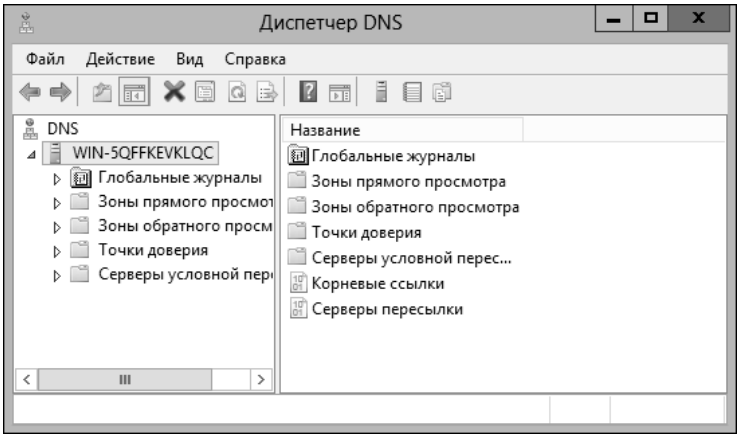


Рис. 9.1. Консоль **Диспетчер DNS** используется для управления DNS-серверами сети

- для подключения к удаленному серверу выберите переключатель **другой компьютер** (The following computer) и введите имя сервера или IP-адрес, а затем нажмите кнопку **OK**.

11. Запись для DNS-сервера должна появиться в представлении дерева консоли **Диспетчер DNS**. Щелкните правой кнопкой мыши на записи сервера и выберите команду **Настроить DNS-сервер** (Configure A DNS Server). Будет запущен мастер настройки DNS-сервера (Configure A DNS Server Wizard). Нажмите кнопку **Далее**.
12. На странице **Выбор действия по настройке** (Select Configuration Action) установите переключатель **Настроить только корневые ссылки** (Configure root hints only), чтобы указать, что только базовые DNS-структуры должны быть созданы в этот раз (рис. 9.2).

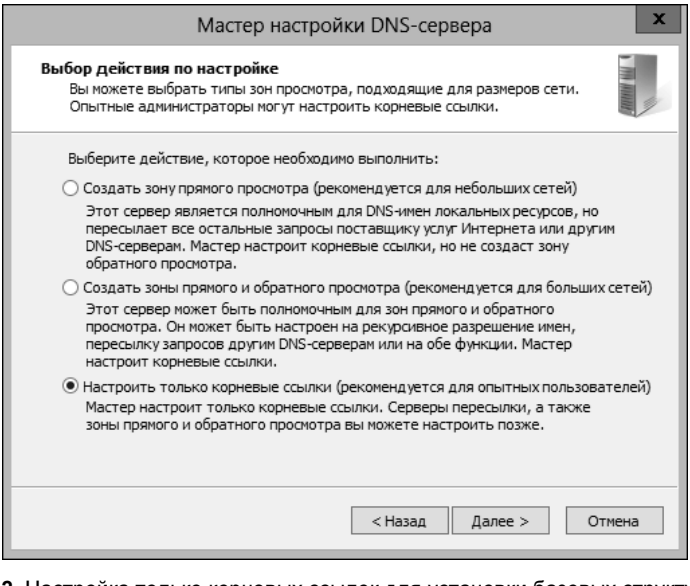


Рис. 9.2. Настройка только корневых ссылок для установки базовых структур DNS

13. Нажмите кнопку **Далее**. Мастер произведет поиск существующих структур DNS и при необходимости модифицирует их.
14. Нажмите кнопку **Готово** для завершения процесса.

> ***Практический совет***
>
> Если мастер не может настроить корневые ссылки, нужно настроить их вручную или скопировать их с другого сервера. Однако стандартный набор корневых ссылок уже включен в DNS-сервер, и они должны быть добавлены автоматически. Чтобы убедиться в этом, щелкните правой кнопкой мыши по записи DNS-сервера и выберите команду **Свойства**. В окне **Свойства** настроенные в данный момент корневые структуры должны быть показаны на вкладке **Корневые ссылки** (Root Hints).

Настройка основного DNS-сервера

У каждого домена есть основной DNS-сервер. Можно интегрировать этот сервер в Active Directory или оставить его работать в качестве основного сервера. Основные серверы обладают зонами прямого и обратного просмотра. Прямой просмотр служит для разрешения доменных имен в IP-адреса. Обратный просмотр нужен для проверки подлинности DNS-запросов посредством разрешения IP-адресов в доменные имена.

После установки службы **DNS-сервер** на сервер можно сконфигурировать основной сервер с помощью следующих действий:

1. Запустите консоль **Диспетчер DNS**. Если необходимый сервер не отображается, подключитесь к нему, как было описано ранее.
2. Запись DNS-сервера должна быть выведена в дереве консоли **Диспетчер DNS**. Щелкните правой кнопкой мыши на записи сервера и выберите команду **Создать новую зону** (New Zone). Будет запущен мастер создания новой зоны (New Zone Wizard). Нажмите кнопку **Далее**.
3. Можно выбрать тип зоны (рис. 9.3). Если основной сервер настраивается с интеграцией в Active Directory (на контроллере домена), выберите переключатель **Основная зона** (Primary zone) и убедитесь, что отмечен флажок **Сохранять зону в Active Directory** (Store the zone in Active Directory). Если интеграция DNS с Active Directory не нужна, выберите переключатель **Основная зона** и сбросьте флажок **Сохранять зону в Active Directory**. Нажмите кнопку **Далее**.
4. Если зона интегрируется с Active Directory, выберите одну из стратегий репликации (в противном случае перейдите к шагу 6).
   - **Для всех DNS-серверов, работающих на контроллерах домена в этом лесу** (To all DNS servers running on domain controllers in this forest) — выберите эту стратегию для самой обширной репликации. Помните, что лес Active Directory содержит также все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - **Для всех DNS-серверов, работающих на контроллерах домена в этом домене** (To all DNS servers running on domain controllers in this domain) — выберите эту стратегию, если нужно реплицировать DNS-информацию в пределах текущего домена.

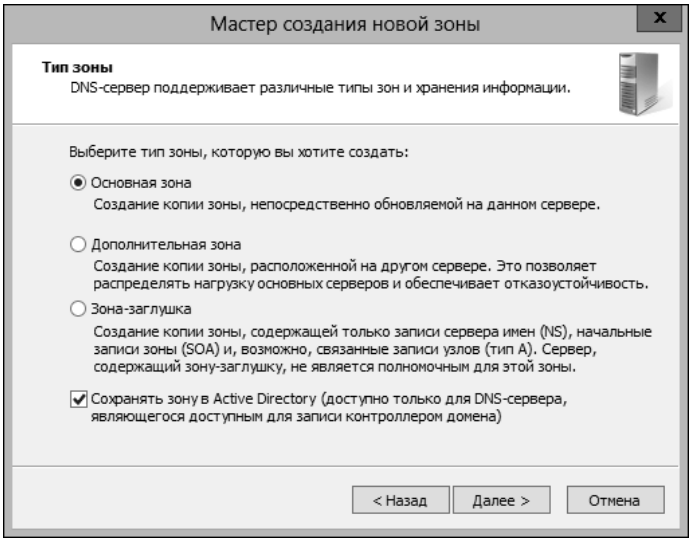


Рис. 9.3. Мастер создания новой зоны: выбор типа зоны

- **Для всех контроллеров домена в этом домене (для совместимости с Windows 2000)** (To all domain controllers in this domain (for Windows 2000 compatibility)) — выберите эту стратегию, если нужно реплицировать DNS-информацию всем контроллерам домена в текущем домене, что необходимо для совместимости с Windows 2000. Хотя эта стратегия обеспечивает более широкую репликацию DNS-информации внутри домена и обеспечивает совместимость с Windows 2000, не каждый контроллер домена является DNS-сервером (и не нужно настраивать каждый контроллер домена как DNS-сервер).

5. Нажмите кнопку **Далее**. Выберите переключатель **Зона прямого просмотра** (Forward Lookup Zone), а затем нажмите кнопку **Далее**.
6. Введите полное DNS-имя зоны. Имя зоны определяет, как сервер или зона вписываются в доменную иерархию DNS. Например, если создается основной сервер для домена **microsoft.com**, в качестве имени зоны следует ввести **microsoft.com**. Нажмите кнопку **Далее**.
7. Если настраивается основная зона, которая не интегрируется с Active Directory, нужно указать имя файла зоны. Имя файла базы данных зоны DNS по умолчанию должно быть уже введено. Оставьте это имя без изменений или введите новое. Нажмите кнопку **Далее**.
8. Укажите, будут ли разрешены динамические обновления.

   - **Разрешить только безопасные динамические обновления** (Allow only secure dynamic updates) — когда зона интегрирована с Active Directory, можно использовать списки управления доступом для ограничения круга клиентов, которые могут осуществлять динамические обновления. Когда включена эта опция, только клиенты с авторизированными учетными записями компьютера и одобренными списками управления доступом могут динамически обновлять свои записи ресурсов в DNS.

- **Разрешить любые динамические обновления** (Allow both nonsecure and secure dynamic updates) — выберите эту опцию, чтобы разрешить любому клиенту обновлять свои записи ресурсов в DNS. Клиенты могут быть безопасными и небезопасными.
- **Запретить динамические обновления** (Do not allow dynamic updates) — отключает динамические обновления DNS. Нужно выбрать эту опцию, только если зона не интегрирована с Active Directory.

9. Нажмите кнопку **Далее**. А затем нажмите кнопку **Готово** для завершения этого процесса. Новая зона будет добавлена на сервер, базовые DNS-записи будут созданы автоматически.
10. Один DNS-сервер может предоставлять сервис для нескольких доменов. Если у вас есть несколько родительских доменов, например **microsoft.com** и **msn.com**, нужно повторить этот процесс для настройки остальных зон просмотра. Также надо настроить зоны обратного просмотра. Следуйте рекомендациям *разд. "Настройка зон обратного просмотра" далее в этой главе*.
11. Еще необходимо создать дополнительные записи для любых компьютеров, к которым надо открыть доступ из других DNS-доменов, выполнив действия, описанные в *разд. "Управление записями DNS" далее в этой главе*.

Практический совет

У большинства организаций есть частная и публичная области сети. Публичная область сети — это, как правило, веб-сервер и внешние почтовые серверы. Публичные области сети предприятия не должны разрешать неограниченный доступ. Вместо этого публичные области должны быть настроены как часть сети периметра. (Сети периметра также известны как DMZ, демилитаризованная зона, и как *экранированные подсети*. Эти области защищены брандмауэром организации, который ограничивает доступ к внешней сети и запрещает доступ к внутренней сети.) В противном случае, публичные области сети должны располагаться в отдельной и защищенной брандмауэром области.

Частные области сети — те области, в которых располагаются внутренние серверы организации и рабочие станции. В публичных областях сети параметры DNS находятся в публичном интернет-пространстве. Здесь можно использовать DNS-имя **.com**, **.org**, **.net** или любое другое, зарегистрированное у интернет-регистратора, и выделенные IP-адреса. В частной области сети DNS-настройки будут в пространстве частной сети. Здесь можно использовать **adatum.com** в качестве DNS-имени организации и частные IP-адреса, как было показано в *главе 7*.

Настройка дополнительного DNS-сервера

Дополнительные серверы обеспечивают отказоустойчивость DNS-службы сети. Если используется полная интеграция с Active Directory, настраивать дополнительные серверы не нужно. Достаточно запустить службу DNS на нескольких контроллерах домена, и Active Directory будет реплицировать информацию DNS на все контроллеры. При использовании частичной интеграции следует настроить дополнительные серверы, чтобы уменьшить нагрузку на основной сервер. В небольшой или средней сети можно использовать в качестве дополнительных серверов DNS-серверы интернет-провайдера. Свяжитесь с провайдером, чтобы он настроил дополнительные DNS-службы. Альтернативно, вы можете поместить ваши публичные DNS-записи на выделенный, внешний DNS-сервис, а частные DNS-записи хранить на своих внутренних серверах DNS.

Поскольку дополнительные серверы используют зоны прямого просмотра для большинства типов запросов, зоны обратного просмотра, скорее всего, не понадобятся. Но зоны обратного просмотра нужны основным серверам, поэтому необходимо настроить их, чтобы обеспечить корректное разрешение доменных имен.

Для установки дополнительных серверов с целью повышения отказоустойчивости и балансировки нагрузки выполните следующие действия:

1. Запустите консоль **Диспетчер DNS**. Если нужного сервера нет в списке, подключитесь к нему, как было описано ранее.
2. Щелкните правой кнопкой мыши на записи сервера, а затем выберите команду **Создать новую зону**. Будет запущен мастер создания новой зоны. Нажмите кнопку **Далее**.
3. На странице **Тип зоны** (Zone Type) выберите переключатель **Дополнительная зона** (Secondary Zone). Нажмите кнопку **Далее**.
4. Дополнительные серверы могут использовать как зоны прямого просмотра, так и зоны обратного просмотра. Сначала нужно создать зону прямого просмотра, поэтому выберите переключатель **Зона прямого просмотра** (Forward Lookup Zone) и нажмите кнопку **Далее**.
5. Введите DNS-имя зоны и нажмите кнопку **Далее**.
6. В списке **Основные серверы** (Master Servers) введите IP-адрес основного сервера зоны и нажмите клавишу <Enter>. Мастер попытается проверить сервер. Если произошла ошибка, убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Если нужно скопировать данные зоны с других серверов на случай недоступности первого сервера, повторите этот шаг.
7. Нажмите кнопку **Далее**, а затем кнопку **Готово**. В большой сети, возможно, придется настроить зоны обратного просмотра на дополнительных серверах. Если это так, воспользуйтесь рекомендациями из следующего раздела.

Настройка зон обратного просмотра

Прямые просмотры используются для разрешения доменных имен в IP-адреса. Обратные просмотры служат для разрешения IP-адресов в доменные имена. Каждый сегмент сети должен иметь зону обратного просмотра. Например, если есть три подсети — 192.168.10.0, 192.168.11.0 и 192.168.12.0, должны быть и три зоны обратного просмотра.

Стандартное имя зоны обратного просмотра составляется из идентификатора сети, выстроенного в обратном порядке, и суффикса in-addr.arpa. Зоны обратного просмотра из предыдущего примера будут называться 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa и 12.168.192.in-addr.arpa. Записи зон обратного и прямого просмотра должны быть синхронизированы. В случае сбоя синхронизации может произойти сбой проверки подлинности в домене.

Создать зоны обратного просмотра можно с помощью следующих действий:

1. Запустите консоль **Диспетчер DNS**. Если нужного сервера нет в списке, подключитесь к нему, как было описано ранее.

2. Щелкните правой кнопкой мыши на записи сервера, а затем выберите команду **Создать новую зону**. Будет запущен мастер создания новой зоны. Нажмите кнопку **Далее**.
3. Если настраивается основной сервер, интегрированный в Active Directory (контроллер домена), выберите переключатель **Основная зона** (Primary Zone) и убедитесь, что флажок **Сохранять зону в Active Directory** (Store the zone in Active Directory) установлен. Если интеграция DNS с Active Directory не нужна, выберите переключатель **Основная зона** и сбросьте флажок **Сохранять зону в Active Directory**. Нажмите кнопку **Далее**.
4. Если настраивается зона обратного просмотра для дополнительного сервера, выберите переключатель **Дополнительная зона** (Secondary Zone) и нажмите кнопку **Далее**.
5. Если зона интегрируется с Active Directory, выберите одну из следующих стратегий.
   - **Для всех DNS-серверов, работающих на контроллерах домена в этом лесу** (To all DNS servers running on domain controllers in this forest) — выберите эту стратегию для самой обширной репликации. Помните, что лес Active Directory содержит также все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - **Для всех DNS-серверов, работающих на контроллерах домена в этом домене** (To all DNS servers running on domain controllers in this domain) — выберите эту стратегию, если нужно реплицировать DNS-информацию в пределах текущего домена.
   - **Для всех контроллеров домена в этом домене (для совместимости с Windows 2000)** (To all domain controllers in this domain (for Windows 2000 compatibility)) — выберите эту стратегию, если нужно реплицировать DNS-информацию всем контроллерам домена в текущем домене, что необходимо для совместимости с Windows 2000. Хотя эта стратегия обеспечивает более широкую репликацию DNS-информации внутри домена и совместимость с Windows 2000, не каждый контроллер домена является DNS-сервером (и не нужно настраивать каждый контроллер домена как DNS-сервер).
6. Выберите переключатель **Зона обратного просмотра** (Reverse Lookup Zone) и нажмите кнопку **Далее**.
7. Укажите, для каких адресов нужно создать зону обратного просмотра (IPv4 или IPv6), и нажмите кнопку **Далее**. Выполните одно из следующих действий.
   - Если настраивается зона обратного просмотра для IPv4, введите идентификатор сети для зоны обратного просмотра. Вводимые значения определяют стандартное имя зоны обратного просмотра. Нажмите кнопку **Далее**.
   - Если есть несколько подсетей в одной сети, например 192.168.10 и 192.168.11, можно ввести только часть сети в качестве имени зоны. Например, в этом случае нужно использовать имя 168.192.in-addr.arpa и разрешить консоли **Диспетчер DNS** создать необходимые зоны подсетей, когда они понадобятся.

- Если настраивается зона обратного просмотра для IPv6, введите префикс сети для зоны обратного просмотра. Имена зон автоматически генерируются на основе вводимых значений. В зависимости от введенного префикса можно создать до восьми зон. Нажмите кнопку **Далее**.

8. Если настраивается основной или дополнительный сервер, не интегрированный в Active Directory, введите имя файла зоны. Имя файла для базы данных зоны DNS должно быть уже введено. Оставьте его неизменным или введите новое имя. Нажмите кнопку **Далее**.
9. Укажите, будут ли разрешены динамические обновления.
   - **Разрешить только безопасные динамические обновления** — когда зона интегрирована с Active Directory, можно использовать списки управления доступом для ограничения круга клиентов, которые могут осуществлять динамические обновления. Когда включена эта опция, только клиенты с авторизированными учетными записями компьютера и одобренными списками управления доступом могут динамически обновлять свои записи ресурсов в DNS.
   - **Разрешить любые динамические обновления** — выберите эту опцию, чтобы разрешить любому клиенту обновлять свои записи ресурсов в DNS. Клиенты могут быть безопасными и небезопасными.
   - **Запретить динамические обновления** — отключает динамические обновления DNS. Нужно выбрать эту опцию, только если зона не интегрирована с Active Directory.
10. Нажмите кнопку **Далее**, а затем кнопку **Готово** для завершения этого процесса. Новая зона будет добавлена на сервер, базовые DNS-записи будут созданы автоматически.

После установки зон обратного просмотра необходимо убедиться в правильности обработки делегирования для зоны. Свяжитесь с IT-отделом или интернет-провайдером, чтобы проверить регистрацию зон в родительском домене.

Настройка глобальных имен

Зона GlobalNames — это специальная зона прямого просмотра, которую нужно интегрировать с AD DS. Если все DNS-серверы работают под управлением Windows Server 2008 или более поздних версий, при развертывании зоны GlobalNames создаются статические, глобальные записи с однокомпонентными именами без использования WINS. Это позволяет пользователям получать доступ к хостам по однокомпонентным именам, не прибегая к FQDN-именам. Использовать зону GlobalNames нужно в случаях, если разрешение имен было решено возложить на DNS, полностью отказавшись от WINS, чтобы в перспективе перейти на IPv6. Поскольку для регистрации обновлений в зоне GlobalNames нельзя использовать динамические обновления, настраивать разрешение однокомпонентных имен следует только для основных серверов.

Разместить зону GlobalNames можно с помощью следующих действий:

1. В консоли **Диспетчер DNS** выберите DNS-сервер, который также является контроллером домена. Если нужного сервера нет в списке, подключитесь к нему, как было описано ранее.

2. Щелкните правой кнопкой мыши на узле **Зоны прямого просмотра** (Forward Lookup Zones) и выберите команду **Создать новую зону**. В окне мастера создания новой зоны нажмите кнопку **Далее**, чтобы по умолчанию создать основную зону, интегрированную с AD DS. На странице **Область репликации зоны, интегрированной в Active Directory** (Active Directory Zone Replication Scope) задайте репликацию зоны в лесе и нажмите кнопку **Далее**. На странице **Имя зоны** (Zone Name) введите имя `GlobalNames`. Два раза нажмите кнопку **Далее** и кнопку **Готово**.

3. На каждом полномочном DNS-сервере леса введите в командной строке с повышенными полномочиями команду

   ```
   Set-DnsServerGlobalNameZone -ComputerName ServerName -Enable $True
   ```

   где *ServerName* — имя DNS-сервера, содержащего зону GlobalNames. Чтобы указать локальный компьютер, просто опустите параметр `-ComputerName`, например,

   ```
   Set-DnsServerGlobalNameZone -Enable $True
   ```

4. Для каждого сервера, доступ к которому должны иметь пользователи, в зону GlobalNames добавьте запись CNAME: в консоли **Диспетчер DNS** щелкните правой кнопкой мыши на узле **GlobalNames**, выберите команду **Создать псевдоним (CNAME)** (New Alias (CNAME)) и создайте новую запись ресурса в открывшемся диалоговом окне.

> ***Примечание***
>
> Полномочный DNS-сервер пытается разрешить запросы в следующем порядке, используя: данные локальной зоны, зону GlobalNames, DNS-суффиксы, WINS. Для динамических обновлений полномочный DNS-сервер проверяет зону GlobalNames перед проверкой данных локальной зоны.

> ***Совет***
>
> Если нужно, чтобы DNS-клиенты из другого леса использовали зону GlobalNames для разрешения имен, необходимо добавить запись ресурса SRV с именем службы _globalnames._msdcs в DNS-раздел леса. Запись должна указывать FQDN-имя DNS-сервера, содержащего зону GlobalNames.

Управление DNS-серверами

Консоль **Диспетчер DNS** — это утилита, используемая для управления локальным и удаленными DNS-серверами. Как показано на рис. 9.4, главное окно консоли **Диспетчер DNS** разделено на две панели. Левая панель позволяет получить доступ к DNS-серверам и их зонам. Правая панель показывает подробности для выбранного в данный момент элемента. Можно работать с консолью **Диспетчер DNS** тремя способами:

- дважды щелкните на элементе на левой панели, чтобы развернуть список файлов для элемента;
- выделите элемент на левой панели, чтобы просмотреть на правой панели сведения о нем, например состояние зоны и доменные записи;
- щелкните на элементе правой кнопкой мыши, чтобы открыть контекстное меню для элемента.

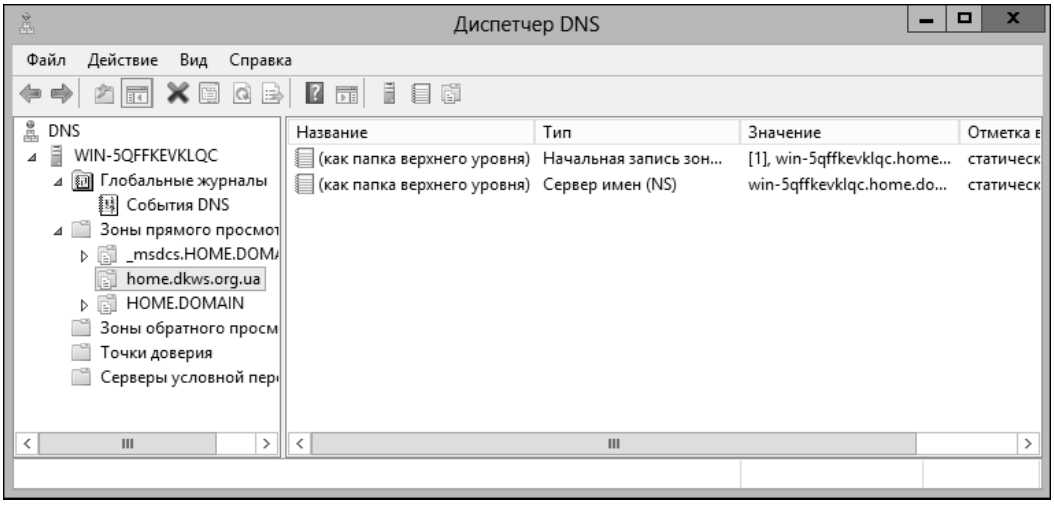


Рис. 9.4. Управляйте локальным и удаленными DNS-серверами с помощью консоли **Диспетчер DNS**

Папки **Зоны прямого просмотра** (Forward Lookup Zones) и **Зоны обратного просмотра** (Reverse Lookup Zones) предоставляют доступ к доменам и подсетям, настроенным для использования на данном сервере. Выбирая папки домена или подсети в левой панели, можно управлять DNS-записями для домена или подсети соответственно.

Добавление и удаление серверов для управления

Можно использовать консоль **Диспетчер DNS** для управления DNS-серверами так:

1. Щелкните правой кнопкой мыши на узле **DNS** в дереве консоли и выберите команду **Подключение к DNS-серверу** (Connect To DNS Server).
2. Если подключаетесь к локальному компьютеру, выберите переключатель **этот компьютер**. В противном случае выберите переключатель **другой компьютер**, а затем введите IP-адрес или FQDN-имя узла удаленного компьютера, к которому нужно подключиться.
3. Нажмите кнопку **OK**. Операционная система Windows Server 2012 R2 попытается подключиться к серверу. Если получится, сервер будет добавлен в консоль.

> ***Примечание***
>
> Если сервер отключен от сети или недоступен по другой причине (например, есть проблемы со службой **Удаленный вызов процедур - RPC**), соединение не удастся. Но все еще можно добавить сервер в консоль, нажав кнопку **Да**, когда появится запрос, нужно ли добавить недоступный сервер.

В консоли **Диспетчер DNS** можно удалить сервер, щелкнув на записи сервера правой кнопкой мыши и выбрав команду **Удалить**. Для подтверждения действия нажмите кнопку **Да**. Удаление сервера аннулирует его только из списка серверов в консоли, оно не удаляет фактически сам сервер.

Запуск и остановка DNS-сервера

Для управления DNS-серверами можно использовать службу **DNS-сервер**. Управлять службой (запустить, остановить, приостановить, возобновить работу и перезапустить) можно через оснастку **Службы**, из командной строки и в консоли **Диспетчер DNS**. Щелкните правой кнопкой мыши на сервере и выберите команду **Все задачи** (All Tasks), а далее нужную команду: **Запустить** (Start), **Остановить** (Stop), **Приостановить** (Pause), **Продолжить** (Resume) или **Перезапустить** (Restart).

> ***Примечание***
>
> В диспетчере серверов тоже можно управлять DNS-сервером: разверните узел **DNS**, щелкните правой кнопкой мыши на сервере, а затем в контекстном меню выберите нужную команду (**Запустить службы**, **Остановить службы** и т. д.).

Использование DNSSEC и подпись зон

Операционная система Windows 7 и более поздние версии, так же как и Windows Server 2008 R2 и более поздние версии, поддерживают DNSSEC (DNS Security Extensions, расширения безопасности DNS). Расширения безопасности DNSSEC определены в нескольких рекомендациях RFC: 4033, 4034 и 4035. Эти RFC добавляют проверку подлинности, целостность данных и отказ в доступе к DNS. DNSSEC добавляет следующие записи ресурсов:

- DNSKEY (Domain Name System Key);
- RRSIG (Resource Record Signature);
- NSEC (NextSECure);
- DS (Domain Services).

DNS-клиент, запущенный на этих операционных системах, может отправлять запросы для определения поддержки DNSSEC, которые позволяют DNS-серверам безопасно подписывать зоны, размещать подписанные DNSSEC зоны, обрабатывать соответствующие записи и осуществлять проверку подлинности и аутентификацию. Способ работы DNS-клиента с DNSSEC задается в таблице политик разрешения имен (Name Resolution Policy Table, NRPT), которая содержит настройки, определяющие поведение DNS-клиента. Обычно таблицей NRPT нужно управлять через групповую политику.

Когда DNS-сервер, размещающий подписанную зону, получает запрос, сервер возвращает цифровые подписи вместе с запрошенными клиентом записями. Распознаватель или другой сервер, настроенный на проверку подписи, могут получить открытый ключ пары "открытый/закрытый ключи" и установить, что ответ является подлинным.

В качестве части плана предразвертывания нужно идентифицировать DNS-зоны, которые будут защищены цифровыми подписями. DNS-сервер для Windows Server 2012 R2 обладает следующими расширениями для DNSSEC.

- Поддержка динамических обновлений в зонах, интегрированных в Active Directory. Ранее, если зона домена Active Directory была подписана, нужно было вручную обновлять все SRV-записи и другие ресурсные записи. Теперь в этом нет необходимости, поскольку DNS-сервер делает это автоматически.

- Поддержка онлайн-подписей, автоматического управления ключами, автоматического распределения *якорей доверия* (trust anchors). Ранее нужно было настраивать и управлять подписями, ключами и якорями. Теперь в этом нет необходимости, поскольку DNS-сервер делает это автоматически.
- Поддержка проверки записей, подписанных с учетом обновленных стандартов DNSSEC (стандарты NSEC3 и RSA/SHA-2). Ранее записи подписывались с помощью стандартов NSEC3 и RSA/SHA-2.

ОС Windows Server 2012 R2 позволяет авторитетному серверу DNS работать как мастер ключей (key master) для DNSSEC. Мастер ключей управляет ключами как в интегрированных в Active Directory зонах, защищенных DNSSEC, так и в стандартных зонах, защищенных DNSSEC. Когда у зоны есть назначенный мастер ключей, он отвечает за весь процесс, связанный с ключами, — от их генерирования до хранения, вращения и удаления.

Хотя подписание ключей и задачи управления могут быть инициированы только мастером ключей, другие первичные серверы DNS могут использовать подписание зоны, но через мастера ключей. Администратору нужно выбрать мастера ключей для подписания зоны с помощью DNSSEC. Администратор может передать роль мастера ключей другому серверу DNS в любое время.

Также помните о следующем.

- Для зон, не интегрированных с Active Directory, основной и все дополнительные серверы, размещающие зону, должны работать под управлением Windows Server 2008 R2 или более поздней версии или под управлением другой операционной системы, где есть DNSSEC-совместимый DNS-сервер.
- Для зон, интегрированных с Active Directory, каждый контроллер домена, который является DNS-сервером в домене, должен работать под управлением Windows Server 2008 R2 или более поздней версии, если подписанная зона настроена для репликации всем DNS-серверам в домене. Каждый контроллер домена, который действует как DNS-сервер в лесу, должен работать под управлением Windows Server 2008 R2 или более поздней версии, если подписанная зона реплицируется всем DNS-серверам леса.
- Для смешанного окружения все серверы, являющиеся *авторитетными* (заслуживающими доверия), для DNSSEC-подписанной зоны должны поддерживать DNSSEC. DNS-клиенты с поддержкой DNSSEC, запрашивающие DNSSEC-данные и проверку подлинности, должны быть настроены на использование DNS-запросов серверу с поддержкой DNSSEC. Серверы с поддержкой DNSSEC должны быть настроены так, чтобы они отправляли рекурсивные запросы серверам без поддержки DNSSEC.

Защита DNS-зон с помощью цифровых подписей — это многоэтапный процесс. Как часть этого процесса, нужно назначить *мастер ключей* (key master). Любой авторитетный сервер, содержащий основную копию зоны, может выступать в роли такого сервера. Далее нужно сгенерировать ключ для подписи ключа (Key Signing Key, KSK) и ключ для подписи зоны (Zone Signing Key, ZSK). *Ключ для подписи ключа* — аутентификационный ключ, имеющий закрытый и открытый ключи, связанные с ними. Закры-

тый ключ (private key) служит для подписи всех записей DNSKEY в корне зоны. Открытый ключ (public key) используется как якорь доверия для проверки DNS-ответов. *Ключ для подписи зоны* применяется для подписей записей зоны.

После того как ключи будут сгенерированы, необходимо создать записи для отрицания существования при проверке подлинности с использованием более безопасного стандарта NSEC3 или менее безопасного стандарта NSEC. Поскольку якоря доверия используются для проверки DNS-ответов, также нужно указать, как якоря доверия будут обновляться и распространяться. Обычно нужно автоматически обновлять и распространять якоря доверия. По умолчанию записи подписываются с помощью шифрования SHA-1 и SHA-256. При желании можно выбрать другие алгоритмы шифрования.

Не нужно производить процесс настройки при каждой подписи зоны. Ключи и другие параметры подписи можно использовать повторно.

Чтобы подписать зону, выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на зоне, которую нужно подписать. Из контекстного меню выберите команду **DNSSEC | Подписать зону** (Sign The Zone). Будет запущен мастер подписывания зоны (Zone Signing Wizard). Прочитайте приветствие и нажмите кнопку **Далее**.
2. На странице **Параметры подписывания** (Signing Options) выберите переключатель **Настроить параметры подписывания зоны** (Customize zone signing parameters) и нажмите кнопку **Далее**.
3. Выберите мастер ключей для зоны. Любой сервер, заслуживающий доверия, который содержит основную копию зоны, может действовать в роли мастера ключей. Когда будете готовы продолжить, нажмите кнопку **Далее** дважды.
4. На странице **Ключ подписывания ключа (KSK)** (Key Signing Key) настройте KSK-ключ. Нажмите кнопку **Добавить**, примите или измените параметры по умолчанию и нажмите кнопку **OK**. Как только будете готовы, нажмите кнопку **Далее** дважды.
5. На странице **Ключ подписывания зоны** (Zone Signing Key) настройте ZSK-ключ. Нажмите кнопку **Добавить**, примите или измените параметры по умолчанию, а затем нажмите кнопку **OK**. Когда будете готовы, нажмите кнопку **Далее** пять раз.
6. Когда мастер подпишет зону, нажмите кнопку **Готово**.

Чтобы подписать зону с использованием существующих параметров подписи, выполните следующие действия:

1. В консоли **Диспетчер DN**S щелкните правой кнопкой мыши на зоне, которую нужно подписать. Из контекстного меню выберите команду **DNSSEC | Подписать зону**. Будет запущен мастер подписывания зоны. Прочитайте приветствие и нажмите кнопку **Далее**.
2. На странице **Параметры подписывания** выберите переключатель **Подписать зону с использованием параметров существующей зоны** (Sign the zone with parameters of an existing zone). Введите имя существующей подписанной зоны, например cpandl.com, и нажмите кнопку **Далее**.

3. На странице **Мастер ключей** (Key Master) выберите мастер ключей для зоны. Любой сервер, заслуживающий доверия, который содержит основную копию зоны, может действовать в роли мастера ключей. Как только будете готовы продолжить, нажмите кнопку **Далее** дважды.
4. После того как мастер подпишет зону, нажмите кнопку **Готово**.

Создание дочерних доменов в зонах

Используя консоль **Диспетчер DNS**, можно создать дочерние домены в зоне. Например, если создана основная зона **microsoft.com**, можно создать поддомены **hr.microsoft.com** и **mis.microsoft.com**.

Создать дочерние домены можно так:

1. В консоли **Диспетчер DNS** разверните папку **Зоны прямого просмотра** для сервера, с которым нужно работать.
2. Щелкните правой кнопкой мыши на записи родительского домена и выберите команду **Создать домен** (New Domain).
3. Введите имя нового домена и нажмите кнопку **OK**. Для **hr.microsoft.com** нужно просто ввести hr. Для **mis.microsoft.com** нужно ввести mis.

Создание дочерних доменов в отдельных зонах

По мере роста организации иногда нужно разделить пространство имен DNS на отдельные зоны. Штаб-квартира корпорации может находиться в зоне родительского домена **microsoft.com**. Филиалы могут иметь зону для каждого офиса, например **memphis.microsoft.com**, **newyork.microsoft.com** и **la.microsoft.com**.

Создать дочерние домены в разных зонах можно так:

1. В каждом дочернем домене установите DNS-сервер и создайте необходимые зоны прямого и обратного просмотра для дочернего домена, как было описано ранее в *разд. "Установка DNS-серверов"*.
2. Делегируйте полномочия для каждого дочернего домена на полномочном DNS-сервере родительского домена. Делегирование полномочий позволяет дочернему домену разрешать и отвечать на DNS-запросы компьютеров, находящихся внутри и за пределами локальной подсети.

Чтобы делегировать полномочия дочернему домену, выполните следующие действия:

1. В консоли **Диспетчер DNS** раскройте папку **Зоны прямого просмотра** нужного сервера.
2. Щелкните правой кнопкой мыши по родительскому домену и выберите команду **Создать делегирование** (New Delegation). Запустится мастер делегирования (New Delegation Wizard). Нажмите кнопку **Далее**.
3. Введите имя делегированного домена, например service, а затем нажмите кнопку **Далее** (рис. 9.5). Введенное имя будет отражено в поле **Полное доменное имя (FQDN)** (Fully qualified domain name (FQDN)).

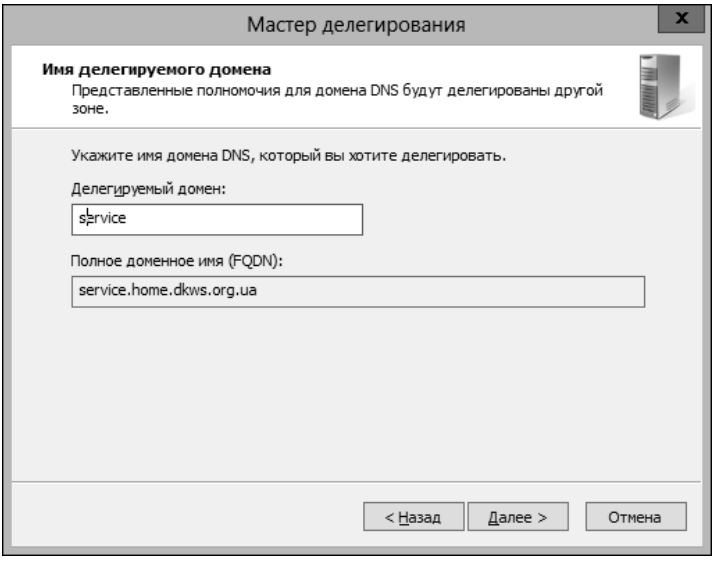


Рис. 9.5. При вводе имени делегированного домена

4. Нажмите кнопку **Добавить**. Откроется окно **Новая запись сервера имен** (New Name Server Record).
5. В поле **Полное доменное имя сервера** (Server fully qualified domain name) введите полное имя DNS-сервера для дочернего домена, например corpserver01.memphis.adatum.com, а затем нажмите кнопку **Разрешить в адрес** (Resolve). Сервер отправит запрос и добавит разрешенный IP-адрес сервера в список **IP-адреса записи сервера имен** (Name Servers).
6. Повторите шаг 5, чтобы добавить дополнительные серверы имен. Порядок записей определяет, какой из IP-адресов будет использован первым. При необходимости измените порядок с помощью кнопок **Вверх** (Up) и **Вниз** (Down). Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Новая запись сервера имен**.
7. Нажмите кнопку **Далее**, а затем кнопку **Готово**.

Удаление домена или подсети

Удаление домена или подсети удаляет ее без возможности восстановления с DNS-сервера. Для удаления домена или подсети выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на записи домена или подсети.
2. Из контекстного меню выберите команду **Удалить** и подтвердите удаление, нажав кнопку **Да**.
3. Если домен (или подсеть) интегрирован с Active Directory, будет отображено предупреждение. Нажмите кнопку **Да**, чтобы подтвердить удаление DNS-информации из Active Directory.

Примечание

Удаление домена или подсети удаляет все DNS-записи в файле зоны, но не удаляет файлы зоны с основного или дополнительного сервера, который не интегрирован с Active Directory. Фактически файл зоны останется в каталоге *%SystemRoot%*\System32\Dns. Можно удалить этот файл после удаления зоны из консоли **Диспетчер DNS**.

Управление записями DNS

После создания необходимых файлов зоны можно добавить в них записи. Для компьютеров, к которым необходим доступ из Active Directory и доменов DNS, нужно создать записи DNS. Хотя существует много типов записей DNS, большинство из них не используется часто. Давайте сконцентрируем внимание на тех записях, которые чаще всего востребованы.

- A (IPv4-адрес) — используется для преобразования имени узла в IPv4-адрес. Когда у компьютера есть несколько сетевых карт, IPv4-адресов (или несколько и сетевых карт, и адресов), для компьютера должно быть создано несколько записей адреса.
- AAAA (IPv6-адрес) — используется для преобразования имени узла в IPv6-адрес. Когда у компьютера несколько сетевых карт, IPv6-адресов (или несколько и сетевых карт, и адресов), для компьютера должно быть создано несколько записей адреса.
- CNAME (canonical name, каноническое имя) — устанавливает псевдоним для имени узла. Например, можно с помощью этой записи установить псевдоним **www.microsoft.com** для узла **zeta.microsoft.com**.
- MX (mail exhanger) — указывает сервер обмена почты для домена, позволяющий отправлять сообщения электронной почты корректным почтовым серверам в домене.
- NS (name server) — определяет сервер имен для домена. У каждого основного и дополнительного сервера должна быть эта запись.
- PTR (указатель) — создает указатель, преобразующий IP-адрес в имя узла (обратный запрос).
- SOA (start of authority, начало полномочий) — объявляет хост, обладающий наибольшими полномочиями в зоне и потому являющийся наилучшим источником DNS-информации в зоне. Начальная запись зоны (SOA) должна быть в каждом файле зоны (который создается автоматически при добавлении зоны). Также она объявляет другую информацию о зоне, например ответственное лицо, интервал обновления, интервал повтора и т. д.
- SRV (service location) — определяет местоположение сервера, предоставляющего определенный сервис. Active Directory использует записи SRV для определения местоположения контроллеров домена, глобальных серверов каталога, серверов LDAP и серверов Kerberos. Большинство записей SRV создается автоматически. Например, Active Directory создает запись SRV при повышении статуса сервера до контроллера домена. Серверы LDAP также могут добавить запись SRV, чтобы указать, что они доступны для обработки запросов hanVdle LDAP в определенной зоне.

Добавление записей адреса и указателя

Записи типов A и AAAA используются для преобразования имен узла в IP-адреса. Запись PTR служит для обратного запроса, т. е. для преобразования IP-адреса в имя узла. Можно создать записи адреса и указателя одновременно или по отдельности.

Чтобы создать новый элемент узла при помощи записей адреса и указателя, выполните следующие действия:

1. В консоли **Диспетчер DNS** раскройте папку **Зоны прямого просмотра** нужного сервера.
2. Щелкните правой кнопкой мыши на домене, который нужно обновить, и выберите команду **Создать узел (A или AAAA)** (New Host (A Or AAAA)). Откроется окно, показанное на рис. 9.6.

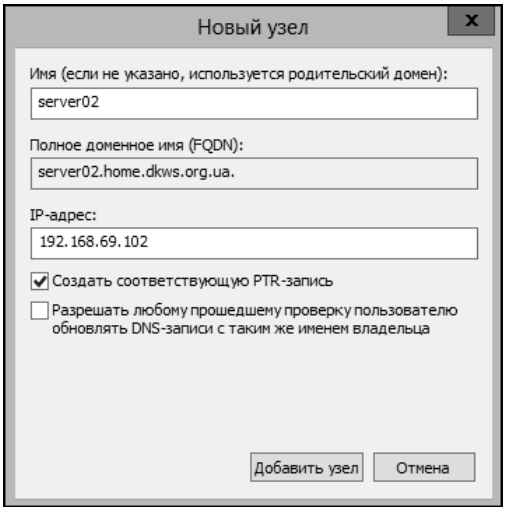


Рис. 9.6. Используйте окно **Новый узел** для одновременного создания записей A и PTR

3. Введите имя компьютера, например servicespc85, и IP-адрес, например 192.168.10.58.
4. Установите флажок **Создать соответствующую PTR-запись** (Create associated pointer (PTR) record).

> ***Примечание***
>
> Можно создать PTR-записи, только если соответствующая зона обратного просмотра доступна. Создать этот файл можно, следуя рекомендациям из *разд. "Настройка зон обратного просмотра" ранее в этой главе*. Опция **Разрешать любому прошедшему проверку пользователю...** (Allow Any Authenticated User) доступна, только когда DNS-сервер настроен на контроллере домена.

5. Нажмите кнопку **Добавить узел** (Add Host), а затем кнопку **OK**. Повторите этот процесс для добавления других узлов.
6. Нажмите кнопку **Готово**, когда закончите.

Добавление записи указателя позже

Чтобы позже добавить PTR-запись для узла, выполните следующие действия:

1. В консоли **Диспетчер DNS** раскройте папку **Зоны обратного просмотра** нужного сервера.
2. Щелкните правой кнопкой мыши на подсети, которую нужно обновить, и выберите команду **Создать указатель** (New Pointer (PTR)).
3. Введите IP-адрес узла, например 192.168.1.95, и имя узла, например servicespc54. Нажмите кнопку **OK**.

Добавление DNS-псевдонимов с помощью CNAME

Псевдонимы узлов определяются посредством записи CNAME. Псевдонимы позволяют одному узлу выдавать себя за несколько узлов. Например, узел **gamma.microsoft.com** может быть как узлом **www.microsoft.com**, так и **ftp.microsoft.com**.

Для создания записи CNAME выполните следующие действия:

1. В консоли **Диспетчер DNS** разверните папку **Зоны прямого просмотра** нужного сервера.
2. Щелкните правой кнопкой мыши на домене, который нужно обновить, и выберите команду **Создать псевдоним (CNAME)** (New alias (CNAME)).
3. В поле **Псевдоним** (Alias Name) введите псевдоним. Псевдоним — это однокомпонентное имя, например www или ftp.
4. В поле **Полное доменное имя (FQDN) конечного узла** (Fully qualified domain name (FQDN) for target host) введите полное имя компьютера, для которого создается псевдоним.
5. Нажмите кнопку **OK**.

Добавление почтовых серверов

Записи MX используются для идентификации серверов обмена почтовыми сообщениями домена, которые отвечают за обработку или пересылку почты внутри домена. Создавая MX-запись, нужно указать номер предпочтения почтового сервера — число от 0 до 65 535, определяющее приоритет почтового сервера в домене. Почтовый сервер с наименьшим предпочтением обладает наибольшим приоритетом и получает почту в первую очередь. В случае сбоя доставки почты используется следующий предпочитаемый номер по возрастанию.

Для создания MX-записи выполните следующие действия:

1. В консоли **Диспетчер DNS** разверните папку **Зоны прямого просмотра** нужного сервера.
2. Щелкните правой кнопкой мыши на домене, который нужно обновить, и выберите команду **Создать почтовый обменник (MX)** (New Mail Exchanger (MX)).

3. Теперь можно создать запись почтового сервера, заполнив следующие поля.
   - **Узел или дочерний домен** (Host or child domain) — при желании введите однокомпонентное имя почтового сервера. В большинстве случаев можно оставить это поле незаполненным, и таким образом имя почтового сервера будет совпадать с именем родительского домена.
   - **Полное доменное имя (FQDN)** (Fully qualified domain name (FQDN)) — введите FQDN-имя домена, к которому относится запись почтового сервера, например **cpandl.com**.
   - **Полное доменное имя (FQDN) почтового сервера** (Fully qualified domain name (FQDN) of mail server) — введите FQDN-имя почтового сервера, например **corpmail.cpand.com**. Сообщения для ранее указанного домена передаются на этот сервер с целью доставки.
   - **Приоритет почтового сервера** (Mail Server Priority) — введите номер предпочтения для узла от 0 до 65 535.

   Примечание

   Назначайте номера предпочтения, оставляя возможность для роста. Например, используйте 10 для сервера с наивысшим приоритетом, 20 — для следующего сервера, 30 — еще для одного сервера.

   Практический совет

   Нельзя вводить многокомпонентное имя в поле **Узел или дочерний домен**. Если нужно ввести многокомпонентное имя, будет создана MX-запись с неправильным уровнем DNS-иерархии. Создайте дополнительный уровень домена, а затем добавьте MX-запись на этом уровне.

4. Нажмите кнопку **OK**.

Добавление серверов имен

Записи NS указывают серверы имен для домена. Каждый основной и дополнительный серверы имен должны быть объявлены с помощью этой записи. Если дополнительные службы имен предоставляет интернет-провайдер, убедитесь, что вставили соответствующие NS-записи.

Создать NS-запись можно так:

1. В консоли **Диспетчер DNS** разверните папку **Зоны прямого просмотра** нужного сервера.
2. Отобразите DNS-записи домена, развернув его узел в дереве консоли.
3. Щелкните правой кнопкой мыши на существующей NS-записи в области просмотра и выберите команду **Свойства**. Диалоговое окно свойств домена откроется на вкладке **Серверы имен** (Name Servers) (рис. 9.7).
4. Нажмите кнопку **Добавить**. Откроется диалоговое окно **Новая запись сервера имен** (New Name Server Record).
5. В поле **Полное доменное имя (FQDN) сервера** (Server fully qualified domain name (FQDN)) введите полное хост-имя DNS-сервера дочернего домена, например

corpserver01.cpandl.com. Нажмите кнопку **Разрешить в адрес** (Resolve). Сервер разрешит имя и добавит разрешенный IP-адрес в список **IP-адреса записи сервера имен** (Name Servers).

6. Повторите шаг 5, чтобы определить дополнительные серверы имен. Порядок записей определяет, какой из IP-адресов будет использован первым. При необходимости измените порядок с помощью кнопок **Вверх** и **Вниз**. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Новая запись сервера имен**.
7. Нажмите кнопку **OK**, чтобы сохранить изменения.

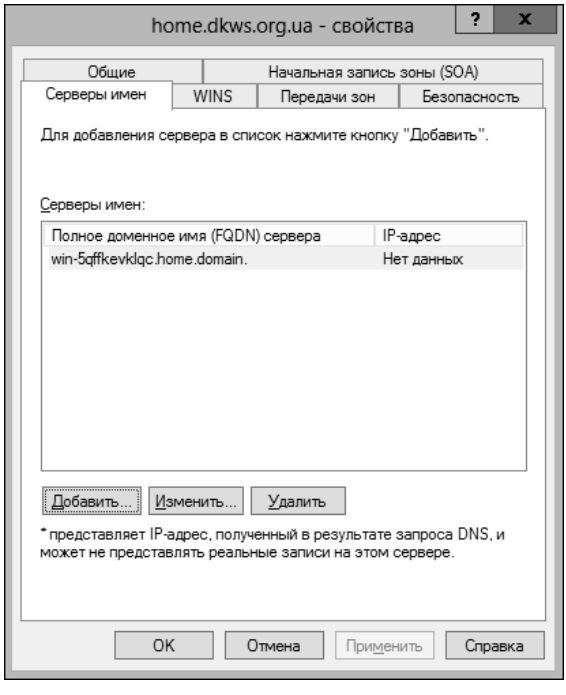


Рис. 9.7. Настройте серверы имен для домена

Просмотр и обновление DNS-записей

Чтобы просмотреть или обновить DNS-записи, выполните следующие действия:

1. Дважды щелкните на зоне, с которой нужно работать. На правой панели будут отображены записи зоны.
2. Дважды щелкните на записи DNS, которую нужно просмотреть или обновить. Откроется окно **Свойства**. Внесите необходимые изменения и нажмите кнопку **OK**.

Обновление свойств зоны и записи SOA

У каждой зоны есть свои отдельные свойства, которые можно настроить. Эти свойства устанавливают общие параметры зоны посредством записи SOA, уведомления об изменении и WINS-интеграции.

В консоли **Диспетчер DNS** можно установить свойства зоны одним из двух способов:

- щелкните правой кнопкой мыши на зоне, которую нужно обновить, и выберите команду **Свойства**;
- выберите зону, а затем выберите команду **Свойства** из меню **Действия**.

Окна **Свойства** для зон прямого и обратного просмотра идентичны за исключением вкладок **WINS** и **WINS-R**. В зонах прямого просмотра используется вкладка **WINS** для настройки просмотров NetBIOS-имен компьютеров. В зонах обратного просмотра используется вкладка **WINS-R** для настройки обратного просмотра для NetBIOS-имен компьютера.

Изменение записи SOA

Начальная запись SOA объявляет полномочный сервер имен зоны и устанавливает общие свойства зоны, например интервалы повторов и обновлений. Можно изменить эту информацию так:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на зоне, которую нужно обновить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Начальная запись зоны (SOA)** (Start of Authority (SOA)) и обновите текстовые поля, показанные на рис. 9.8.

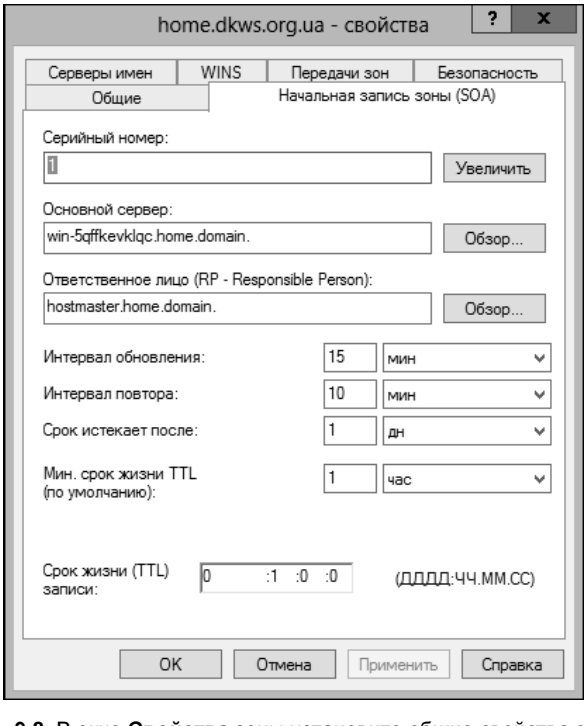


Рис. 9.8. В окне **Свойства** зоны установите общие свойства зоны

На вкладке **Начальная запись зоны (SOA)** доступны следующие параметры.

- **Серийный номер** (Serial number) — отражает версию файлов базы данных DNS. Номер обновляется автоматически при внесении изменений в файлы зоны, но можно обновить его и вручную. По этому номеру дополнительные серверы определяют, изменилась ли зона. Если серийный номер основного сервера превышает серийный номер дополнительного сервера, записи изменились, и дополнительный сервер может запросить DNS-записи зоны. Кроме того, можно настроить DNS на уведомление дополнительных серверов об изменениях (что ускоряет процесс обновления).
- **Основной сервер** (Primary server) — полное доменное имя сервера, в конце которого стоит точка. Она обозначает конец имени и гарантирует, что к записи не будет добавлена информация о домене.
- **Ответственное лицо** (Responsible person) — адрес электронной почты лица, ответственного за домен. По умолчанию здесь стоит имя hostmaster, за которым следует точка. Это обозначает адрес hostmaster@*домен*.com. При вводе здесь другого адреса замените точкой символ @ в адресе электронной почты и в конце адреса также поставьте точку.
- **Интервал обновления** (Refresh interval) — интервал, через который дополнительный сервер проводит проверку обновлений зоны. Если интервал установлен в 60 минут, изменения на дополнительном сервере отобразятся через час. Можно уменьшить сетевой трафик, увеличивая это значение.
- **Интервал повтора** (Retry interval) — время после сбоя, в течение которого дополнительный сервер не загружает базы данных зоны. Если задан интервал 10 минут, после сбоя передачи базы данных зоны дополнительный сервер ждет 10 минут, прежде чем отправить новый запрос.
- **Срок истекает после** (Expires after) — период времени, в течение которого информация зоны на дополнительном сервере считается достоверной. Если дополнительный сервер в течение этого времени не может загрузить данные с основного сервера, данные в кэше дополнительного сервера устаревают, и дополнительный сервер перестает отвечать на DNS-запросы. Установка этого параметра в 7 дней позволяет данным на дополнительном сервере быть достоверными неделю.
- **Мин. срок жизни TTL (по умолчанию)** (Minimum (default) TTL) — минимальное время жизни записей на дополнительном сервере. Данное значение можно установить в днях, часах, минутах или секундах. Когда это время заканчивается, дополнительный сервер считает срок действия соответствующей записи истекшим и сбрасывает ее. После этого необходимо отправлять очередной запрос на основной сервер. Делайте минимальный срок жизни относительно большим, например 24 часа. Это сократит сетевой трафик и повысит производительность. С другой стороны, нужно помнить, что высокое значение замедляет распространение обновлений через Интернет.
- **Срок жизни (TTL) записи** (TTL for this record) — время жизни конкретной SOA-записи в формате ДД:ЧЧ:ММ:СС. Как правило, оно должно совпадать с минимальным временем жизни всех записей.

Разрешение и запрещение передачи зоны

При передаче зоны отправляется копия информации зоны другим DNS-серверам. Эти серверы могут находиться в одном и том же домене или в разных доменах. По соображениям безопасности в Windows Server 2012 R2 передача зоны отключена. Чтобы включить эту функцию для дополнительных серверов организации или для DNS-серверов интернет-провайдера, нужно разрешить передачу зоны и указать типы серверов, на которые разрешено передавать зону.

Хотя можно разрешить передачу зоны любому серверу, это открывает потенциальные проблемы с безопасностью. Вместо этого нужно ограничить доступ к информации зоны так, чтобы запрашивать обновления с основного сервера зоны могли только указанные вами серверы. Это позволит ограничить запросы определенной группой дополнительных серверов, например серверов имен поставщика Интернета, а также скрыть внутреннюю сеть от внешнего мира.

Чтобы разрешить передачи зоны и ограничить доступ к базе данных основной зоны, выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на домене или подсети, которые хотите обновить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Передачи зон** (Zone Transfers) (рис. 9.9).
3. Чтобы ограничить переносы серверами имен, перечисленными на вкладке **Серверы имен** (Name Servers), установите флажок **Разрешить передачи зон** (Allow zone

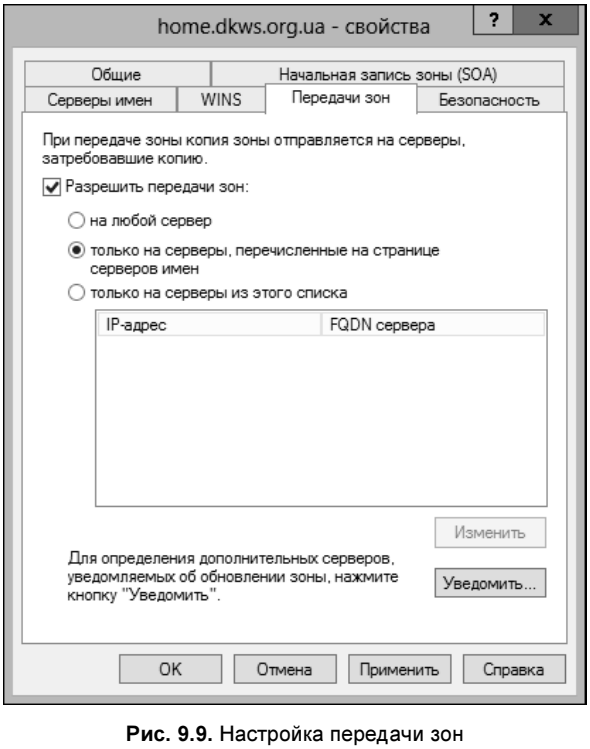


Рис. 9.9. Настройка передачи зон

transfers) и переключатель **только на серверы, перечисленные на странице серверов имен** (Only to servers listed on the Name Servers tab).

4. Чтобы ограничить переносы указанными серверами, установите флажок **Разрешить передачи зон** и выберите переключатель **только на серверы из этого списка** (Only to the following servers). Затем нажмите кнопку **Изменить**, чтобы открыть диалоговое окно **Разрешить передачи зон** (Allow Zone Transfers). Щелкните на колонке **IP-адрес** (IP Address), введите IP-адрес дополнительного сервера зоны и нажмите клавишу <Enter>. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Если необходимо копировать данные зоны из других серверов на случай недоступности первого сервера, добавьте IP-адреса и других серверов. Нажмите кнопку **OK**.
5. Нажмите кнопку **OK**, чтобы сохранить изменения.

Уведомление дополнительных серверов об изменениях

Свойства зоны устанавливаются посредством SOA-записи. Параметры зоны регулируют распространение информации DNS по сети. Можно также указать основному серверу, чтобы он рассылал уведомления дополнительным серверам имен при наличии изменений в базе данных зоны. Для этого выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на домене или подсети, которые нужно обновить, и выберите команду **Свойства**.
2. На вкладке **Передачи зон** нажмите кнопку **Уведомить** (Notify). Откроется окно, изображенное на рис. 9.10.

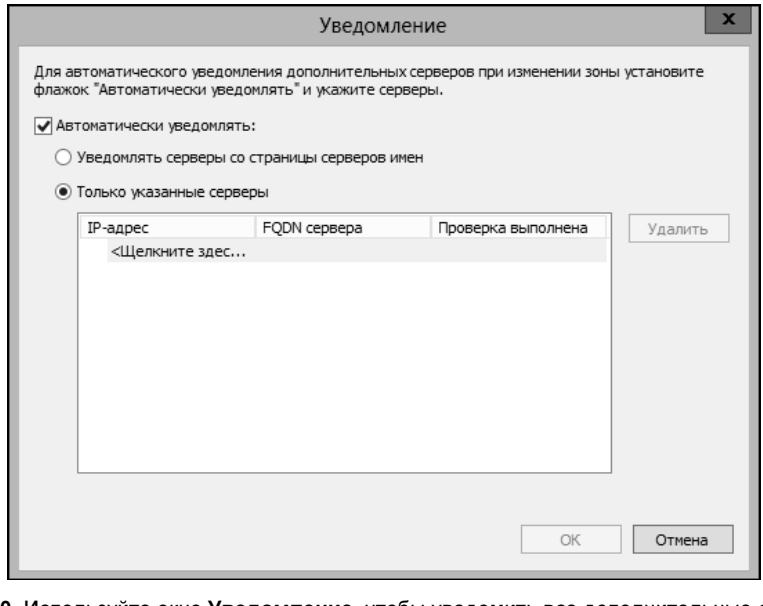


Рис. 9.10. Используйте окно **Уведомление**, чтобы уведомить все дополнительные серверы, указанные либо на вкладке **Серверы имен**, либо в списке этого окна

3. Чтобы уведомлять серверы имен, перечисленные на вкладке **Серверы имен**, установите флажок **Автоматически уведомлять** (Automatically notify) и переключатель **Уведомлять серверы со страницы серверов имен** (Servers listed on the Name Servers tab).
4. Чтобы указать серверы для получения уведомлений, установите флажок **Автоматически уведомлять** и переключатель **Только указанные серверы** (The following servers). Щелкните в списке на IP-адресе, введите IP-адрес дополнительного сервера зоны и нажмите клавишу <Enter>. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Если нужно уведомлять другие серверы, добавьте их IP-адреса.
5. Дважды нажмите кнопку **OK**.

Установка типа зоны

При создании зоны назначаются тип зоны и режим интеграции с Active Directory. Можно изменить тип и режим интеграции в любое время с помощью следующих действий:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на домене или подсети, которые нужно обновить, и выберите команду **Свойства**.
2. На вкладке **Общие** напротив параметра **Тип** нажмите кнопку **Изменить**. В окне **Изменение типа зоны** (Change Zone Type) выберите новый тип зоны.
3. Для интегрирования зоны с Active Directory установите параметр **Хранить зону в Active Directory** (Store the zone in Active Directory).
4. Чтобы удалить зону с Active Directory, выключите параметр **Хранить зону в Active Directory** (Store the zone in Active Directory).
5. Дважды нажмите кнопку **OK**.

Включение и выключение динамических обновлений

Динамические обновления позволяют DNS-клиентам регистрировать и обслуживать свои записи адреса и указателя. Это полезно для компьютеров, которые динамически настраиваются средствами DHCP. Включение динамических обновлений поможет динамически настроенным компьютерам определить положение друг друга в сети. Если зона интегрирована в Active Directory, есть возможность включить запрос на безопасные обновления. При безопасных обновлениях определение компьютеров и пользователей, которым позволено динамически обновлять DNS, происходит при помощи списков управления доступом.

Можно включить и отключить динамические обновления с помощью следующих действий:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на домене или подсети, которые нужно обновить, и из контекстного меню выберите команду **Свойства**.

2. Используйте список **Динамическое обновление** (Dynamic Updates) на вкладке **Общие**, чтобы включить или выключить динамические обновления:
   - **Никакие** (None) — отключает динамические обновления;
   - **Небезопасные и безопасные** (Nonsecure and Secure) — включает небезопасные и безопасные динамические обновления;
   - **Только безопасные** (Secure Only) — включает только безопасные динамические обновления. Этот вариант доступен лишь при интеграции с Active Directory.
3. Нажмите кнопку **OK**.

> ***Примечание***
> Параметры интеграции DNS также должны быть настроены для DHCP. Подробно речь об интеграции DHCP и DNS шла в *главе 8*.

Управление конфигурацией DNS-сервера и безопасностью

Окно **Свойства сервера** (Server Properties) используется для управления основной конфигурацией DNS-серверов. С его помощью можно включать и отключать IP-адреса для сервера и контролировать доступ к серверам за пределами организации. Также можно настроить параметры наблюдения, журналирования и другие расширенные параметры.

Включение и отключение IP-адресов для DNS-сервера

По умолчанию многодомные DNS-серверы отвечают на DNS-запросы по всем доступным сетевым интерфейсам и IP-адресам, настроенным для использования.

С помощью консоли **Диспетчер DNS** можно заставить сервер отвечать на запросы только с заданных IP-адресов. Нужно убедиться, что у сервера есть как минимум один IPv4-интерфейс и один IPv6-интерфейс.

Чтобы указать, какие IP-адреса будут использоваться для ответа на запросы, выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду **Свойства**.
2. На вкладке **Интерфейсы** (Interfaces) выберите переключатель **только по указанным IP-адресам** (Only the following IP addresses). Выберите IP-адреса, по которым сервер должен отвечать на DNS-запросы. Только выбранные IP-адреса будут использоваться для DNS. Все другие IP-адреса на сервере будут недоступны для DNS.
3. Нажмите кнопку **OK**.

Управление доступом к внешним DNS-серверам

Ограничение доступа к информации зоны позволяет указать, какие внутренние и внешние серверы могут получать доступ к основному серверу. Для внешних серверов

это означает управление возможностью подключения из внешнего мира. Также можно задать, какие DNS-серверы организации могут получать доступ к серверам за ее пределами. Для этого следует настроить внутри домена DNS-пересылку.

С точки зрения пересылки серверы DNS в домене можно настроить одним из следующих образов.

- **Серверы без пересылки** (Nonforwarders) — серверы должны передавать DNS-запросы, которые они не смогли разрешить, на заданные серверы пересылки. В целом, эти серверы выступают в роли DNS-акцептов для серверов пересылки.
- **Только пересылка** (Forwarding-only) — серверы способны только кэшировать ответы и передавать запросы на серверы пересылки. Известны также как *кэширующие DNS-серверы*.
- **Серверы пересылки** (Forwarders Servers) — серверы, получающие запросы от серверов без пересылки или только с пересылкой. Для разрешения запросов серверы пересылки используют нормальные способы коммуникаций DNS.
- **Серверы условной пересылки** (Conditional forwarders) — серверы, перенаправляющие запросы на основе домена DNS. Условное перенаправление удобно, когда в организации есть несколько внутренних доменов.

> ***Примечание***
>
> Нельзя настроить корневой сервер домена для пересылки (за исключением условной пересылки, используемой с внутренним разрешением имен). Все остальные серверы можно настроить для пересылки.

Создание серверов без пересылки и кэширующих серверов

Для создания серверов без пересылки или кэширующих серверов выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Дополнительно**. Чтобы настроить сервер в качестве сервера без пересылки, убедитесь, что сброшен флажок **Отключить рекурсию (и серверы пересылки)** (Disable recursion), нажмите кнопку **OK** и пропустите следующие действия. Чтобы настроить сервер как сервер пересылки (кэширующий сервер), убедитесь, что установлен флажок **Отключить рекурсию (и серверы пересылки)**.
3. На вкладке **Сервер пересылки** (Forwarders) нажмите кнопку **Изменить**. Откроется окно **Редактировать серверы пересылки** (Edit Forwarders).
4. Щелкните по колонке **IP-адрес**, введите IP-адрес сервера пересылки сети и нажмите клавишу <Enter>. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Повторите процесс, чтобы задать IP-адреса других серверов пересылки.
5. Установите значение поля **Время ожидания пересылки** (Forward queries time out). Это значение задает время, в течение которого сервер без пересылки повторяет попытки опросить текущий сервер пересылки при отсутствии ответа. По истечении

времени ожидания сервер без пересылки пытается запросить следующий сервер пересылок из списка. По умолчанию время ожидания равно 3 секундам. Нажмите кнопку **OK**.

Создание серверов пересылки

Выступать в роли сервера пересылок способен любой DNS-сервер, если он не настроен в качестве сервера без пересылок или кэширующего сервера. На серверах пересылки в сети убедитесь в том, что флажок **Отключить рекурсию** сброшен и сервер не настроен на перенаправление запросов на другие DNS-серверы в домене.

Настройка сервера условной пересылки

Если есть несколько внутренних доменов, нужно задуматься о настройке условной пересылки, которая позволяет направлять запросы конкретных доменов для разрешения на конкретные DNS-серверы. Условная пересылка полезна, если в организации есть несколько внутренних доменов и нужно разрешать запросы между ними.

Для настройки условной пересылки выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на папке **Серверы условной пересылки** (Conditional Forwarders) нужного сервера. В контекстном меню выберите команду **Создать сервер условной пересылки** (New Conditional Forwarder).
2. В диалоговом окне **Создать сервер условной пересылки** (New Conditional Forwarder) введите имя домена, в который следует пересылать запросы, например **adatum.com**.
3. Щелкните по колонке **IP-адрес**, введите IP-адрес полномочного DNS-сервера в указанном домене и нажмите клавишу <Enter>. Повторите процесс, чтобы указать дополнительные IP-адреса.
4. При использовании интеграции DNS с Active Directory установите флажок **Сохранять условный сервер пересылки в Active Directory и реплицировать ее следующим образом** (Store this conditional forwarder in Active Directory) и выберите одну из следующих стратегий репликации.
   - **Все DNS-серверы в этом лесу** (All DNS servers in this forest) — самая широкая стратегия репликации. Лес Active Directory включает все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - **Все DNS-серверы в этом домене** (All DNS servers in this domain) — выберите эту стратегию, чтобы реплицировать информацию DNS внутри текущего домена и его дочерних доменов.
   - **Все контроллеры домена в этом домене** (All domain controllers in this domain) — выберите эту стратегию, если хотите реплицировать информацию DNS на все контроллеры домена внутри текущего домена и его дочерних доменов. Хотя эта стратегия обеспечивает более широкую репликацию информации DNS внутри домена, не каждый контроллер домена является DNS-сервером (и не нужно настраивать каждый контроллер домена как DNS-сервер).

5. Установите время ожидания пересылки — время, в течение которого сервер пытается запросить сервер пересылки в случае отсутствия ответа. По истечении времени ожидания сервер пытается запросить следующий полномочный сервер из списка. Время ожидания по умолчанию — 5 секунд. Нажмите кнопку **OK**.
6. Повторите эту процедуру, чтобы настроить условную пересылку для других доменов.

Включение и отключение протоколирования событий

По умолчанию служба DNS отслеживает все DNS-события в журнале событий DNS-сервера. Записи этого журнала содержат информацию обо всех DNS-событиях и доступны через узел **Просмотр событий** в оснастке **Управление компьютером**. Это означает, что все информационные сообщения, предупреждения и ошибки будут записаны. Можно изменить параметры протоколирования так:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду **Свойства**.
2. Используйте параметры на вкладке **Журнал событий** (Event Logging). Чтобы отключить журналирование, установите переключатель **не заносить никакие события** (No Events).
3. Нажмите кнопку **OK**.

Использование журнала отладки для отслеживания активности DNS

Обычно журнал событий DNS-сервер используется для наблюдения за деятельностью DNS-сервера. В этом журнале записаны все события DNS, а просмотреть его можно в узле **Просмотр событий** оснастки **Управление компьютером**. При поиске неисправностей DNS весьма полезной может оказаться настройка временного журнала для отслеживания определенных событий DNS. Не забудьте отключить события после окончания отладки.

Для настройки отладки выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Ведение журнала отладки** (Debug Logging) (рис. 9.11), установите флажок **Записывать пакеты в журнал для отладки** (Log packets for debugging), а затем отметьте флажки событий, временное наблюдение за которыми необходимо вести.
3. В поле **Имя и путь к файлу** (File path and name) введите имя файла журнала, например dns.log. По умолчанию журналы хранятся в папке *%SystemRoot%*\System32\Dns.
4. Нажмите кнопку **OK**. Завершив отладку, отключите протоколирование, сбросив флажок **Записывать пакеты в журнал для отладки** (Log packets for debugging).

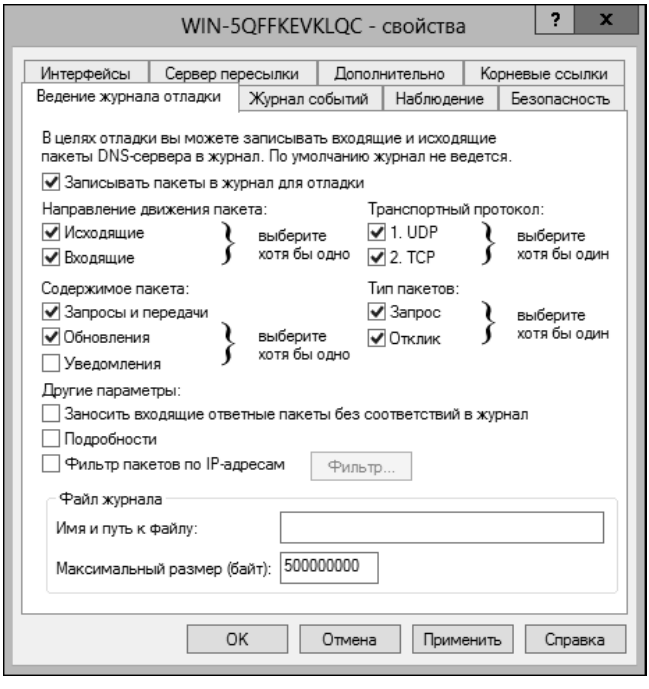


Рис. 9.11. Используйте вкладку **Ведение журнала отладки** для выбора отслеживаемых событий

Мониторинг DNS-сервера

ОС Windows Server 2012 R2 обладает встроенной возможностью мониторинга DNS-сервера. Эта процедура позволяет убедиться, что разрешение DNS имен настроено правильно.

Чтобы настроить ручное или автоматическое выполнение мониторинга, выполните следующие действия:

1. В консоли **Диспетчер DNS** щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Наблюдение** (Monitoring) (рис. 9.12). Можно провести два типа тестов. Чтобы проверить разрешение DNS на текущем сервере, установите флажок **Простой запрос к этому DNS-серверу** (Simple query against this DNS server). Чтобы проверить разрешение DNS в домене, установите флажок **Рекурсивный запрос к другим DNS-серверам** (A recursive query to other DNS servers).
3. Можно провести тестирование вручную. Для этого нажмите кнопку **Тест** (Test Now). Чтобы запланировать автоматический мониторинг, установите флажок **Автоматическое тестирование** (Perform automatic testing at the following interval) и интервал в секундах, минутах или часах.
4. Результаты тестирования отображаются в разделе **Результаты теста** (Test Results). Здесь указаны дата и время проведения теста, а также его результаты, например

Пройден (Pass). Причиной отдельного сбоя может стать временная неисправность. Несколько сбоев указывают на проблему с разрешением имен.

Примечание

Если провалены все рекурсивные тесты, нужно отключить рекурсию, выбрав опцию **Отключить рекурсию** (Disable Recursion) на вкладке **Дополнительно**.

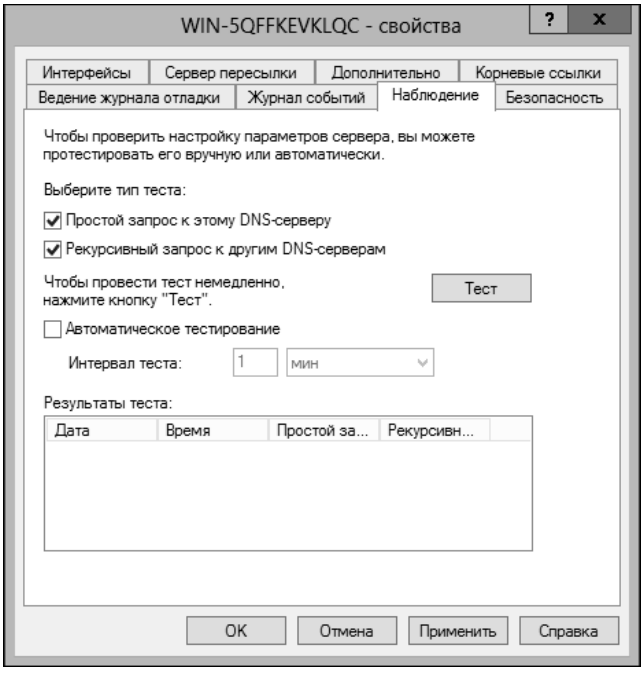


Рис. 9.12. Можно произвести ручное наблюдение или настроить сервер для автоматического мониторинга

Практический совет

Если в данный момент диагностируется DNS, нужно производить тестирование каждые 10–15 секунд. Этот интервал обеспечивает быструю последовательность результатов теста. Если же просто нужно контролировать работу DNS, можете установить более длительный временной интервал, например два или три часа.

ГЛАВА 10

Администрирование сетевых принтеров и служб печати

Администратору следует выполнить два основных действия, чтобы пользователи всей сети получили доступ к устройствам печати, подключенным к Windows Server 2012 R2. Во-первых, администратору нужно установить сервер печати, а во-вторых, использовать его, чтобы предоставить общий доступ к устройствам печати в сети.

В этой главе рассматриваются основы установки общей печати и описывается, как пользователи могут получить доступ к принтерам по сети. Также вы найдете советы относительно администрирования принтеров и решения проблем, возникающих с сетевыми принтерами.

Управление ролью *Службы печати и документов*

Роль **Службы печати и документов** предоставляет центральное расположение для совместного использования принтеров в сети. Когда доступ к одним и тем же принтерам нужен множеству пользователей, в домене необходимо настроить серверы печати. В более ранних выпусках операционной системы Windows Server все серверы устанавливались вместе с основными службами печати. В Windows Server 2012 R2 необходимо настроить сервер должным образом, чтобы превратить его в сервер печати.

Использование устройств печати

В сети используются два типа устройств печати:

- *локальное устройство печати* — устройство печати, физически подключенное к компьютеру пользователя и используемое только пользователями, которые зарегистрировались на этом компьютере;
- *сетевое устройство печати* — устройство печати, настроенное для удаленного доступа по сети. Оно может быть подключено к серверу печати или непосредственно к сети через сетевой адаптер (NIC, Network Interface Card).

Примечание

Ключевая разница между локальным и сетевым принтерами в том, что локальный принтер не используется совместно. Можно очень просто превратить локальный принтер в сетевой. О том, как это сделать, будет рассказано в *разд. "Предоставление общего доступа к принтеру" далее в этой главе*.

Сетевой принтер подключается либо к серверу печати, либо непосредственно к сети, если у принтера есть такая возможность. *Сервер печати* (print server) — это рабочая станция или сервер, настроенные для совместного использования одного или нескольких принтеров. Эти принтеры могут быть физически подключены к компьютеру или непосредственно к сети. Недостаток сервера печати на базе операционной системы рабочей станции заключается в ограничении числа одновременных соединений. Используя ОС Windows Server 2012 R2, практически можно не волноваться о превышении такого предела.

Любую систему, работающую под управлением ОС Windows Server 2012 R2, можно настроить в качестве сервера печати. Основная задача сервера печати — предоставлять общий доступ к устройствам печати по сети и управлять спулом печати. Основное преимущество серверов печати заключается в том, что у принтеров есть централизованно управляемая очередь печати и администратору не нужно устанавливать драйверы принтера на всех клиентских системах.

Однако следует отметить, что не обязательно использовать сервер печати. Можно подключать пользователей непосредственно к присоединенному к сети принтеру. Если сделать это, сетевой принтер будет управляться, как локальный принтер, непосредственно подсоединенный к компьютеру пользователя. Ключевая разница в том, что к принтеру могут подключаться несколько пользователей и у каждого из них будет разная очередь печати. Каждая отдельная очередь печати управляется независимо от других очередей, что усложняет администрирование и разрешение проблем.

Основы печати

Понимание того, как работает печать, может иметь большое значение при диагностике проблем печати. Когда распечатываются документы, взаимодействует много процессов, драйверов и устройств. Если используется принтер, подключенный к серверу печати, основные операции следующие.

- **Драйвер принтера.** Когда в приложении распечатывается документ, компьютер использует драйвер принтера для обработки процесса печати. Если устройство печати присоединено физически к компьютеру, драйвер принтера находится на локальном жестком диске компьютера. Если устройство печати находится на удаленном компьютере, драйвер принтера может быть загружен с удаленного компьютера. Доступность драйверов принтера на удаленном компьютере конфигурируется операционной системой и архитектурой чипа. Если компьютер не может получить последний драйвер принтера, администратор, вероятно, не включил драйвер для операционной системы компьютера. Для получения дополнительной информации обратитесь к *разд. "Управление драйверами принтера" далее в этой главе*.
- **Локальный диспетчер печати и процессор печати.** Приложение, в котором производится печать, использует драйвер принтера, чтобы перевести документ в фор-

мат файла, понятный выбранному устройству печати. После этого компьютер передает документ локальному диспетчеру печати (print spooler). Локальный диспетчер печати поочередно передает документ процессору печати, который создает необработанные (raw) данные печати, необходимые для печати на принтере.

- **Маршрутизатор печати и диспетчер печати на сервер печати.** Необработанные данные передаются обратно локальному диспетчеру печати. Если производится печать на удаленном принтере, необработанные данные передаются к диспетчеру печати, находящемуся на сервере печати. В системах на базе Windows Server 2012 R2 маршрутизатор печати (Winspool.drv) обрабатывает задачи определения местоположения удаленного принтера, задачи маршрутизации заданий печати и управляет загрузкой драйверов принтера на локальную систему при необходимости. Если происходит сбой какой-то из этих задач, виноват маршрутизатор печати. Дополнительная информация представлена в *разд. "Решение проблем с очередью печати"* и *"Установка разрешений принтера" далее в этой главе*. Если данные процедуры не работают, можно заменить или восстановить Winspool.drv.

  Основная причина загрузки драйверов принтеров на клиентские компьютеры заключается в поддержке единственного расположения для установки обновлений драйверов. Вместо того чтобы установить новый драйвер на всех клиентских системах, можно установить его один раз на сервере печати и разрешить клиентам загружать новый драйвер. Дополнительная информация приведена в *разд. "Управление драйверами принтера" далее в этой главе*.

- **Принтер (очередь печати).** Документ из диспетчера печати отправляется в стек принтера, который в некоторых операционных системах называется *очередью печати* — для выбранного устройства печати. Когда документ находится в очереди, он называется *заданием печати* — задача, которую должен обработать диспетчер печати. Сколько времени документ проведет в стеке принтера, зависит от его приоритета и позиции в стеке. Дополнительная информация будет приведена в *разд. "Планирование и приоритезация заданий печати" далее в этой главе*.

- **Монитор печати.** Когда документ достигает вершины стека принтера, монитор печати отправляет документ устройству печати, которое фактически выполняет его печать. Если принтер настроен на уведомление пользователя о завершении печати, пользователь получит сообщение. Какой именно монитор печати будет использоваться операционной системой Windows Server 2012 R2, зависит от конфигурации устройства печати и от его типа. Также могут быть мониторы печати, предоставляемые производителем устройства печати. Как правило, монитор печати представляет собой динамическую библиотеку (DLL). Если она повреждена, ее нужно переустановить.

- **Устройство печати** — это физическое устройство, выполняющее печать документов на бумаге. Типичные проблемы и ошибки устройств печати — **Вставьте бумагу в лоток X** (Insert Paper Into Tray X), **Низкий уровень тонера** (Low Toner), **Закончилась бумага** (Out of Paper), **Закончился тонер** (Out Of Toner) или **Закончились чернила** (Out Of Ink), **Замятие бумаги** (Paper Jam), **Принтер оффлайн** (Printer Offline).

На возможность установки и управления принтерами может влиять групповая политика. Если есть проблемы, связанные с групповой политикой, нужно исследовать ключевые политики, находящиеся в следующих расположениях:

- **Конфигурация компьютера\Административные шаблоны\Принтеры** (Computer Configuration\Administrative Templates\Printers);
- **Конфигурация пользователя\ Административные шаблоны\ Панель управления\ Принтеры** (User Configuration\Administrative Templates\Control Panel\Printers);
- **Конфигурация пользователя\Административные шаблоны\Меню "Пуск" и панель задач** (User Configuration\Administrative Templates\Start Menu And Taskbar).

> ***Практический совет***
>
> ОС Windows Server 2012 R2 — 64-разрядная операционная система, и очередь печати, работающая на этой операционной системе, не может функционировать без собственного 64-разрядного драйвера принтера. Поэтому нужно проверить доступность требуемых 64-разрядных драйверов печати, если будете выполнять миграцию с серверов печати, работающих под управлением 32-разрядных операционных систем, на Windows Server 2012 R2. Следует иметь в виду, что если в организации все еще используются старые принтеры, у них могут быть сторонние 32-разрядные драйверы и может вообще не быть 64-разрядных эквивалентов.

Настройка серверов печати

Для настройки сервера как сервера печати нужно добавить роль **Службы печати и документов** (Print and Document Services) и настроить эту роль для использования одной или нескольких следующих служб роли:

- **Сервер печати** (Print Server) — настраивает сервер для работы в качестве сервера печати и устанавливает консоль **Управление печатью** (Print Management), позволяющую управлять несколькими принтерами и серверами печати, выполнять миграцию принтеров с других серверов печати (и на другие серверы печати), а также управлять заданиями печати.
- **Служба LPD** (Line Printer Daemon (LPD) Service) — позволяет UNIX-совместимым компьютерам, имеющим службу LPR (Line Printer Remote), использовать разделяемые принтеры на сервере.
- **Печать через Интернет** (Internet Printing) — создает веб-сайт, где авторизованные пользователи могут управлять заданиями печати сервера. Также позволяет пользователям, у которых установлен клиент печати через Интернет (Internet Printing Client), подключаться к совместно используемым принтерам на сервере посредством протокола межсетевой печати (IEE, Internet Printing Protocol). Адрес по умолчанию для IPP — **http://Имя_сервера/Printers**, например **http://PrintServer15/Printers** или **http://www.cpandl.com/Printers**.
- **Сервер распределенного сканирования** (Distributed Scan Server) — настраивает сервер для работы в качестве сервера сканирования, позволяющего запустить процессы сканирования. Процессы сканирования — это правила, определяющие настройки сканирования и контролирующие отправку сканированных документов по сети. При установке этой службы роли устанавливается оснастка **Управление ска-**

нированием (Scan Management), позволяющая вам управлять WSD[1]-совместимыми сканерами, серверами сканирования и процессами сканирования.

Добавить роль **Службы печати и документов** можно так:

1. В консоли **Диспетчер серверов** в меню **Управление** выберите команду **Добавить роли и компоненты** (Add Roles And Features). Будет запущен мастер добавления ролей и компонентов. Если мастер отобразит страницу **Перед началом работы** (Before You Begin), прочитайте вступительный текст и затем нажмите кнопку **Далее**.
2. На странице **Выбор типа установки** (Installation Type) по умолчанию отмечен переключатель **Установка ролей или компонентов** (Role-Based Or Feature-Based Installation). Нажмите кнопку **Далее**.
3. На странице **Выбор целевого сервера** (Server Selection) можно указать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите сервер из пула серверов либо сервер, на котором можно смонтировать виртуальный жесткий диск (VHD). При добавлении ролей и компонентов на VHD нажмите кнопку **Обзор** (Browse), а затем используйте окно **Обзор виртуальных жестких дисков** (Browse For Virtual Hard Disks) для выбора вашего VHD. Когда будете готовы продолжить, нажмите кнопку **Далее**.
4. На странице **Выбор ролей сервера** (Server Roles) выберите роль **Службы печати и документов** и нажмите кнопку **Далее** трижды.
5. На странице **Выбор служб ролей** выберите одну или более службу роли. Например, чтобы разрешить функциональную совместимость с UNIX, выберите службу роли **Служба LPD**. Нажмите кнопку **Далее**.
6. При установке службы роли **Печать через Интернет** также необходимо установить **Веб-сервер (IIS)**. Будет отображено соответствующее диалоговое окно. Нажмите кнопку **Добавить компоненты** для закрытия этого окна и установки требуемых компонентов на сервер. По окончанию выбора компонентов нажмите кнопку **Далее**.

   Примечание

   Если сервер, на котором необходимо установить роль **Службы печати и документов**, не обладает всеми необходимыми двоичными файлами, сервер получит их через Центр обновления Windows (по умолчанию) или из местоположения, указанного групповой политикой. Можно также указать альтернативный источник для файлов. Для этого щелкните по ссылке **Указать альтернативный исходный путь** (Specify An Alternate Source Path), в появившемся окне укажите альтернативный путь и нажмите кнопку **OK**. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer2012\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2-12\install.wim:4.

7. После просмотра параметров установки и их сохранения нажмите кнопку **Установить** (Install) для начала процесса установки. Страница **Ход установки** (Installation Progress) позволяет отслеживать процесс инсталляции. Если мастер бы закрыт, нажмите значок **Уведомления** (Notifications) в диспетчере серверов, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.

[1] Web Services on Devices.

8. Когда роль **Службы печати и документов** будет установлена, страница **Ход установки** будет обновлена, чтобы отразить этот факт. Просмотрите подробности установки и убедитесь, что все фазы инсталляции завершены успешно.
9. При установке сервера распределенного сканирования будет отображено уведомление о том, что необходима дополнительная настройка. Щелкните по предоставленной ссылке, чтобы открылась оснастка **Управление сканированием**, разверните узел **Управление сканированием** (Scan Management), затем щелкните правой кнопкой мыши на узле **Управляемые сканеры** (Managed Scanners) и выберите команду **Управление** (Manage), чтобы открыть диалоговое окно **Добавление или удаление сканеров** (Add Or Remove Scanners). Используя это окно для идентификации распределенных сканеров на предприятии.

При установке службы роли **Сервер распределенного сканирования** группа безопасности **Операторы сканирования** (Scan Operators) будет добавлена в контейнер **Пользователи** (Users) в AD DS для текущего домена входа. Все пользователи, которые будут заниматься управлением службой распределенного сканирования, должны быть добавлены в эту группу.

> ***Практический совет***
>
> Есть несколько способов добавить необходимые двоичные файлы. В командной строке можно ввести команду `DISM /Online /Enable-Feature /FeatureName:PrintServer /All /LimitAccess /Source:E:\Sources\SxS`, где E: — смонтированный образ ISO или DVD-диск. Также в приглашении Windows PowerShell можно ввести команду `Enable-WindowsOptionalFeature -Online -FeatureName "PrintServer" -All -LimitAccess Source "E:\Sources\SxS"`, где E: — смонтированный ISO-образ или DVD.

Включение и отключение общего доступа к файлам и принтерам

Настройки общего доступа к файлам и принтерам управляют доступом к общим файлам и принтерам, подключенным к компьютеру. Управлять конфигурацией общего доступа к файлам и принтерам можно так:

1. В Проводнике выберите **Сеть** (Network) на левой панели. На панели инструментов Проводника выберите вкладку **Сеть**, а затем нажмите кнопку **Управление сетями и общим доступом** (Network And Sharing Center).
2. В окне **Центр управления сетями и общим доступом** (Network and Sharing Center) щелкните по ссылке **Изменить дополнительные параметры общего доступа** (Change Advanced Sharing Settings) на панели слева. Выберите профиль сети, для которой нужно изменить параметры общего доступа к файлам и принтерам. Обычно это профиль **Доменный** (Domain).
3. Установите параметры общего доступа к файлам и принтерам:
   - если нужно включить общий доступ к файлам и принтерам, отметьте переключатель **Включить общий доступ к файлам и принтерам**;
   - если нужно выключить общий доступ, отметьте переключатель **Выключить общий доступ к файлам и принтерам**.

Начало работы с оснасткой *Управление печатью*

Оснастка **Управление печатью** (Print Management) является основным инструментом для работы с принтерами и серверами печати. После установки роли **Службы печати и документов** эта оснастка будет доступна в меню **Средства** диспетчера серверов. Также можно добавить эту оснастку к любой пользовательской консоли управления, созданной администратором.

Используя управление печатью (рис. 10.1), можно установить новые принтеры, а также просмотреть и настроить уже установленные. Кроме того, данная оснастка используется для управления Windows-серверами печати. Также оснастка **Управление печатью** позволяет просмотреть состояние принтеров и серверов печати. Если развернуть узел уровня сервера и выбрать подузел **Принтеры** (Printers), будет отображен список принтеров, размещенных на этом сервере. Если доступ к серверу печати осуществляется с использованием удаленного рабочего стола (Remote Desktop), также в этом списке будут компьютеры, подключенные к локальному компьютеру, с которого осуществляется доступ к серверу печати. Перенаправляемые принтеры отмечаются соответствующим суффиксом.

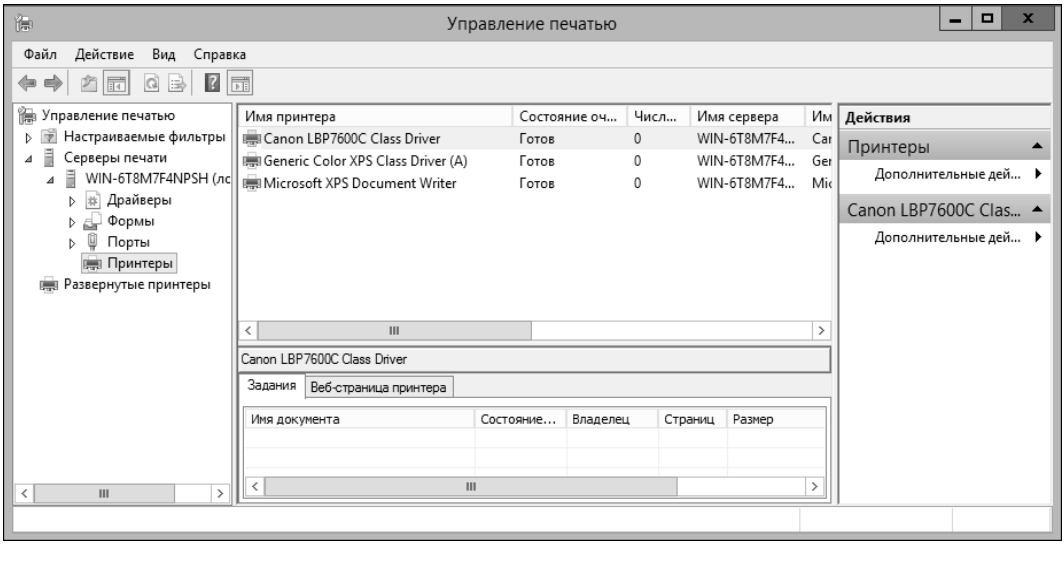


Рис. 10.1. Использование **Управления печатью** для работы с серверами печати и принтерами всего предприятия

По умолчанию оснастка **Управление печатью** позволяет управлять локальными серверами печати. Администратор может управлять и контролировать другие серверы печати в организации, добавляя их в консоль. Кроме того, для управления удаленным сервером печати пользователь должен быть членом локальной группы **Администраторы** на сервере печати или членом группы **Администраторы домена** для домена, в состав которого входит управляемый сервер.

При выборе узла **Принтеры** для некоторого сервера печати оснастка отображает основную панель, на которой содержатся сведения об имени принтера, состоянии очереди, числе заданий в очереди и имени сервера, на котором размещен принтер. Можно щелкнуть правой кнопкой по узлу **Принтеры** и выбрать команду **Показать расширенное представление** (Show Extended View). Этим действием включается расширенное представление, упрощающее отслеживать состояние как принтеров, так и заданий печати. Расширенное представление содержит информацию о состоянии задания печати, имя его владельца, число страниц, размер задания, дату и время постановки задания, порт и приоритет задания.

Кроме того, если у принтера есть веб-страница, расширенное представление позволяет отобразить ее, если щелкнуть по вкладке **Веб-страница принтера** (Printer Web Page). Веб-страница предоставляет подробности о состоянии принтера, его физических свойствах и его конфигурации, а также иногда позволяет удаленное администрирование.

Добавить серверы печати в оснастке **Управление печатью** можно так:

1. В оснастке **Управление печатью** щелкните правой кнопкой мыши по узлу **Серверы печати** (Print Servers) на левой панели и затем выберите команду **Добавление или удаление серверов** (Add/Remove Servers).
2. В окне **Добавление и удаление серверов** (рис. 10.2) будет отображен список уже добавленных серверов печати. Выполните одно из следующих действий и нажмите кнопку **Добавить к списку** (Add To List):
   - введите или вставьте имена серверов печати в список **Добавить серверы**. Используйте запятые для разделения имен компьютеров;

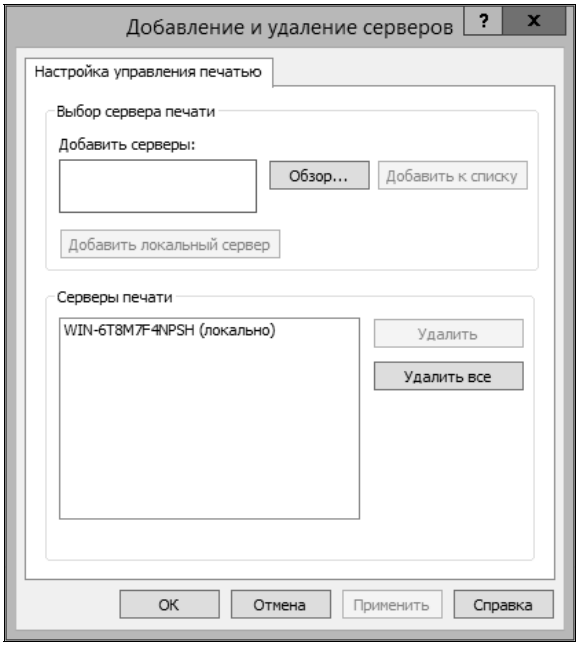


Рис. 10.2. Добавление сервера печати позволяет управлять сервером и контролировать его

- нажмите кнопку **Обзор** для отображения окна **Выбор сервера печати** (Select Print Server). Выберите сервер, который нужно добавить, и нажмите кнопку **Выбрать сервер** (Select Server).

3. Повторите предыдущий шаг при необходимости и нажмите кнопку **OK**.

Удалить сервер печати из оснастки **Управление печатью** можно так:

1. В оснастке **Управление печатью** щелкните правой кнопкой мыши по узлу **Серверы печати** на левой панели и затем выберите команду **Добавление или удаление серверов**.
2. В окне **Добавление или удаление серверов** будет отображен список уже добавленных серверов печати. Выберите один или более серверов из списка **Серверы печати** и нажмите кнопку **Удалить**.

Установка принтеров

В следующих разделах представлены методы установки принтеров. ОС Windows Server 2012 R2 делает все возможное, чтобы администратор мог установить и управлять принтерами из любой точки сети. Для установки или настройки нового принтера на Windows Server 2012 R2 пользователь должен быть членом группы **Администраторы**, **Операторы печати** или **Операторы сервера**. Для подключения к принтеру и печати документов у пользователя должны быть соответствующие разрешения доступа. Подробно о них мы поговорим в *разд. "Установка разрешений принтера" далее в этой главе*.

Использование функции автоматической установки принтера

Оснастка **Управление печатью** может автоматически определить все сетевые принтеры, размещенные в той же подсети, что и компьютер, с которого запущена консоль управления. После определения принтера оснастка может автоматически установить надлежащие драйверы принтера, настроить очереди печати и предоставить общий доступ к принтерам. Для автоматической установки сетевых принтеров и настройки сервера печати выполните следующие действия:

1. Запустите оснастку **Управление печатью**, выбрав соответствующую команду в меню **Средства** (Tools) диспетчера серверов.
2. В оснастке **Управление печатью** разверните узел **Серверы печати**, дважды щелкнув на нем.
3. Щелкните правой кнопкой мыши на записи локального или удаленного сервера, с которым нужно работать, а затем выберите команду **Добавить принтер** (Add Printer), чтобы открыть окно мастера установки сетевого принтера (Network Printer Installation Wizard).
4. На странице **Установка принтера** (Printer Installation) выберите переключатель **Выполнить поиск принтеров в сети** (Search The Network For Printers) и нажмите кнопку **Далее**.

5. Мастер выполнит поиск сетевых принтеров в локальной подсети. Если принтеры будут найдены, мастер отобразит список имен принтеров и их IP-адресов (рис. 10.3). Выберите принтер, который нужно установить, и нажмите кнопку **Далее**, а затем повторите эту процедуру для установки автоматически обнаруженного принтера. Если принтер, который нужно установить, не приведен в этом списке, убедитесь, что он включен и находится онлайн, а затем повторите эту процедуру. Если принтер включен, находится онлайн, но все равно не отображается, обратитесь к *разд. "Установка присоединенных к сети устройств печати" далее в этой главе* для завершения установки.

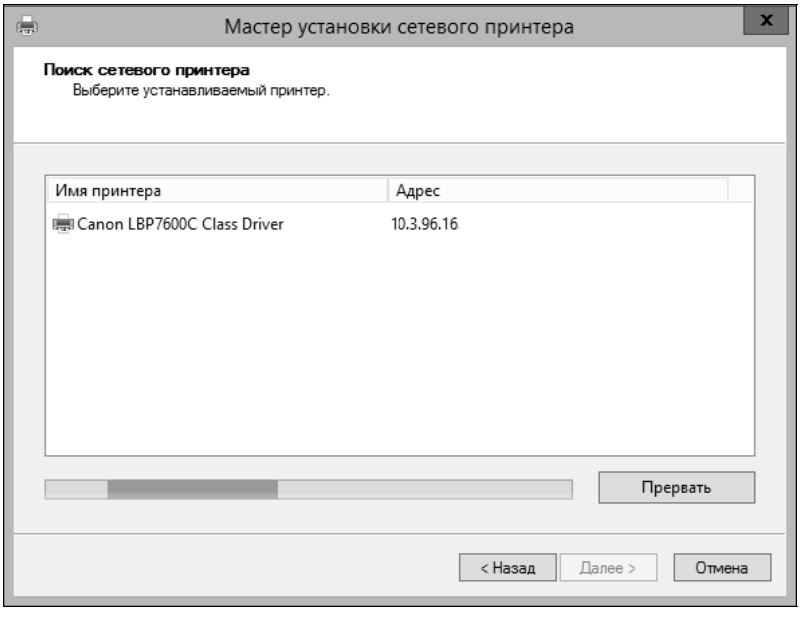


Рис. 10.3. Мастер выводит имена и IP-адреса обнаруженных принтеров

6. Мастер автоматически обнаружит конфигурацию TCP/IP-порта выбранного принтера и запросит всю необходимую конфигурационную информацию у принтера. После этого мастер установит имя по умолчанию и имя общего ресурса (рис. 10.4). По умолчанию принтер настраивается как общий ресурс. Имя принтера — это имя, которое используется для работы с принтером в оснастке **Управление принтером**. Имя общего ресурса — это то имя, которое увидят пользователи, когда будут работать с принтером. При желании можно заполнить поля **Размещение** и **Комментарий**, что поможет пользователям идентифицировать ваш принтер. Например, можно указать размещение принтера "Кабинет 314, здание 7".

Примечание

Имя принтера и имя общего ресурса не должны превышать 256 символов и могут содержать пробелы. В больших организациях имя общего ресурса должно быть логичным, поскольку именно оно помогает быстро обнаружить принтер. Например, можно указать имя общего ресурса "Canon на 3-м этаже (комната 314)", что означает, что принтер находится на третьем этаже, в комнате 314 и называется Canon.

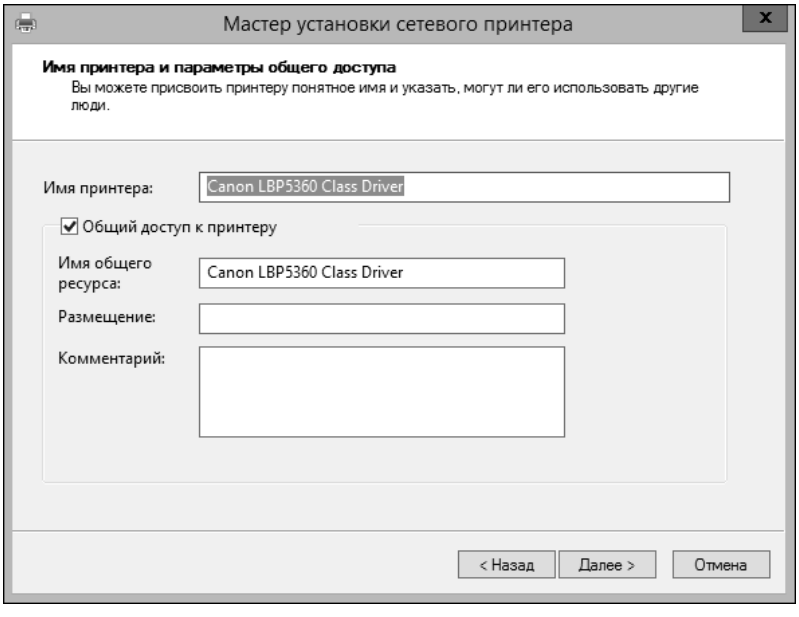


Рис. 10.4. Установите имя принтера и имя общего ресурса

7. На следующей странице можно будет проверить настройки. Если готовы продолжить, нажмите кнопку **Далее**.
8. При предоставлении общего доступа к принтеру Windows Server автоматически делает доступными драйверы, чтобы пользователи могли загрузить их при первом подключении к принтеру. Страница состояния должна подтвердить, что установка принтера и его драйвера прошла успешно. Если возникли проблемы с установкой, обратите внимание на предоставленные ошибки. Например, кто-то может выключить принтер, пока происходит попытка его настройки. Если это так, то нужно заново включить принтер и повторить эту процедуру.
9. При желании можно распечатать тестовую страницу, для этого отметьте флажок **Напечатать пробную страницу** и затем нажмите кнопку **Готово**. В противном случае просто нажмите кнопку **Готово**.
10. По умолчанию общий ресурс принтера не перечислен в Active Directory. Перечисление общего ресурса принтера в Active Directory существенно упрощает поиск принтера пользователями. Если необходимо добавить общий ресурс принтера в Active Directory, выберите узел **Принтеры** на панели слева, щелкните по записи принтера в главном окне и выберите команду **Перечислить в Active Directory**.
11. По умолчанию задания печати отправляются на сервер печати, где они прорисовываются и отправляются на принтер. Это поведение можно изменить, используя прямую печать в филиалах (Branch Office Direct Printing). Когда используется прямая печать в филиалах, задания печати прорисовываются на клиентских компьютерах, а затем отправляются непосредственно принтеру. Если нужно включить прямую печать в филиалах, выберите узел **Принтеры** на панели слева, щелкните правой кнопкой мыши по принтеру и выберите команду **Включить прямую печать в филиалах** (Enable Branch Office Direct Printing).

Установка и настройка физически подключенных устройств печати

Большинство физически подключаемых устройств печати подключаются к компьютеру посредством USB-кабеля. Физически подключенные принтеры можно настроить как локальные устройства печати или как сетевые устройства печати. Ключевая разница в том, что локальные устройства доступны только пользователям, зарегистрированным на компьютере, а сетевые устройства доступны всем пользователям сети как общие устройства печати. Помните, что рабочая станция или сервер становятся сервером печати для настраиваемого устройства. Если компьютер выключен или находится в состоянии сна, принтер не будет доступен.

Чтобы установить физически подключенное устройство, нужно зайти на его сервер печати либо локально, либо удаленно — через удаленный рабочий стол. Установка локального PnP-принтера (когда администратор зарегистрировался на сервере печати и имеет физический доступ к принтеру) совсем проста. После установки принтера необходимо настроить его для использования.

Установить и настроить устройство печати можно с помощью следующих действий:

1. Включите принтер и подключите его к серверу, используя соответствующий кабель.
2. Если ОС Windows Server автоматически определила устройство печати, начнется установка устройства и необходимых драйверов. Если драйверы не найдены, следует вставить диск к принтеру в дисковод CD/DVD.
3. Если Windows Server не определил принтер автоматически, необходимо произвести установку устройства вручную, как описано в следующем наборе инструкций.
4. После установки принтера его нужно настроить. В оснастке **Управление печатью** разверните узел **Серверы печати** (Print Servers) и узел сервера, с которым нужно работать. Далее выберите узел **Принтеры** (Printers) для сервера, который вы настраиваете, и увидите список доступных принтеров в основной части окна оснастки. Щелкните правой кнопкой мыши на принтере, который нужно настроить, и выберите команду **Управление общим доступом**. Откроется окно **Свойства** с выбранной вкладкой **Доступ** (рис. 10.5).
5. Если включить флажок **Общий доступ к данному принтеру**, Windows Server установит параметр **Имя общего ресурса** равным имени принтера. При необходимости можно ввести другое имя в это поле.
6. По умолчанию включен флажок **Прорисовка заданий печати на клиентских компьютерах** (Render print jobs on client computers), что настраивает принтер для прямой печати в филиалах (Branch Office Direct Printing). Когда включена прямая печать в филиалах, задания печати передаются непосредственно на сервер печати для их прорисовки, а затем отправляются на принтер. Сбросьте флажок **Прорисовка заданий печати на клиентских компьютерах**.
7. Внесение общего ресурса принтера в Active Directory существенно упрощает поиск принтера пользователями. Если нужно, чтобы общий ресурс принтера был внесен в Active Directory, включите флажок **Внести в Active Directory**.
8. Нажмите кнопку **OK**.

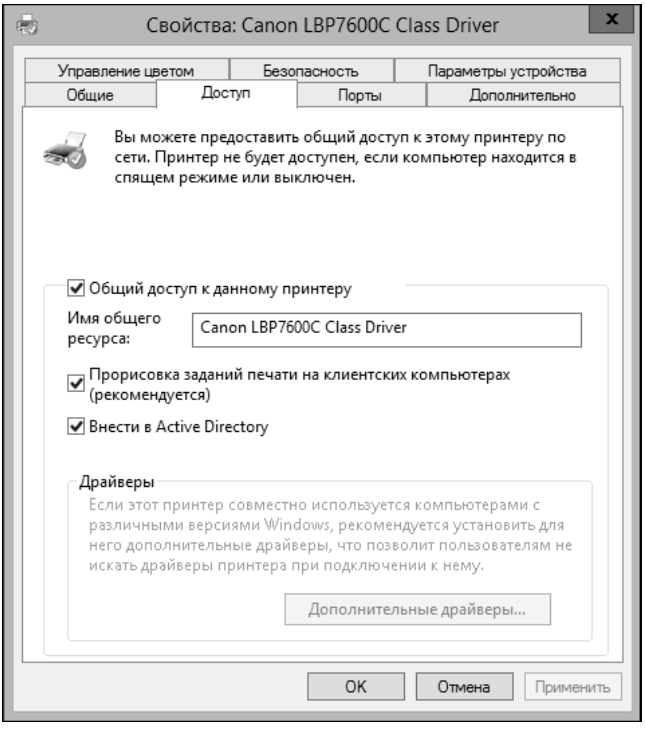


Рис. 10.5. Настройте принтер, используя диалог **Свойства**

Иногда Windows Server не обнаруживает принтер. В этом случае для установки устройств печати нужно выполнить следующие действия:

1. В оснастке **Управление печатью** разверните узел **Серверы печати** и узел сервера, с которым нужно работать.
2. Щелкните правой кнопкой мыши на узле **Принтеры** и выберите команду **Добавить принтер**. Откроется окно **Мастер установки сетевого принтера** (Network Printer Installation Wizard).
3. На странице **Установка принтера** (Printer Installation), показанной на рис. 10.6, отметьте переключатель **Добавить новый принтер, используя существующий порт**, а затем выберите LPT-, COM- или USB-порт. Также можно выбрать печать в файл. В этом случае Windows Server 2012 R2 попросит пользователей ввести имя файла, в который осуществляется печать. Нажмите кнопку **Далее**.
4. На странице **Драйвер принтера** (Printer Driver) выберите один из следующих вариантов (рис. 10.7).
   - Если Windows определила тип принтера по выбранному порту и автоматически нашла совместимый данный, она сообщит производителя принтера и его модель в поле, которое находится под опцией **Использовать драйвер принтера**, **выбранный мастером установки** (Use the printer driver that the wizard selected). Эта опция будет выбрана по умолчанию (если Windows определила принтер). Чтобы принять эти настройки, нажмите кнопку **Далее**.

- Если совместимый драйвер не доступен, вам нужно выбрать один из уже установленных на этом компьютере драйверов. Выберите опцию **Использовать имеющийся на этом компьютере драйвер** (Use an existing driver on the computer). Затем выберите драйвер из списка под этой опцией и нажмите кнопку **Далее**.

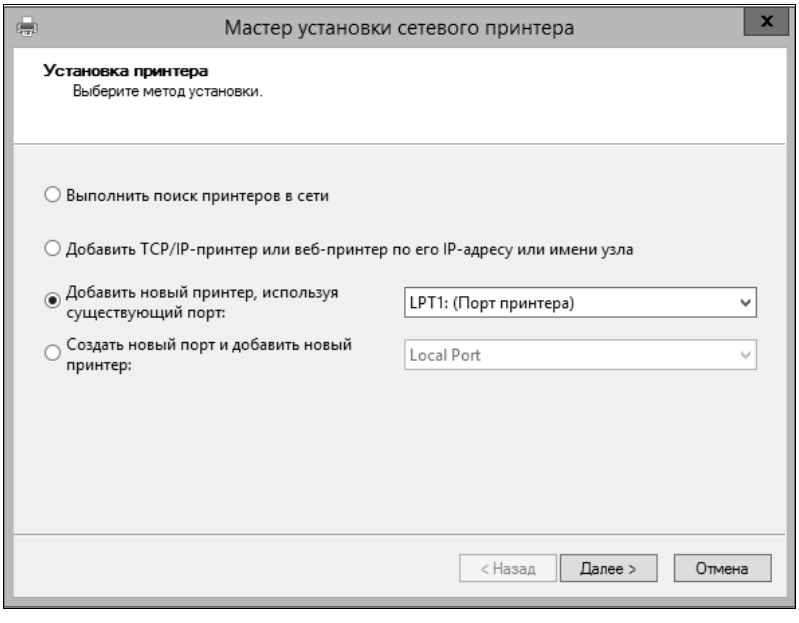


Рис. 10.6. Выберите существующий порт

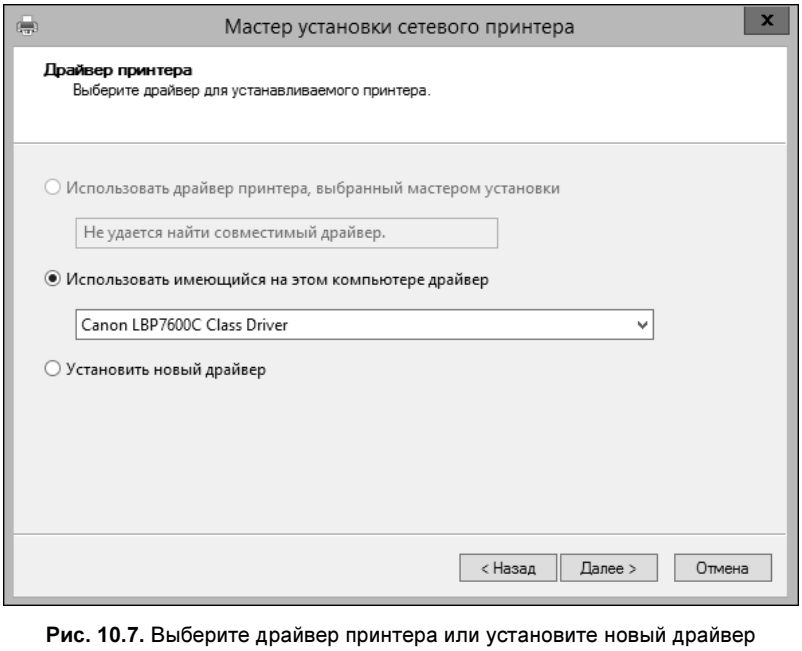


Рис. 10.7. Выберите драйвер принтера или установите новый драйвер

- Если для принтера доступно несколько драйверов, например драйверы PCL и PostScript, выберите предпочитаемый драйвер из списка под опцией **Использовать имеющийся на этом компьютере драйвер**. После выбора надлежащего драйвера нажмите кнопку **OK**.
- Если совместимый драйвер недоступен и необходимо установить новый драйвер, выберите опцию **Установить новый драйвер** (Install a new driver) и нажмите кнопку **Далее**. Далее нужно указать производителя и модель принтера. В результате Windows Server 2012 R2 назначит драйвер принтера устройству печати. После выбора производителя принтера укажите его модель.

Практический совет

Если нужный производитель и/или нужная модель принтера не отображаются в списке, нажмите кнопку **Центр обновления Windows**. Windows подключится к сайту Windows Update для обновления списка принтеров и затем покажет дополнительные модели. Данный процесс занимает всего несколько минут. Когда этот процесс будет завершен, появится возможность выбрать производителя и модель принтера. Если опять в списке нет нужного производителя или нужной модели, загрузите драйвер принтера с сайта производителя и распакуйте файлы драйвера. Нажмите кнопку **Установить с диска** (Have Disk). В окне **Установка с диска** (Install From Disk) нажмите кнопку **Обзор** (Browse). В окне **Поиск файла** (Locate File) выберите inf-файл драйвера принтера и нажмите кнопку **Открыть** (Open).

Примечание

Если драйвер для используемой модели принтера недоступен, можно выбрать универсальный драйвер для подобного класса устройств печати. Обратитесь к документации принтера для получения дополнительной информации.

5. Присвойте имя принтеру. Имя будет отображаться в оснастке **Управление печатью**.
6. Укажите, должен ли принтер быть доступным для удаленных пользователей. Если должен, установите флажок **Общий доступ к принтеру** (Share This Printer) и введите имя общего ресурса. В больших организациях имя должно помочь обнаружить принтер. Например, "Этаж 3, комната 314" означает, что принтер находится в комнате 314 на третьем этаже.
7. При желании заполните поля **Размещение** (Location) и **Комментарий** (Comment). Эта информация также поможет пользователям определить размещение принтера и его возможности. Нажмите кнопку **Далее**.
8. Последняя страница позволит проверить параметры. Если готовы продолжить установку, нажмите кнопку **Далее**.
9. После установки драйвера принтера и его настройки будет отображена страница состояния. Убедитесь, что установка драйвера и принтера прошла успешно. Если есть ошибки, нужно устранить их и повторить этот процесс. Для проверки принтера включите флажок **Напечатать пробную страницу** (Print test page) и нажмите кнопку **Готово**.

Когда мастер установки сетевого принтера завершит установку нового принтера, в папке Принтеры появится только что установленный принтер с указанным при установке именем. Можно изменить свойства принтера и проверить его состояние в любое

время, но об этом мы поговорим в *разд. "Настройка свойств принтера" далее в этой главе*.

> ***Совет***
>
> Если повторить этот процесс, можно создать дополнительные принтеры для одного и того же устройства печати. Все, что для этого нужно — указать другое имя принтера и другое имя общего ресурса. В результате можно указать различные настройки для разных принтеров, но физическое устройство печати будет одно. Например, можно создать высокоприоритетный принтер для заданий печати, которые должны быть выполнены в первую очередь, и низкоприоритетный принтер для несрочных заданий.

Установка присоединенных к сети устройств печати

Присоединенное к сети устройство печати — это устройство печати, подключенное непосредственно к сети через встроенный сетевой или беспроводной адаптер. Такие устройства настраиваются как сетевые устройства печати, поэтому они доступны сетевым пользователям как общие устройства печати. Помните, что сервер, на котором будет настроено устройство печати, становится сервером печати для этого устройства.

Установить присоединенное к сети устройство печати можно с помощью следующих действий:

1. В оснастке **Управление печатью** разверните узел **Серверы печати** и узел для сервера, с которым нужно работать.
2. Щелкните правой кнопкой мыши по узлу **Принтеры** и затем выберите команду **Добавить принтер**.
3. На странице **Установка принтера** выберите переключатель **Добавить TCP/IP принтер или веб-принтер по его IP-адресу или имени узла** (Add a TCP/IP or web services printer by IP address or hostname), а затем нажмите кнопку **Далее**.
4. На странице **Адрес принтера** (Printer Address) выберите один из вариантов в списке **Тип устройства** (Type of device):
   - **Автообнаружение** (Autodetect) — выберите этот вариант, если не уверены, какой тип устройства нужно выбрать. Windows Server попытается автоматически обнаружить тип устройства;
   - **Устройство TCP/IP** (TCP/IP Device) — выберите этот тип, если уверены, что устройство является TCP/IP-устройством;
   - **Принтер веб-служб** (Web Services Printer) — выберите этот вариант, если уверены, что принтер является WSD-совместимым принтером;
   - **Безопасный принтер веб-служб** (Web Services Secure Printer) — выберите этот вариант, если уверены, что принтер поддерживает безопасную WSD-печать.

> ***Практический совет***
>
> При использовании безопасных WSD-принтеров серверы печати создают приватный безопасный канал к сетевому устройству по сети без необходимости применения дополнительных технологий безопасности вроде IPSec. Однако пользователи и компьютеры, работающие с безопасным принтером, должны быть членами домена Active Directory. Для управления разрешениями доступа к принтеру используются настройки домена, а AD DS действует как доверительный арбитр между сервером печати и принтером.

5. Введите имя узла или IP-адрес принтера, например 192.168.1.90. При использовании автоопределения или устройства TCP/IP мастер автоматически установит имя порта в то же значение (значение адреса принтера), но можно указать другое значение.

   Совет

   Имя порта не имеет значения, пока оно уникально на сервере. Если настраиваете несколько принтеров на сервер печати, убедитесь, что записали сопоставление "порт — принтер".

6. По умолчанию включен флажок **Автоматический поиск драйвера принтера** (Auto detect the printer driver to use). Когда будет нажата кнопка **Далее**, мастер попытается связаться с принтером и автоматически настроит устройство печати. Если мастер не может определить устройство печати, убедитесь, что все следующее истинно:
   - выбран правильный тип устройства печати;
   - устройство печати включено и подключено к сети;
   - принтер правильно настроен;
   - введены правильный IP-адрес или имя принтера.
7. Если неправильно установлен тип устройства, IP-адрес или имя принтера, нажмите кнопку **OK**, чтобы закрыть диалог предупреждения. Далее нажмите кнопку **Назад** и повторите ввод данных о принтере.
8. На странице **Драйвер принтера** выберите один из следующих вариантов.
   - Если Windows определила тип принтера по выбранному порту и автоматически нашла совместимый данный, она сообщит производителя принтера и его модель в поле, которое находится под опцией **Использовать драйвер принтера**, **выбранный мастером установки** (Use the printer driver that the wizard selected). Эта опция будет выбрана по умолчанию (если Windows определила принтера). Чтобы принять эти настройки, нажмите кнопку **Далее**.
   - Если совместимый драйвер не доступен, вам нужно выбрать один из уже установленных на этом компьютере драйверов. Выберите опцию **Использовать имеющийся на этом компьютере драйвер** (Use an existing driver). Затем выберите драйвер из списка под этой опцией и нажмите кнопку **Далее**.
   - Если совместимый драйвер недоступен и необходимо установить новый драйвер, выберите опцию **Установить новый драйвер** (Install a new driver) и нажмите кнопку **Далее**. Далее нужно указать производителя и модель принтера. В результате ОС Windows Server 2012 R2 назначит драйвер принтера устройству печати. После выбора производителя принтера укажите его модель.

     Практический совет

     Если нужный производитель и/или нужная модель принтера не отображаются в списке, нажмите кнопку **Центр обновления Windows**. Windows подключится к сайту Windows Update для обновления списка принтеров и затем покажет дополнительные модели. Данный процесс занимает всего несколько минут. Когда этот процесс будет завершен, появится возможность выбрать производителя и модель принтера. Если опять в списке нет нужного производителя или нужной модели, загрузите драйвер принтера с сайта производителя и

распакуйте файлы драйвера. Нажмите кнопку **Установить с диска**. В окне **Установка с диска** нажмите кнопку **Обзор**. В окне **Поиск файла** выберите inf-файл драйвера принтера и нажмите кнопку **Открыть**.

9. Присвойте имя принтеру. Имя будет отображаться в оснастке **Управление печатью**.
10. Укажите, должен ли принтер быть доступным для удаленных пользователей. Чтобы сделать принтер доступным для удаленных пользователей, включите флажок **Общий доступ к принтеру** и введите имя общего ресурса. В больших организациях имя должно помочь обнаружить принтер. Например, "Этаж 3, комната 314" означает, что принтер находится в комнате 314 на третьем этаже.
11. При желании заполните поля **Размещение** и **Комментарий**. Эта информация также поможет пользователям определить размещение принтера и его возможности. Нажмите кнопку **Далее**.
12. Последняя страница позволит проверить параметры. Если готовы продолжить установку, нажмите кнопку **Далее**.
13. После установки драйвера принтера и его настройки будет отображена страница состояния. Убедитесь, что установка драйвера и принтера прошла успешно. Если есть ошибки, нужно устранить их и повторить этот процесс. Для проверки принтера включите флажок **Напечатать пробную страницу** и нажмите кнопку **Готово**. Чтобы добавить еще один принтер, отметьте переключатель **Добавить другой принтер** (Add Another Printer) и затем нажмите кнопку **Готово**.
14. По умолчанию общий ресурс принтера не перечислен в Active Directory. Перечисление общего ресурса принтера в Active Directory упрощает поиск принтера для пользователей. Если нужно внести принтер в Active Directory, выберите узел **Принтеры** в оснастке **Управление печатью**, щелкните правой кнопкой мыши на принтере и выберите команду **Перечислить в Active Directory**.
15. По умолчанию задания печати передаются на сервер печати, а затем отправляются на принтер. Данное поведение можно изменить с помощью прямой печати в филиалах, когда задания печати будут воспроизводиться на клиентских компьютерах, а затем уже отправляться непосредственно на принтер. Если нужно включить прямую печать в филиалах, выберите узел **Принтеры** на левой панели, щелкните правой кнопкой мыши по принтеру в главном окне и выберите команду **Включить прямую печать в филиалах** (Enable Branch Office Direct Printing).

Когда мастер установки сетевого принтера завершит установку нового принтера, в папке Принтеры появится только что установленный принтер с указанным при установке именем. Можно изменить свойства принтера и проверить его состояние в любое время, но об этом мы поговорим в *разд. "Настройка свойств принтера" далее в этой главе*.

Совет

Если повторить этот процесс, можно создать дополнительные принтеры для одного и того же устройства печати. Все, что для этого нужно — указать другое имя принтера и другое имя общего ресурса. В результате можно указать различные настройки для разных принтеров, но физическое устройство печати будет одно. Например, можно создать высокоприоритетный принтер для заданий печати, которые должны быть выполнены в первую очередь, и низкоприоритетный принтер для не срочных заданий.

Подключение к сетевым принтерам

После создания сетевого принтера к нему могут подключаться удаленные пользователи и использовать его, как любой другой принтер. Администратору нужно установить соединение с принтером для каждого пользователя или же пользователи могут сделать это самостоятельно. Для создания соединения с принтером в Windows 7 выполните следующие действия:

1. После входа пользователя в систему нажмите кнопку **Пуск**, а затем выберите команду меню **Устройства и принтеры** (Devices and Printers). В окне **Устройства и принтеры** нажмите кнопку **Установка принтера** (Add A Printer) для запуска мастера установки принтера.
2. Нажмите кнопку **Добавить сетевой, беспроводной или Bluetooth-принтер** (Add A Network, Wireless Or Bluetooth Printer). Мастер произведет поиск доступных устройств.
3. Если принтер, который нужно добавить, перечислен в списке найденных принтеров, выберите его и нажмите кнопку **Далее**.
4. Если принтер не перечислен в списке найденных, нажмите кнопку **Нужный принтер отсутствует в списке** (The Printer That I Want Isn't Listed). На странице **Найти принтер по имени или TCP/IP-адресу** (Find A Printer By Name Or TCP/IP Address) выполните одно из следующих действий.
   - Для просмотра сети на наличие общих принтеров выберите **Обзор принтеров** (Find A Printer In The Directory) и нажмите кнопку **Далее**. Выберите компьютер, к которому подключен принтер, а затем и сам принтер.
   - Чтобы указать общий принтер по имени, установите переключатель **Выбрать общий принтер по имени** (Select a shared printer by name). Введите UNC-путь к общему принтеру, например \\PrintServer12\Twelfth Floor NE, или веб-путь к интернет-принтеру, например **http://PrintServer12/Printers/IPrinter52/.printer**.
   - Чтобы указать общий принтер по его TCP/IP-адресу, выберите **Добавить принтер по его TCP/IP-адресу или имени узла** (Add a printer using a TCP/IP address or hostname) и нажмите кнопку **Далее**. Укажите тип устройства и введите имя узла или IP-адрес принтера, например 192.168.1.90. Если вы выберете тип устройства **Автовыбор** (Autodetect) или **Устройство TCP/IP** (TCP/IP Device), мастер установит значение порта в то же значение (значение имени или IP-адреса), но можно выбрать другое значение. Нажмите кнопку **Далее**.
5. На странице **Введите имя принтера** (Type A Printer Name) имя принтера уже будет введено. Можно либо принять имя по умолчанию, либо выбрать новое имя. Нажмите кнопку **Далее** для установки принтера, а затем нажмите кнопку **Готово**. Теперь пользователь может печатать на сетевом принтере, выбрав его в приложении. Значок установленного принтера будет помещен в папку **Устройства и принтеры** (Devices and Printers).

Для создания соединения с принтером в ОС Windows 8.1 выполните эти действия:

1. В окне **Устройства и принтеры** нажмите кнопку **Добавление принтера** (Add A Printer). Мастер добавления принтера попытается автоматически определить прин-

тер. Если мастер обнаружит принтер, с которым нужно работать, щелкните по нему в предоставленном списке, следуйте дальнейшим инструкциям и пропустите оставшиеся шаги этой процедуры. Если мастер не обнаружил принтер, нажмите кнопку **Нужный принтер отсутствует в списке** (The Printer That I Want Isn't Listed) и выполните оставшуюся часть этой процедуры.

2. Выберите переключатель **Добавить принтер Bluetooth, беспроводной принтер или принтер с возможностью обнаружения в сети** (Add Bluetooth, wireless or network discoverable printer) и нажмите кнопку **Далее**.
3. В списке доступных принтеров выберите нужный принтер и затем нажмите кнопку **Далее**.
4. Если будет нужно, установите драйвер принтера на компьютер. Выполните дополнительные шаги мастера и нажмите кнопку **Готово**. Проверить, работает ли принтер, можно, распечатав пробную страницу.

Если при подключении к принтеру возникли проблемы, попытайтесь продиагностировать проблему.

- Убедитесь, что брандмауэр не блокирует соединение с принтером. Необходимо открыть порт на брандмауэре, чтобы разрешить доступ между компьютером и принтером.
- Убедитесь, что принтер включен и подключен к той же сети, что и компьютер. Если сеть состоит из нескольких подсетей, соединенных вместе, попытайтесь подключить принтер к той же подсети, что и компьютер. Определить подсеть можно, посмотрев на IP-адрес компьютера.
- Убедитесь, что принтер настроен для широковещания своего присутствия в сети. Большинство принтеров делают это автоматически.
- Убедитесь, что принтеру назначен IP-адрес и другие сетевые параметры. Если в сети работает DHCP, DHCP-сервер автоматически назначит IP-адрес принтеру при подключении принтера к сети.

Развертывание соединений принтера

Подключение к сетевым принтерам — предельно простой процесс, но его можно сделать еще проще, если развернуть соединения с принтерами посредством групповой политики. Развернуть соединения принтеров к компьютерам или пользователям можно через объекты GPO, которые применяет Windows. Разверните соединения группам пользователям, когда нужно, чтобы пользователи имели доступ к принтерам с любого компьютера, с которого они входят в сеть. Разверните соединения группам компьютеров, если нужно, чтобы все пользователи компьютеров имели доступ к принтерам. Windows добавляет или удаляет соединения принтеров при запуске компьютера или при входе пользователя в сеть.

Чтобы развернуть соединения принтеров с компьютерами, необходимо выполнить эти действия:

1. В оснастке **Управление печатью** разверните узел **Серверы печати** и узел сервера, с которым нужно работать.

2. Выберите узел **Принтеры** сервера печати. В главной части окна щелкните правой кнопкой по принтеру, который нужно развернуть, и выберите команду **Развернуть с помощью групповой политики** (Deploy With Group Policy). Будет открыто окно **Развертывание с помощью групповой политики** (Deploy with Group Policy), показанное на рис. 10.8.

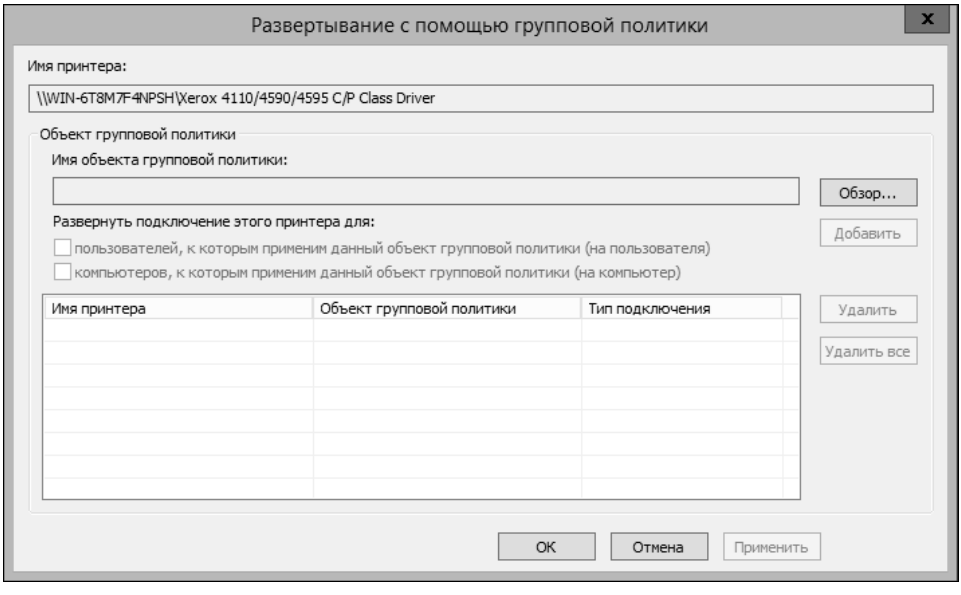


Рис. 10.8. Выберите GPO для развертывания соединения принтера

3. Нажмите кнопку **Обзор**. В окне **Поиск объекта групповой политики** (Browse For Group Policy Object) выберите GPO и затем нажмите кнопку **OK**.
4. Выполните одно из следующих действий.
   - Чтобы развернуть подключение этого принтера для пользователей, отметьте флажок **пользователей, к которым применим данный объект групповой политики (на пользователя)** (The users that this GPO applies to), находящийся под надписью **Развернуть подключение этого принтера для** (Deploy this printer connection to the following).
   - Чтобы развернуть подключение этого принтера для компьютеров, включите флажок **компьютеров, к которым применим данный объект групповой политики (на компьютер)**.
5. Нажмите кнопку **Добавить** для создания записи подключения принтера.
6. Повторите шаги 3–5 для развертывания подключения принтера к другим GPO.
7. Нажмите кнопку **OK** для сохранения изменений в GPO. В диалоге подтверждения убедитесь, что все операции были завершены успешно. Если возникнет ошибка, нажмите кнопку **Подробности** для получения дополнительной информации об ошибке. Большинство ошибок связано с разрешениями доступа к GPO, с которым происходит работа. Если используемая учетная запись не имеет соответствующих

разрешений, необходимо использовать учетную запись с дополнительными привилегиями. Нажмите кнопку **OK**.

Изменение параметров ограничений указания и печати

Параметр групповой политики **Ограничения указания и печати** (Point And Print Restrictions) используется для управления клиентскими функциями указания и печати, в том числе запросами безопасности. Данный параметр находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Принтеры** (Computer Configuration\Politics\Administrative Templates\Printers).

Таблица 10.1 подытоживает, как используется параметр **Ограничения указания и печати**. Обратите внимание, что до Windows 7 и Windows Vista Service Pack 2 этот параметр считается политикой конфигурации пользователя. Если настроить параметр **Ограничения указания и печати** в конфигурации пользователя, данный параметр будет проигнорирован компьютерами под управлением Windows Vista Service Pack 2, Windows 7 и более поздних версий Windows.

Таблица 10.1. *Ограничения указания и печати*

Значение политики	Поведение политики
Включено	Клиенты могут указывать и печатать только на компьютерах своего леса. Клиенты можно настроить для показа (или сокрытия) предупреждений и приглашений повышения прав до администратора[1], когда пользователи пытаются установить или обновить существующий драйвер принтера
Не задано	Клиенты могут указывать и печатать на любом сервере в лесу. Клиенты также не будут показывать предупреждение и требовать прав администратора при печати и обновлении драйвера для существующего подключения принтера
Выключено	Клиенты могут указывать и печатать на любом сервере. Также клиенты не будут показывать предупреждение и требовать прав администратора при печати или обновлении драйвера пользователем

По умолчанию Windows разрешает пользователю, который не является членом локальной группы **Администраторы**, устанавливать только надежные драйверы принтеров, например те, которые предоставляются самой Windows, или драйверы с цифровой подписью. При включении параметра **Ограничения указания и печати** можно разрешить пользователям, которые не являются членами локальной группы **Администраторы**, устанавливать подключения принтеров, развернутые в групповой политике, которые включают дополнительные или обновленные драйверы принтера без цифровой подписи. Если не включить этот параметр, пользователям придется предоставить учетные данные, принадлежащие локальной группе **Администраторы**.

Включить и настроить ограничения указания и печати можно с помощью следующих действий:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которым нужно работать, а затем выберите команду **Изменить** (Edit). В результате будет открыт редактор политики для GPO.

[1] Попросту говоря, окно запроса UAC. — *Прим. пер.*

2. В редакторе управления групповыми политиками разверните узел **Конфигурация компьютера\Политики\Административные шаблоны** (Computer Configuration\Politics\Administrative Templates), а затем выберите узел **Принтеры** (Printers).
3. Дважды щелкните по параметру **Ограничения указания и печати** (Point and Print Restrictions).
4. В окне **Ограничения указания и печати** (рис. 10.9) установите переключатель **Включено** (Enabled).

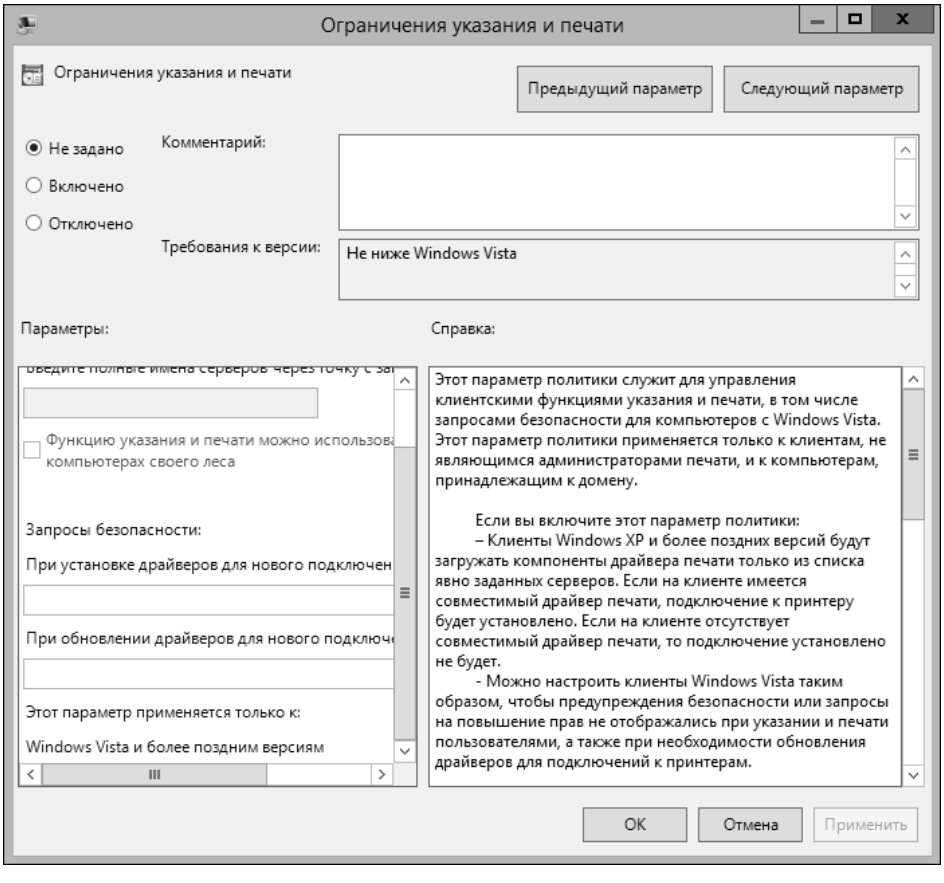


Рис. 10.9. Настройка ограничений указаний и печати

5. Когда ограничения указания и печати включены, можно настроить политику так, что пользователи смогут указывать и печатать только через определенные серверы из списка. Для применения этого ограничения выберите соответствующий переключатель и введите список полных имен серверов, разделяя их запятыми. Чтобы удалить это ограничение, выключите переключатель.
6. Когда ограничения указания и печати включены, можно настроить политику так, что пользователи смогут указывать и печатать только на серверах в своем лесу. Для применения этого ограничения включите соответствующий переключатель. Чтобы удалить это ограничение, выключите переключатель.

7. Когда будут установлены драйверы для нового соединения, клиенты смогут показать или не показывать предупреждение или приглашение повышения прав до администратора. Используйте соответствующий список для выбора опции, которую нужно применить.
8. Когда драйверы для существующего соединения будут обновлены, клиенты могут показать или не показывать предупреждение или приглашение повышения прав до администратора. Используйте соответствующий список для выбора опции, которую нужно применить.
9. Нажмите **OK** для применения конфигурации.

Перемещение принтеров на новый сервер печати

Мастер переноса принтеров (Printer Migration Wizard) используется для перемещения очередей принтеров, драйверов, процессоров и портов принтера с одного сервера печати на другой. Мастер переноса принтеров является эффективным средством для консолидации нескольких серверов печати или замены старого сервера новым. При перемещении принтеров сервер, на котором в данный момент находятся принтеры, является исходным сервером, а сервер, на который нужно эти принтеры переместить, — сервером назначения. Учитывая эту терминологию, переместить принтеры на новый сервер печати можно так:

1. В консоли **Управление печатью** щелкните правой кнопкой мыши на исходном сервере и выберите команду **Экспортировать принтеры в файл** (Export Printers To A File). Будет открыто окно **Перенос принтеров** (Printer Migration Wizard).
2. На начальной странице обратите внимание на то, какие объекты принтера будут экспортированы, и нажмите кнопку **Далее**.
3. На странице **Выберите расположение файла** (Select The File Location) нажмите кнопку **Обзор**. В предоставленном диалоговом окне выберите расположение для файла миграции принтеров. После ввода имени файла нажмите кнопку **Сохранить** (Save).
4. Файл миграции принтеров будет сохранен с расширением printerExport. Нажмите кнопку **Далее** для сохранения настроек принтера в этот файл.
5. После того как мастер завершит процесс экспорта, нажмите кнопку **Открыть просмотр событий** (Open Event Viewer) для просмотра событий, сгенерированных во время экспорта. Если произошли ошибки, можно использовать записи события для определения того, что случилось, и того, что нужно предпринять для разрешения проблемы. По окончанию закройте окно **Просмотр событий** (Event Viewer).
6. На странице **Экспорт** (Exporting) нажмите кнопку **Готово**, чтобы закрыть окно мастера.
7. В консоли **Управление печатью** щелкните правой кнопкой мыши по серверу назначения и выберите команду **Импортировать принтеры из файла** (Import Printers From A File). Опять будет открыто окно **Перенос принтеров**.
8. На странице **Выберите расположение файла** нажмите кнопку **Обзор**. В диалоговом окне выберите ранее сохраненный файл миграции принтеров и нажмите кнопку **Открыть**.

9. Нажмите кнопку **Далее**. Обратите внимание на объекты, которые будут импортированы, и нажмите кнопку **Далее**. На странице **Выберите параметры импорта** (Select Import Options) выберите одну из следующих опций из списка **Режим импорта** (Import mode):

   - **Сохранить существующие принтеры** (Keep existing printers) — при выборе этой опции и наличии очередей принтеров с такими же именами, как у импортируемых, мастер создает копии, чтобы гарантировать, что будут доступны как исходные очереди принтеров, так и импортированные;
   - **Перезаписать существующие принтеры** (Overwrite existing printers) — при выборе этой опции и наличии очередей принтеров с такими же именами, как у импортируемых, мастер перезапишет существующие очереди принтеров информацией из файла импорта.

10. На странице **Выберите параметры импорта** (Select Import Options) из списка **Перечислить в каталоге** (List in the directory) выберите одну из опций:

    - **Перечислить принтеры, которые были в списке ранее** (List printers that were previously listed) — выбор этой опции перечислит только те принтеры, которые ранее были перечислены в Active Directory;
    - **Составить список всех принтеров** (List all printers) — выберите эту опцию, если нужно перечислить все принтеры в Active Directory;
    - **Не составлять список принтеров** (Don't list any printers) — выберите эту опцию, если не нужно перечислять принтеры в Active Directory.

11. Нажмите кнопку **Далее** для начала процесса импорта. После того как мастер завершит процесс импорта, нажмите кнопку **Открыть просмотр событий** для просмотра событий, сгенерированных во время экспорта. Если произошли ошибки, можно использовать записи события для определения того, что случилось, и того, что нужно предпринять для разрешения проблемы. По окончанию закройте окно **Просмотр событий**.

12. На странице **Импорт** (Importing) нажмите кнопку **Готово** для выхода из мастера переноса принтеров.

Автоматический мониторинг принтеров и очередей принтеров

Фильтры принтеров отображают только принтеры, очереди принтеров и драйверы принтеров, которые соответствуют определенным критериям. Посредством автоматического уведомления можно использовать фильтры принтеров для автоматического мониторинга принтеров.

Просмотреть существующие фильтры можно, развернув узел **Настраиваемые фильтры** (Custom Filters) в консоли **Управление печатью**. Если развернуть узел **Настраиваемые фильтры** и выбрать фильтры, основная панель покажет все принтеры или драйверы принтеров, которые соответствуют критерию фильтра.

Консоль **Управление печатью** содержит следующие фильтры принтеров:

- **Все принтеры** (All Printers) — перечисляет все принтеры, связанные с серверами печати, которые были добавлены в консоль;
- **Все драйверы** (All Drivers) — перечисляет все драйверы принтеров, связанные с серверами печати, которые были добавлены в консоль;
- **В состоянии "Не готов"** (Printers Not Ready) — перечисляет все принтеры, не находящиеся в состоянии "Готов", например принтеры с ошибками;
- **С заданиями печати** (Printers With Jobs) — перечисляет все принтеры, связанные с серверами печати, у которых есть активные или отложенные задания печати.

Создать новый фильтр можно так:

1. В консоли **Управление печати** щелкните правой кнопкой мыши на узле **Настраиваемые фильтры** и выберите команду **Добавить новый фильтр принтеров** (Add New Printer Filter) для запуска мастера создания фильтра принтеров.
2. На странице **Имя и описание фильтра** (Printer Filter Name And Description) введите имя и описание фильтра. Если справа от имени фильтра в круглых скобках нужно выводить число элементов, соответствующих критерию фильтра, отметьте переключатель **Показывать общее число элементов после имени фильтра** (Display the total number of printers). Нажмите кнопку **Далее**.
3. На странице **Определение фильтра** (Define A Filter) определите фильтр, указав поле, условие и значение критерия. Если нужно придерживаться нескольких критериев, определите дополнительный критерий во второй, третьей и всех последующих строках. Нажмите кнопку **Далее**, когда будете готовы продолжить.

> ***Примечание***
>
> При использовании фильтров для мониторинга и уведомления в основном используется поле **Состояние очереди** (Queue Status). Это поле позволяет получать уведомления, когда принтер находится в определенном состоянии. Доступные значения состояния: **Готов**, **Приостановлен**, **Ошибка**, **Удаление**, **Застряла бумага**, **Нет бумаги**, **Требуется ручная подача**, **Неполадки с бумагой**, **Отключен**, **Идет ввод-вывод**, **Занят**, **Печать**, **Выходной лоток полон**, **Недоступен**, **Ожидание**, **Обработка**, **Инициализация**, **Прогрев**, **Тонер или чернила на исходе**, **Нет тонера или чернил**, **Нет бумаги**, **Требуется внимание**, **Недостаточно памяти**, **Открыта дверца**.

> ***Совет***
>
> При создании фильтра можно выбрать условие "совпадает с" или "не совпадает". Например, если нужно получить уведомление о состоянии принтера, обратите внимание на поле **Состояние очереди**, которое может принимать значения **Удаление**, **Инициализация**, **Идет ввод-вывод**, **Печать**, **Обработка**, **Ожидание**, **Прогрев** и **Готов**.

4. На странице **Настроить уведомления (не обязательно)** (Set Notifications (Optional)) можно определить действия, которые будут выполнены: отправка сообщения по электронной почте или запуск сценария (можно указать оба действия). Нажмите кнопку **Готово** для завершения конфигурации.

Изменить существующий пользовательский фильтр можно так:

1. В консоли **Управление печатью** разверните узел **Настраиваемые фильтры**. Щелкните по фильтру, который нужно изменить. Из контекстного меню выберите команду **Свойства**.

2. В окне **Свойства** используйте предоставленные опции для управления настройками фильтра. В этом окне есть следующие три вкладки:
   - **Общие** (General) — показывает имя и описание фильтра принтера. Введите новое имя и описание в случае необходимости;
   - **Критерий фильтра** (Filter Criteria) — показывает критерий фильтра. Введите новый критерий в случае необходимости;
   - **Уведомление** (Notification) — показывает параметры электронной почты и сценария. Введите новый e-mail или сценарий в случае необходимости.

Решение проблем с очередью печати

Windows Server 2012 R2 использует службу **Диспетчер печати** (Print Spooler) для управления спулингом заданий печати. Если эта служба не запущена, задания печати не могут быть поставлены в очереди. Используйте консоль **Службы** (Services) для проверки состояния диспетчера очереди печати. Выполните следующие действия для проверки и перезапуска службы **Диспетчер печати**:

1. Из меню **Средства** (Tools) диспетчера серверов выберите команду **Управление компьютером**.
2. Если нужно подключиться к удаленному компьютеру, щелкните правой кнопкой мыши по записи **Управление компьютером** (Computer Management) в дереве консоли, а затем выберите команду **Подключиться к другому компьютеру** (Connect To Another Computer). После этого можно выбрать систему, службами которой нужно управлять.
3. Разверните узел **Службы и приложения** (Services And Applications) и выберите узел **Службы** (Services).
4. Выберите службу **Диспетчер печати** (Print Spooler). Состояние службы должно быть **Выполняется** (Started). Тип запуска должен быть **Автоматически** (Automatic). Если это не так, дважды щелкните по службе **Диспетчер печати** и измените параметр **Тип запуска** (Startup Type) на **Автоматически**.

> ***Совет***
>
> Очереди печати иногда могут быть повреждены. Симптом поврежденной очереди — "замороженный" принтер или невозможность отправки заданий печати на устройство печати. Иногда устройство печати может напечатать страницы с "мусором" вместо текста. В большинстве случаев проблему можно решить путем перезапуска службы **Диспетчер печати**. Другие проблемы с очередями печати связаны с разрешениями, о них мы поговорим в *разд. "Установка разрешений принтера" далее в этой главе*.

Настройка свойств принтера

В данном разделе описывается, как установить часто используемые свойства принтера. После установки сетевого принтера его свойства можно задать так:

1. В консоли **Управление печатью** разверните узел **Серверы печати** (Print Servers) и узел сервера, с которым нужно работать.

2. Выберите узел **Принтеры** (Printers) выбранного сервера. На главной панели щелкните правой кнопкой мыши на принтере, с которым нужно работать, и выберите команду **Свойства**. После этого можно установить свойства принтера.

Добавление комментариев и информации о расположении

Чтобы было проще определить, какой принтер и когда нужно использовать, можно добавить комментарии и информацию о расположении принтеров. Комментарии предоставляют общую информацию о принтере, например, тип устройства печати и кто отвечает за него. Расположение описывает физическое расположение устройства печати. После установки полей **Расположение** и **Комментарий** приложения могут отображать их. Например, Microsoft Word отображает эту информацию в диалоге печати, когда вы выбираете команду **Печать** (Print) из меню **Файл**. Установить значения комментария и расположения можно на вкладке **Общие** (General) диалога **Свойства** принтера. Введите комментарий в поле **Комментарий** (Comment), а информацию о расположении в поле **Расположение** (Location).

Перечисление принтеров в Active Directory

Перечисление принтеров в Active Directory упрощает для пользователей их поиск и установку. Перечислить принтер в Active Directory можно одним из способов:

- щелкните правой кнопкой мыши по имени принтера и выберите команду **Перечислить в Active Directory** (List In Directory);
- откройте диалог **Свойства** принтера, перейдите на вкладку **Доступ** (Sharing), отметьте переключатель **Внести в Active Directory** (List In Directory).

Управление драйверами принтера

В домене Windows Server 2012 R2 нужно настраивать и обновлять драйверы принтера только на серверах печати. Не требуется обновлять драйверы на клиентах Windows. Вместо этого следует настроить сетевой принтер, чтобы он предоставлял драйверы клиентским системам при необходимости.

Обновление драйвера принтера

Для обновления драйвера принтера выполните следующие действия:

1. Откройте диалог **Свойства** принтера и перейдите на вкладку **Дополнительно** (Advanced).
2. Из списка **Драйвер** (Driver) выберите драйвер из перечня установленных в данный момент драйверов. Используйте этот список для выбора нового драйвера из перечня известных драйверов.
3. Если драйвер отсутствует в списке или нужно получить новый драйвер, нажмите кнопку **Сменить** (New driver) для запуска мастера установки драйверов принтера (Add Printer Driver Wizard). Нажмите кнопку **Далее**.

4. Если производитель устройства и/или модель не отображаются в списке, нажмите кнопку **Центр обновления Windows** (Windows Update). ОС подключится к сайту Windows Update для загрузки списка принтеров и покажет дополнительные модели. Эта функция — часть автоматической функции настройки драйвера. Для получения списка драйверов необходимо несколько минут. После этого появится возможность выбрать нужного производителя/модель принтера.
5. Если после этого производитель (или модель) не появился в списке, нажмите кнопку **Установить с диска** (Have Disk) для установки нового драйвера из файла или диска. В диалоге **Установка с диска** (Install From Disk) введите имя папки, в которой находится файл драйвера, или нажмите кнопку **Обзор**, чтобы открыть диалоговое окно **Поиск файла** (Locate File) и выбрать файл драйвера. Нажмите кнопку **ОК**.
6. Нажмите кнопку **Далее**, а затем нажмите кнопку **Готово**.

Настройка драйверов для сетевых клиентов

После установки принтера или изменения драйверов нужно выбрать операционные системы, которые должны загрузить драйвер с сервера печати. Позволяя клиентам загрузить драйвер принтера, администратор обеспечивает единственное расположение для установки обновлений драйвера. Таким образом, вместо того чтобы устанавливать новый драйвер на всех клиентских системах, нужно установить драйвер только на сервере печати и разрешить клиентам загрузить новый драйвер.

Разрешить клиентам загружать новые драйверы можно так:

1. Щелкните правой кнопкой мыши на значке принтера, который нужно настроить, и затем выберите команду **Свойства**.
2. Перейдите на вкладку **Доступ** (Sharing) и нажмите кнопку **Дополнительные драйверы** (Additional Drivers).
3. В диалоговом окне **Дополнительные драйверы** (Additional Drivers) выберите операционные системы, которые могут загрузить драйвер принтера. При необходимости вставьте в привод носитель с Windows Server 2012 R2, диск с драйверами принтера или оба носителя для выбранных операционных систем. Инсталляционный носитель Windows Server 2012 R2 содержит драйверы для большинства операционных систем Windows.

Установка страницы разделителя и изменение режима устройства печати

Страницы разделителя имеют два применения в системах Windows Server 2012 R2:

- их можно использовать в начале задания печати, чтобы пользователям было легче найти свои документы на занятых устройствах печати;
- их можно использовать для изменения режима устройства печати, например, должно ли устройство использовать PostScript или PCL (Printer Control Language).

Для установки страницы разделителя для устройства печати выполните следующие действия:

1. На вкладке **Дополнительно** (Advanced) диалогового окна **Свойства** принтера нажмите кнопку **Страница-разделитель** (Separator Page).
2. В диалоговом окне **Страница-разделитель** (Separator Page) введите имя файла разделителя, который нужно использовать. Обычно нужно использовать один из следующих страниц-разделителей:
   - Pcl.sep — переключает устройство печати в режим PCL и распечатывает страницу-разделитель перед каждым документом;
   - Pscript.sep — переключает устройство в режим PostScript и не печатает страницу-разделитель;
   - Sysprint.sep — устанавливает устройство печати в режим PostScript и печатает страницу-разделитель перед каждым документом.

   Примечание

   Sysprintj.sep — альтернативная версия Sysprint.sep, используется для японских шрифтов.
3. Чтобы прекратить использование страницы-разделителя, откройте диалоговое окно **Страница-разделитель** (Separator Page) и удалите имя файла.

   Примечание

   При работе с локальным сервером нажмите кнопку **Обзор** в диалоговом окне **Страница-разделитель**, откройте папку *%SystemRoot%*\Windows\System32, в которой вы найдете нужные файлы-разделителя. При работе с удаленным сервером кнопка **Обзор** обычно недоступна, поэтому нужно ввести точное имя файла для страницы-разделителя.

Изменение порта принтера

Администратор может изменить порт, используемый устройством печати с помощью окна **Свойства** настраиваемого принтера. Откройте окно **Свойства**, затем перейдите на вкладку **Порты**. Теперь можно добавить, удалить или настроить порт. Чтобы добавить порт, отметьте его переключатель, а чтобы удалить порт, выключите его переключатель. Чтобы добавить новый тип порта, нажмите кнопку **Добавить порт** (Add Port). В диалоговом окне **Порты принтера** (Printer Ports) выберите новый порт и нажмите кнопку **Новый порт** (New Port). Введите допустимое имя порта и нажмите кнопку **OK**. Чтобы удалить порт, выберите его и нажмите кнопку **Удалить порт** (Delete Port).

Планирование и приоритезация заданий печати

Диалоговое окно **Свойства** можно использовать для изменения параметров по умолчанию для планирования и приоритезации заданий печати. Откройте этот диалог и перейдите на вкладку **Дополнительно** (Advanced). Теперь можно изменить расписание и приоритет заданий печати, используя поля, изображенные на рис. 10.10. Каждое из этих полей подробно рассматривается далее.

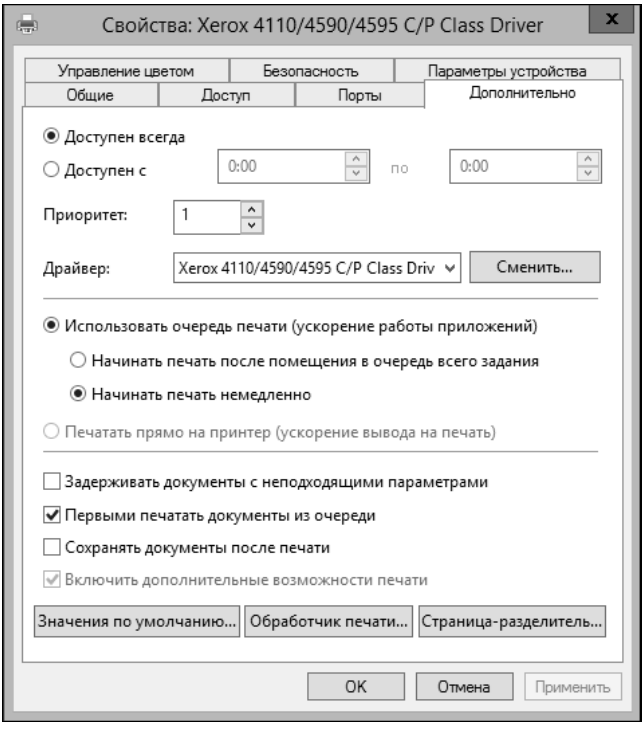


Рис. 10.10. Настройка планирования и приоритезации на вкладке **Дополнительно**

Планирование доступности принтера

Принтеры могут быть всегда доступны или доступны только в определенное время. Доступность принтера можно установить на вкладке **Дополнительно**. Выберите переключатель **Доступен всегда** (Always available), если принтер должен быть доступен всегда. Выберите **Доступен с** (Available from) и задайте часы работы, когда должен работать принтер.

> ***Совет***
>
> Как было упомянуто ранее, можно создать дополнительные принтеры для одного и того же устройства печати. Все, что вы должны сделать — изменить имя принтера и сетевое имя. Чтобы обработать длинные задания печати, которые могут помешать нормальной работе принтера, можно указать, что принтер будет недоступен в нерабочее время. Вы можете создать один принтер, который будет доступен всегда, а другой — который будет доступен только в определенное время. Принтер, который доступен всегда, пользователи могут использовать для длинных заданий печати. Ключ к успеху в том, что пользователи знают о существовании двух принтеров и что пользователи представляют, как использовать разные принтеры.

Установка приоритета принтера

Администратор может установить приоритет по умолчанию для заданий печати в поле **Приоритет** (Priority) на вкладке **Дополнительно** (Advandced). Задания с более высоким приоритетом выполняются перед заданиями с более низким приоритетом.

Конфигурирование очереди печати

Для устройств печати, подключенных к сети, обычно нужно, чтобы принтер сначала ставил файлы в очередь, а потом уже распечатывал. Очередь печати (print spooling) позволяет использовать принтер для управления заданиями печати.

Включение очереди печати

Для включения очереди печати используйте один из вариантов.

- **Использовать очередь печати (ускорение работы приложений)** (Spool print documents so program finishes printing faster) — выберите эту опцию для постановки в очередь заданий печати.
- **Начинать печатать после помещения в очередь всего задания** (Start printing after last page is spooled) — выберите эту опцию, если нужно начинать печатать только после того, как в очередь помещено все задание. Опция гарантирует, что весь документ будет помещен в очередь перед печатью. Если по некоторым причинам печать будет отменена или не будет завершена, задание не будет напечатано.
- **Начинать печатать немедленно** (Start Printing immediately) — печать будет начата немедленно, если устройство печати не используется в данный момент. Если нужно выполнять задания печати как можно быстрее, задание будет напечатано быстрее, чем в предыдущем случае. Опция предпочтительна, если нужно быстрее напечатать задание или чтобы приложение вернуло пользователю контроль, как можно быстрее.

Другие параметры печати

Отключить очередь печати можно, выбрав переключатель **Печатать прямо на принтер** (Print directly to the printer). Следующие дополнительные параметры позволяют настраивать очередь печати.

- **Задерживать документы с неподходящими параметрами** (Hold mismatched documents) — если выбрать эту опцию, задание печати, не соответствующее настройкам устройства печати, будет задержано. Выбор этой опции — отличная идея, если нужно часто менять принтер или назначение лотка.
- **Первыми печатать документы из очереди** (Print spooled documents first) — если выбрать эту опцию, то задания, уже помещенные в очередь, будут распечатаны раньше, чем задания, которые только помещаются в очередь (даже если у заданий, находящихся только в процессе спулинга, есть более высокий приоритет).
- **Сохранять документы после печати** (Keep printed documents) — обычно документы удаляются из очереди после того, как они напечатаны. Чтобы хранить копии таких документов в принтере, можно выбрать эту опцию. Включение этой опции ускорит повторную печать документа. Подробности будут приведены в *разд. "Приостановка, возобновление и перезапуск печати отдельных документов" далее в этой главе*.
- **Включить дополнительные возможности печати** (Enable advanced printing features) — выбор этого флажка приведет к возможности использования дополнительных опций (если они доступны) вроде **Порядок страницы** (Page order) и **Число**

страниц на листе (Pages per sheet). Если возникли проблемы с этими дополнительными возможностями, установите данный флажок.

Предоставление общего доступа к принтеру

Настроить общий доступ к принтеру можно в окне **Свойства** настраиваемого принтера. Щелкните правой кнопкой мыши по принтеру, который нужно настроить, и выберите команду **Управление общим доступом**. В результате будет открыто окно **Свойства** с активной вкладкой **Доступ**. Данную вкладку можно использовать для изменения имени сетевого принтера, а также для предоставления или прекращения общего доступа к принтеру. Далее представлены задачи, касающиеся общего доступа, которые может выполнить администратор.

- **Предоставление общего доступа к локальному принтеру (превращение локального принтера в сетевой).** Для предоставления общего доступа к принтеру выберите опцию **Общий доступ к данному принтеру** и укажите имя общего ресурса в поле **Имя общего ресурса**. Нажмите кнопку **OK**, когда будете готовы.
- **Изменение имени сетевого ресурса.** Для изменения имени общего ресурса просто введите новое имя в поле **Имя общего ресурса** и нажмите кнопку **OK**.
- **Прекращение общего доступа к принтеру.** Для прекращения доступа к принтеру выключите флажок **Общий доступ к данному принтеру** и нажмите кнопку **OK**.

Установка разрешений принтера

Сетевые принтеры являются общими ресурсами. А раз так, администратор может установить разрешения доступа для них. Установить разрешения доступа можно в окне **Свойства** настраиваемого принтера. Откройте окно **Свойства** и перейдите на вкладку **Безопасность** (Security). Администратор может назначить следующие разрешения: **Печать**, **Управление этим принтером**, **Управление документами** и **Особые разрешения**. Таблица 10.2 содержит сводку возможностей этих разрешений.

Таблица 10.2. *Разрешения принтера, используемые Windows Server 2012 R2*

Разрешение	Печать	Управление документами	Управление этим принтером
Печать документов	×	×	×
Приостановка, перезапуск, возобновление и отмена собственных документов	×	×	×
Подключение к принтерам	×	×	×
Управление настройками заданий печати		×	×
Приостановка, перезапуск и удаление заданий печати		×	×
Предоставление общего доступа к принтерам			×
Изменение свойств принтера			×
Изменение разрешениями принтера			×
Удаление принтеров			×

Разрешения по умолчанию используются для любого созданного сетевого принтера. Эти параметры таковы.

- Члены групп **Администраторы**, **Операторы печати** и **Операторы сервера** имеют полный контроль над принтером по умолчанию. Это дает возможность администрировать принтер и его задания печати.
- Создатель или владелец документа может управлять своим документом. В результате пользователь, который отправил на печать документ, может изменить его параметры или удалить его.
- Каждый может печатать на принтере. Все пользователи сети могут получить доступ к принтеру по сети.

Только что были рассмотрены базовые разрешения принтеров. Аналогично, администратор может задать особые разрешения, используемые для создания базовых разрешений для принтеров. Сводка по особым разрешениям приведена в табл. 10.3. Чтобы задать особые разрешения, нажмите кнопку **Дополнительно**.

Таблица 10.3. *Особые разрешения для принтеров*

Специальные разрешения	Печать	Управление документами	Управление этим принтером
Печать	×		×
Управление документами		×	
Управление этим принтером			×
Чтение разрешений	×	×	×
Смена разрешений		×	×
Смена владельца		×	×

Аудит заданий печати

ОС Windows Server 2012 R2 позволяет вам производить аудит общих задач принтера так:

1. Откройте диалоговое окно **Свойства** принтера, а затем перейдите на вкладку **Безопасность**. Нажмите кнопку **Дополнительно** (Advanced), чтобы открыть окно **Дополнительные параметры безопасности** (Advanced Security Settings).

   Примечание

   Действия не отслеживаются по умолчанию. Сначала нужно включить аудит, установив групповую политику для аудита принтера.

2. На вкладке **Аудит** (Auditing) добавьте имена пользователей или групп пользователей, нажав кнопку **Добавить** (Add). Для удаления пользователей или групп пользователей используйте кнопку **Удалить** (Remove).
3. Выберите события, которые нужно отслеживать, включив соответствующие флажки под заголовками **Успех** (Success) и **Отказ** (Failure).
4. Нажмите кнопку **OK**.

Установка значений по умолчанию для документа

Параметры документа по умолчанию используются, только когда вам нужно выполнить печать из приложений, которые не являются Windows-приложениями, например, когда осуществляется печать из командной строки. Параметры по умолчанию для документа можно установить так:

1. Откройте окно **Свойства** (Properties) и щелкните по вкладке **Общие** (General).
2. Нажмите кнопку **Настройка** (Preferences).
3. Используя предоставленные вкладки, установите параметры по умолчанию.

Настройка свойств сервера печати

ОС Windows Server 2012 R2 позволяет администратору контролировать глобальные параметры для серверов печати, используя окно **Свойства: Сервер печати**. В управлении печати щелкните правой кнопкой мыши по записи сервера, с которым нужно работать, а затем выберите команду **Свойства**. Если сервер печати не отображается, добавьте его с помощью окна **Добавление и удаление серверов** (Add/Remove Servers). Чтобы открыть это окно, щелкните правой кнопкой мыши на узле **Серверы печати** (Print Servers) и выберите команду **Добавление и удаление серверов** (Add/Remove Servers).

Далее приводится объяснение некоторых параметров сервера печати.

Задание папки очереди печати и включение печати на NTFS

Папка очереди печати хранит копии всех документов, находящихся в очереди принтера. По умолчанию эта папка находится в *%SystemRoot%*\System32\Spool\Printers. В файловой системе NTFS все пользователи, которые получают доступ к принтеру, должны иметь разрешение **Изменение** (Modify) на этом каталоге. Если такого разрешения нет, пользователь не сможет распечатать документы.

Если произошли проблемы, проверьте разрешение на этом каталоге, выполнив следующие действия:

1. Откройте окно **Свойства: Сервер печати** (Print Server Properties).
2. Перейдите на вкладку **Дополнительные параметры** (Advanced). Запомните путь, указанный в поле **Папка очереди печати** (Spool folder).
3. Откройте Проводник и перейдите к папке, которая используется для очереди печати, щелкните правой кнопкой мыши на папке и выберите команду **Свойства**.
4. Перейдите на вкладку **Безопасность** (Security). Теперь можно проверить, что разрешения установлены надлежащим образом.

Управление большими объемами печати

Принтеры, используемые в корпоративной среде, могут печатать сотни и тысячи документов ежедневно. При печати в таких объемах можно столкнуться с различными про-

блемами — повреждение документов, задержки печати и другие проблемы. Чтобы облегчить часть этого бремени, нужно сделать следующее.

- Используйте принтеры, непосредственно подключенные к сети. Такие принтеры позволяют сократить использование системных ресурсов (особенно использование процессора).
- Используйте прямую печать в филиалах для прорисовки заданий печати на клиентских компьютерах. После прорисовки задания печати будут отправлены непосредственно на принтер. Если прямая печать в филиалах выключена, задания печати отправляются на принтер, где они прорисовываются и затем отправляются на принтер.
- Выделите сервер печати для обслуживания только служб печати. Если сервер печати выполняет другие функции, он не может быстро реагировать на запросы печати и управления. Для увеличения скорости отклика, нужно переместить другие сетевые функции на другие серверы.
- Переместите папку очереди печати на диск, выделенный для печати. По умолчанию папка очереди печати находится на том же диске, что и операционная система. Чтобы повысить производительность дискового ввода-вывода, используйте диск, подключенный к отдельному контроллеру.

Включение уведомления об ошибках задания печати

Серверы печати могут подать звуковой сигнал, чтобы уведомить пользователей, если удаленный документ не может быть распечатан. По умолчанию эта функция выключена, поскольку может быть весьма раздражающей. Если нужно активировать или удалить это уведомление, откройте вкладку **Дополнительные параметры** (Advanced) окна **Свойства: Сервер печати** (Print Server Properties). Установите флажок **Звуковой сигнал при ошибках удаленной печати документов** (Beep on errors of remote documents).

Управление заданиями печати на локальных и удаленных принтерах

Посредством окна **Управление печатью** администратор может управлять заданиями печати и принтерами. Если принтер настроен в системе, получить доступ к окну управления печатью можно, используя один из следующих способов.

- Получите доступ к папке **Устройства и принтеры** (Devices and Printers) сервера печати. Дважды щелкните по значку принтера, с которым нужно работать. Если принтер не настроен в этой системе, можно управлять им удаленно, используя консоль **Сеть** (Network). Дважды щелкните по значку сервера печати, затем дважды щелкните по значку папки **Устройства и принтеры** или просто **Принтеры** (Printers).
- В окне **Управление печатью** (Print Management) дважды щелкните по узлу **Серверы печати** (Print Servers), а затем дважды щелкните по записи сервера печати. Вы-

берите узел **Принтеры** (Printers). Щелкните правой кнопкой мыши по нужному принтеру и выберите команду **Открыть очередь печати** (Open Printer Queue).

- В окне **Управление печатью** щелкните правой кнопкой мыши по узлу **Принтеры** (Printers) и выберите команду **Показать расширенное представление** (Show Extended View). Далее в верхней части окна выберите принтер, а нижняя часть окна отобразит задания печати.

Просмотр очереди принтера и заданий печати

Администратор может теперь управлять заданиями печати и принтерами, используя окно управления печатью (рис. 10.11). Это окно показывает информацию о документах в принтере:

- **Документ** (Document Name) — имя файла документа, которое также может содержать имя приложения, отправившего документ на печать;
- **Состояние** (Status) — состояние задания печати, которое может содержать как состояние документа, так и состояние принтера;
- **Владелец** (Owner) — владелец документа;
- **Число страниц** (Pages) — число страниц в документе;
- **Размер** (Size) — размер документа в килобайтах или мегабайтах;
- **Поставлено в очередь** (Submitted) — время и дата постановки задания в очередь;
- **Порт** (Port) — порт, используемый для печати, например, LPT1, COM3, файл или IP-адрес (если применимо).

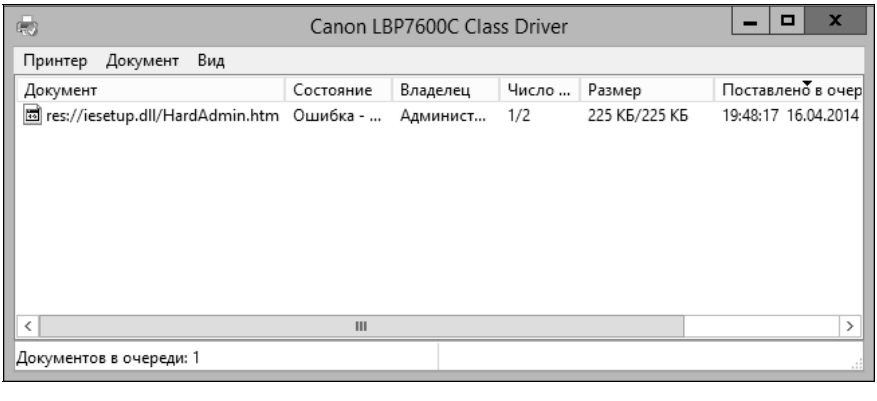


Рис. 10.11. Данное окно позволяет управлять заданиями печати и принтерами

Приостановка и возобновление печати

Иногда нужно приостановить печать. Чтобы сделать это, в окне очереди печати выберите команду **Приостановить печать** (Pause Printing) из меню **Принтер** (галочка напротив этой команды говорит о том, что команда уже выбрана). При этом принтер закончит текущее задание, а все последующие будут приостановлены.

Для возобновления печати выберите команду **Приостановить печать** второй раз. При этом флажок слева от команды будет сброшен.

Очистка очереди печати

Окно очереди печати может использоваться для очистки очереди печати и удаления всего ее содержимого. Чтобы сделать это, выберите команду **Очистить очередь печати** (Cancel All Documents) из меню **Принтер** (Printer). Очистка очереди печати особенно полезна, когда возникла проблема с принтером и пользователи пытались распечатать одни и те же документы несколько раз.

Приостановка, возобновление и перезапуск печати отдельных документов

Можно установить состояние отдельных документов, используя меню **Документ** в окне управления очередью печати. Для изменения состояния документа щелкните правой кнопкой мыши по документу, а далее используйте одну из следующих опций для изменения состояния задания печати:

- **Приостановить** (Pause) — приостанавливает печать текущего документа и переходит к печати других документов;
- **Продолжить** (Resume) — возобновляет печать документа с того места, где печать была приостановлена;
- **Перезапустить** (Restart) — перезапускает печать, печать документа будет начата с самого начала.

Удаление документа и отмена задания печати

Для удаления документа из принтера или отмены задания печати выберите документ в окне очереди печати. Щелкните по нему правой кнопкой мыши и выберите команду **Отменить** (Cancel) или нажмите клавишу <Delete>.

> ***Примечание***
>
> Когда задание печати будет отменено, устройство печати может продолжить печать и распечатать часть или даже весь документ. Это происходит, поскольку большинство устройств печати помещает документы в свой внутренний буфер и может продолжить печатать содержимое документа из кэша.

Проверка свойств документов в принтере

Свойства документа могут подсказать много вещей о печатаемом документе, например, источник страницы, ориентацию и размер. Проверить свойства документа в принтере можно посредством выполнения одного из следующих действий:

- щелкните правой кнопкой мыши по документу в окне очереди печати, а затем выберите команду **Свойства**;
- дважды щелкните по документу в окне очереди печати.

Установка приоритета отдельных документов

Приоритет определяет, когда документ будет распечатан. Документы с более высоким приоритетом будут напечатаны перед документами с более низким приоритетом. Установить приоритет отдельного документа в принтере можно так:

1. Щелкните правой кнопкой мыши по документу в окне очереди печати, а затем выберите команду **Свойства**.
2. На вкладке **Общие** (General) используйте ползунок **Приоритет** (Priority) для установки приоритета документа (от 1 до 99).

Планирование печати отдельных документов

В загруженной среде печати можно запланировать печать документов на принтере. Например, большие задания печати с низким приоритетом можно печатать ночью. Для установки расписания печати выполните эти действия:

1. Щелкните правой кнопкой мыши на документе в окне очереди печати и выберите команду **Свойства**.
2. На вкладке **Общие** (General) выберите переключатель **только с** (Only from) и укажите время, когда данный документ должен быть напечатан. Например, можно указать, что документ должен быть распечатан между полночью и 5-ю часами утра.

ГЛАВА 11

Резервное копирование и восстановление данных

Поскольку данные — основа предприятия, их защита очень важна. И чтобы защитить данные организации, нужно реализовать план резервного копирования и восстановления. Резервное копирование файлов может защитить их от неожиданной потери, повреждения базы данных, сбоев оборудования и даже от стихийных бедствий. Задача администратора — убедиться, что резервные копии создаются часто и хранятся в безопасном месте.

Создание плана резервного копирования и восстановления

Резервное копирование данных — это план страхования. Каждый раз важные файлы случайно удаляются. Критически важные данные могут быть повреждены. Стихийные бедствия могут разрушить офис. Благодаря плану резервного копирования и восстановления можно восстановить свои данные, что бы ни случилось.

Нюансы плана резервного копирования

Настало время создать и реализовать план резервного копирования и восстановления. Нужно выяснить, какие данные нуждаются в резервном копировании, как часто оно должно происходить и т. д. Чтобы все прояснить, ответьте на следующие вопросы.

- **Какие важные или чувствительные данные хранятся на системах?** Знание, насколько данные важны, позволит определить, нужно ли их архивировать, а также когда и как они должны быть заархивированы. Для критических данных, например для базы данных, должны быть избыточные резервные копии, покрывающие несколько резервных периодов. Для чувствительных данных нужно убедиться, что резервные копии физически находятся в безопасном месте или зашифрованы. Для менее важных данных, например для ежедневных пользовательских файлов, нет необходимости в таком тщательно продуманном плане резервного копирования, но следует регулярно архивировать данные и гарантировать, что они могут быть легко восстановлены.

- **Какой тип информации содержат данные?** Данные, на первый взгляд не содержащие ничего интересного для администратора, для кого-то могут быть очень важными. Тип информации поможет определить, нуждаются ли в архивировании эти данные, а также когда и как они должны быть заархивированы.
- **Как часто изменяются данные?** Частота изменений может повлиять на то, как часто эти данные должны архивироваться. Например, данные, которые изменяются ежедневно, должны ежедневно архивироваться.
- **Можно комбинировать резервные копии с теневыми копиями?** *Теневые копии* — копии документов в совместно используемых папках. Эти копии делают восстановление документов очень простым, поскольку можно быстро вернуться к более старой версии документа, если он был удален или случайно перезаписан. Нужно использовать теневые копии в дополнение к стандартным резервным копиям, но не в качестве замены резервного копирования.
- **Как быстро нужно восстановить данные?** Время восстановления — очень важный фактор в плане резервного копирования. Для критических систем резервные копии должны быть восстановлены в оперативном режиме. Чтобы сделать это, возможно, придется изменить свой план резервного копирования.
- **Есть ли оборудование для выполнения резервного копирования?** Организация должна обладать аппаратными средствами резервного копирования. Чтобы выполнить своевременное резервное копирование, возможно, понадобятся несколько таких устройств и несколько наборов носителей резервной копии. К такому оборудованию относятся: жесткие диски, стримеры, накопители на оптических дисках и съемные диски. В большинстве случаев для резервного копирования предпочтительнее использовать жесткие диски.
- **Кто будет ответственен за план восстановления и резервное копирование?** Идеально, когда кто-то один отвечает за резервное копирование в организации и за план восстановления. Этот человек может быть также ответственен за выполнение фактического резервного копирования и восстановление данных.
- **Какое наилучшее время для запланированного резервного копирования?** Планируйте резервное копирование, когда система практически не используется, это ускорит процесс создания резервных копий. Однако не всегда можно осуществить архивирование вне часов пик, поэтому нужно внимательно планировать, когда будут изменяться системные данные.
- **Нужно ли хранить копии за пределами организации?** Хранение копий за пределами организации важно для восстановления систем в случае стихийного бедствия. В безопасном месте также должны храниться копии программного обеспечения, которые понадобятся для восстановления операционных систем.

Практический совет

Целевое время восстановления (Recovery Time objective, RTO) и целевая точка восстановления (Recovery Point Objective, RPO) — важные факторы резервного копирования. RTO представляет собой время восстановления, которое может составить два часа для одного сервера и четыре часа для другого сервера. RPO представляет потенциальную утрату данных, которая в случае с одним сервером может соответствовать одному рабочему дню,

с другим — двум рабочим дням. Среда с высоким RTO — это среда, в которой можно быстро восстановить функциональность сервера после сбоя. Среда с высоким RPO — это среда, в которой восстановленные данные максимально актуальны.

Частота резервных копий всего сервера будет изменяться согласно скорости системы резервного копирования и объема данных, которые нуждаются в резервном копировании. Частота, с которой можно создавать резервные копии, управляет доступными RPO и RTO. Например, в случае с ночными резервными копиями, RPO — один рабочий день, означающий, что любое отключение сервера, вероятно, приведет к потере данных всего рабочего дня. RTO показывает, сколько фактически займет процедура восстановления, и зависит от объема данных, которые нужно восстановить.

Основные типы резервного копирования

Существует много техник архивирования файлов. Используемые техники зависят от типа архивируемых данных, от того, каким будет процесс восстановления, и т. д.

Если просмотреть свойства файла или каталога в Проводнике, можно обнаружить атрибут *"архивный"*. Этот атрибут используется для определения, должен ли тот или иной файл или каталог быть заархивирован. Если атрибут установлен, файл или каталог будет помещен в резервную копию. Могут осуществляться следующие основные типы резервного копирования.

- **Обычная/полная резервная копия.** Все выбранные файлы, независимо от установки атрибута "архивный", будут помещены в резервную копию. После помещения файла в резервную копию атрибут "архивный" очищается. Если файл в дальнейшем будет модифицирован, атрибут снова будет установлен. Это означает, что в следующий раз файл будет нуждаться в архивировании.
- **Копирование.** Все выбранные файлы, независимо от установки атрибута "архивный", будут помещены в резервную копию. Отличие от предыдущего метода в том, что атрибут "архивный" не модифицируется. Это позволяет использовать другие типы резервного копирования позже.
- **Дифференцированное (выборочное) резервное копирование.** Разработано для архивирования копий файлов, которые изменились с последнего обычного резервного копирования. Наличие атрибута "архивный" указывает, что файл был изменен и нуждается в архивировании. Архивируются только файлы с этим атрибутом. Однако после создания резервной копии сам атрибут "архивный" не изменяется, что позволяет выполнить другие типы резервного копирования позже.
- **Добавочное резервное копирование.** Разработано, чтобы архивировать файлы, которые изменились с момента последнего нормального или добавочного резервного копирования. Наличие атрибута "архивный" указывает, что файл был изменен и нуждается в архивировании. Архивируются только файлы с этим атрибутом. После помещения файла в резервную копию атрибут "архивный" очищается. Если файл в дальнейшем будет модифицирован, атрибут снова будет установлен, указывая, что в следующий раз файл нуждается в архивировании.
- **Ежедневное резервное копирование.** Предназначено для архивирования файлов по дате последнего изменения. Если файл был изменен в день создания резервной копии, он архивируется. Данный способ не изменяет атрибут "архивный".

Обычно полные резервные копии создаются раз в неделю и дополняются ежедневными, дифференцированным или добавочным резервным копированием. Также можно создавать расширенную резервную копию каждый месяц или каждый квартал и включать в нее дополнительные файлы, которые не архивируются регулярно.

> ***Совет***
>
> Часто могут пройти недели или месяцы, прежде чем кто-либо заметит, что необходимый файл или источник данных отсутствует. Это не означает, что данный файл не важен. Несмотря на то, что некоторые типы данных используются не часто, они все еще востребованы. Поэтому не забывайте, что нужно также создавать дополнительные наборы резервных копий ежемесячно и/или ежеквартально, чтобы гарантировать восстановление всех необходимых данных.

Дифференцированное и добавочное резервное копирование

Разница между дифференцированным и добавочным резервным копированием очень важна. Чтобы понимать, в чем она заключается, рассмотрим табл. 11.1. Как видите, при дифференцированном резервном копировании архивируются все файлы, которые были изменены с момента полной резервной копии (это означает, что размер дифференцированной резервной копии увеличивается со временем). При добавочном резервном копировании копируются только те файлы, которые были изменены с последнего полного или добавочного резервного копирования (т. е. размер добавочной резервной копии обычно меньше, чем размер полной резервной копии).

Таблица 11.1. *Добавочное и дифференцированное резервное копирование*

День недели	**Еженедельная полная резервная копия с дифференцированным резервным копированием**	**Еженедельная полная резервная копия с добавочным резервным копированием**
Воскресенье	Создается полная резервная копия	Создается полная резервная копия
Понедельник	Дифференцированная резервная копия (далее ДРК) содержит все изменения, начиная с воскресенья	Добавочная резервная копия (далее ДРК) содержит все изменения, начиная с воскресенья
Вторник	ДРК содержит все изменения, начиная с воскресенья	ДРК содержит все изменения, начиная с понедельника
Среда	ДРК содержит все изменения, начиная с воскресенья	ДРК содержит все изменения, начиная со вторника
Четверг	ДРК содержит все изменения, начиная с воскресенья	ДРК содержит все изменения, начиная со среды
Пятница	ДРК содержит все изменения, начиная с воскресенья	ДРК содержит все изменения, начиная с четверга
Суббота	ДРК содержит все изменения, начиная с воскресенья	ДРК содержит все изменения, начиная с пятницы

После того как будет определено, какие данные нужно архивировать и как часто, можно выбрать устройства для создания резервных копий и носители данных, которые поддерживаются этими устройствами. Эти вопросы рассмотрены в следующем разделе.

Выбор устройств и носителей данных для резервного копирования

Для резервного копирования доступно множество утилит. Некоторые — быстрые и дорогие. Другие — медленные, но очень доступные. Решение, подходящее для конкретной организации, зависит от многих факторов, в том числе от следующих.

- *Емкость.* Какой объем данных нужно архивировать? Сможет ли оборудование выдержать требуемую нагрузку в приемлемое время?
- *Надежность.* Надежность оборудования для резервного копирования и носителей данных. Можно ли пожертвовать надежностью ради времени или бюджета?
- *Расширяемость.* Расширяемость решения для резервного копирования. Будет ли выбранное решение соответствовать потребностям организации при ее расширении?
- *Скорость.* Скорость архивирования и восстановления данных. Можно ли пожертвовать скоростью с сервером или временем простоя службы, чтобы уменьшить затраты?
- *Стоимость.* Стоимость решения для резервного копирования. Соответствует ли решение выделенному бюджету?

Общие решения для резервного копирования

Емкость, надежность, расширяемость, скорость и стоимость — факторы, управляющие планом резервного копирования. Если администратор понимает, как эти факторы влияют на организацию, он должен выбрать подходящее решение для резервного копирования. Рассмотрим часто используемые решения для резервного копирования.

- *Стримеры* (ленточные накопители) — наиболее часто используемые устройства для резервного копирования. Для хранения данных стримеры используют картриджи с магнитной лентой. Магнитная лента относительно недорогая, но ненадежная. Ленты могут повредиться или стереться. Они также могут потерять информацию, пролежав долгое время. Средняя емкость картриджей для стримера составляет от 24 до 160 Гбайт. По сравнению с другими решениями для резервного копирования стримеры очень медленные. Но у них есть один коммерческий аргумент — низкая стоимость.
- *Накопители на цифровой аудиопленке* (Digital Audio Tape, DAT). DAT-устройства быстро заменили стандартные стримеры. Сегодня доступно много разных DAT-форматов. Наиболее часто используются форматы DLT (Digital Linear Tape) и SDLT (Super DLT). Стандарты SDLT 320 и 600 позволяют записывать 160 и 300 Гбайт несжатой информации соответственно (320 и 600 Гбайт сжатых данных). В больших организациях используется технология LTO (Linear Tape Open). LTO-3, LTO-4 и LTO-5 позволяют записывать 400, 800 и 1500 Гбайт несжатой информации соответственно (сжатой информации — в два раза больше).
- *Системы автоматической загрузки кассет.* Такие системы базируются на магазинах кассет для создания расширенных томов резервного копирования, способных удовлетворить потребности предприятия в большой емкости. При использовании

автоматической загрузки кассеты в магазине автоматически изменяются по мере необходимости при резервном копировании или восстановлении данных. Большинство систем автозагрузки используют DAT-кассеты, отформатированные как DLT, SDLT или LTO. Типичные DLT-устройства могут записывать до 45 Гбайт информации в час, и можно еще повысить скорость, купив библиотеку с несколькими накопителями. Таким образом, можно записать несколько лент одновременно. Большинство SDLT- и LTO-устройств могут записывать информацию со скоростью 100 Гбайт/ч, а используя несколько накопителей, можно записывать сотни гигабайт в час. В качестве примера для предприятия можно привести решение, использующее 16 LTO-накопителей, достигающее скорости передачи данных более 13,8 Тбайт/час и позволяющее хранить до 500 лент общей емкостью до 800 Тбайт.

- *Жесткие диски* предоставляют один из быстрейших способов резервного копирования и восстановления файлов. С их помощью за минуты можно выполнить те операции, которые в случае со стримерами занимают часы. Когда нужно быстро восстанавливать данные, нет ничего лучше жесткого диска. Недостаток — относительно высокая стоимость по сравнению с системами на магнитной ленте.
- *Системы резервного копирования на основе дисков.* Такие системы предоставляют полные решения резервного копирования и восстановления с использованием больших массивов дисков для достижения высокой производительности. Высокая надежность достигается при использовании избыточных массивов независимых дисков (RAID) для обеспечения избыточности и отказоустойчивости. Типичные системы используют технологию виртуальной библиотеки так, что Windows видит их как системы автозагрузки кассет. Это существенно упрощает работу с такой системой. Например, в решении для предприятия может быть 128 виртуальных дисков и 16 виртуальных библиотек на один узел с общей емкостью хранилища 7,5 Тбайт на один узел. При полной загрузке это решение может хранить до 640 Тбайт информации и передавать данные со скоростью 17,2 Тбит/ч.

> ***Примечание***
>
> Диски и системы на основе дисков могут использоваться между серверами наряду с системами автозагрузки кассет. Архивирование серверов сначала осуществляется на диски (потому что это очень быстро по сравнению с лентой), а автозагрузчик кассет применяется для остального резервного копирования данных предприятия. Наличие данных на кассетах упрощает ротацию резервных копий в удаленном хранилище. Однако резервные копии на магнитную ленту все более и более вытесняются дисковыми системами резервных копий. Если резервное копирование выполняется на массивы дисков, можно переместить данные за пределы предприятия с помощью репликации данных на второй массив в альтернативном дата-центре.

Перед использованием устройства резервного копирования нужно установить его. После установки самих устройств (кроме стандартного стримера и DAT-стримера) нужно установить драйверы устройства и его контроллера (если необходимо).

Покупка и использование носителей резервной копии

Выбор устройства для резервного копирования является важным шагом к реализации плана резервного копирования и восстановления. Но также нужно купить кассеты, диски для реализации плана. Количество кассет и дисков зависит от того, какой объем

данных надо архивировать и как часто нужно создавать резервные копии и расширенные наборы данных.

Типичный способ использования кассет для резервного копирования заключается в настройке расписания вращения между двумя или более наборами кассет. Идея заключается в том, что увеличивается долговечность кассеты, уменьшается ее использование и одновременно сокращается число кассет. При этом под рукой будут все необходимые данные.

Одно из наиболее часто используемых расписаний вращения кассеты — десятикассетное вращение. В этом случае используются 10 кассет, разделенных на два набора по 5 кассет в каждом (одна кассета для каждого рабочего дня). Первый набор кассет используется на одной неделе, а второй — на следующей неделе. В пятницу запланировано полное резервное копирование. С понедельника по четверг — добавочное резервное копирование. Если добавить третий набор кассет, можно каждую неделю отправлять один из наборов кассет во внешнее хранилище.

Расписание с десятью кассетами подходит для пятидневной рабочей недели. В среде 24/7 (круглосуточно, 7 дней в неделю) нужно добавить дополнительные кассеты для субботы и воскресенья. В этом случае используйте два набора по 7 кассет (14 кассет всего). Полное резервное копирование запланируйте на воскресенье, а с понедельника по субботу — добавочное резервное копирование.

Жесткие диски стали более доступными и применяются во многих организациях вместо магнитной ленты. Диски также позволяют использовать расписание вращения, подобное тому, которое используется с кассетами. Однако нужно модифицировать способ вращения дисков в соответствии с объемом архивируемых данных. Ключевая идея состоит в периодическом перемещении дисков во внешнее хранилище.

Выбор утилиты для резервного копирования

Для использования в Windows Server 2012 R2 доступно множество решений резервного копирования и восстановления. При выборе средства резервного копирования следует помнить о типах резервного копирования и типах архивируемых данных. ОС Windows Server 2012 R2 содержит следующие средства резервного копирования и восстановления.

- **Система архивации данных Windows Server** (Windows Server Backup) — базовое и простое в использовании средство резервного копирования и восстановления. Когда этот компонент установлен на сервере, можно открыть эту утилиту из меню **Средства** (Tools) в диспетчере серверов.
- **Средства архивирования командной строки** — набор команд для резервного копирования и восстановления средствами утилиты командной строки Wbadmin. Запускать Wbadmin нужно из командной строки с правами администратора. Введите `wbadmin /?` для вывода полного списка поддерживаемых команд. Также доступны командлеты Windows PowerShell для управления резервными копиями.
- **Модуль резервного копирования Windows Server для Windows PowerShell.** Набор командлетов для резервного копирования и восстановления, доступных через Windows PowerShell. Данные командлеты можно запускать из командной строки

Windows PowerShell. Для получения полного списка доступных командлетов введите команду `get-help *wb*`.

- **Служба Microsoft Online Backup.** Данная служба — это дополнение, которое может быть загружено и установлено в **Системе архивации данных Windows Server** для запланированного резервного копирования с сервера в облачный интернет-сервис. Оперативные резервные копии возможны только для фиксированных NTFS-томов, которые не используют шифрование BitLocker. Тома не могут быть общими ресурсами и обязательно должны быть настроены для чтения/записи.
- **Восстановление системы.** Можно восстановить сервер, используя средство **Восстановление системы**, если нельзя получить доступ к опциям, предоставленным производителем сервера.

> ***Примечание***
>
> Система архивации данных Windows Server и средства резервного копирования командной строки доступны только для управления резервными копиями после установки компонента **Система архивации данных Windows Server**.

Чаще всего будет применяться утилита **Система архивации данных Windows Server**. Ее можно использовать, чтобы создать полную резервную копию или осуществить резервное копирование путем обычного копирования. Эту утилиту нельзя применять для дифференцированного резервного копирования. **Система архивации данных Windows Server** использует **Службу теневого копирования томов** (Volume shadow copy service, VSS) для быстрого создания резервной копии операционной системы, файлов и папок, томов диска. После создания первой полной резервной копии можно настроить **Систему архивации данных Windows Server** для автоматического создания полной или добавочной резервной копии на рекурсивной основе.

Для использования утилиты **Система архивации данных Windows Server** нужен отдельный, выделенный носитель для хранения архивов запланированных резервных копий. Можно создавать резервные копии на внешних и на внутренних дисках, DVD, общих папках. Хотя можно восстановить целые тома из DVD-дисков, нельзя восстанавливать отдельные файлы, папки или данные приложений из резервных копий на DVD.

> ***Примечание***
>
> При работе с утилитой **Система архивации данных Windows Server** нельзя использовать стример. Если нужно создавать резервные копии на кассетах, применяйте стороннюю утилиту резервного копирования.

Утилиту **Система архивации данных Windows Server** можно использовать для простого восстановления отдельных папок и файлов. Вместо того чтобы вручную восстанавливать файлы из многочисленных резервных копий, если файлы сохранены в добавочных резервных копиях, можно восстановить папки и файлы, выбрав дату резервной копии, которую нужно восстановить. Система архивации данных также работает со средствами восстановления Windows, что делает восстановление операционной системы проще. Можно восстановить резервную копию на тот же сервер или на новый сервер, на котором вообще нет операционной системы. Поскольку утилита **Система архивации данных Windows Server** использует VSS, можно легко архивировать дан-

ные совместимых приложений, например Microsoft SQL Server и Windows SharePoint Services.

Система архивации данных Windows Server также содержит автоматическое управление диском. Можно запустить резервное копирование на несколько дисков с вращением путем простого добавления диска в качестве запланированного размещения резервной копии. Как только настроите диск в качестве целевого приемника запланированного размещения резервной копии, утилита **Система архивации данных Windows Server** автоматически будет управлять хранилищем, поэтому больше не нужно беспокоиться о том, что исчерпается дисковое пространство. Утилита использует пространство, выделенное для старых резервных копий, чтобы записать новые резервные копии. Чтобы можно было заранее установить дополнительные хранилища, утилита отображает текущие резервные копии и информацию о заполнении диска.

Основы резервного копирования данных

В Windows Server 2012 R2 для создания резервных копий применяется утилита **Система архивации данных Windows Server**. Ее можно использовать для архивации файлов и папок, восстановления заархивированных файлов и папок, создания снимков состояния системы для резервного копирования и восстановления, а также запланировать автоматическое резервное копирование.

Установка утилит резервного копирования и восстановления Windows

Утилиты резервного копирования и восстановления Windows Server доступны во всех выпусках Windows Server 2012 R2. Однако нельзя установить графические компоненты этих утилит при установке основных серверных компонентов (Server Core) Windows Server 2012 R2. На таких серверах нужно использовать командную строку для управления резервным копированием или запускать удаленный сеанс с другого компьютера.

Установить утилиты резервного копирования и восстановления Windows можно с помощью следующих действий:

1. В диспетчере серверов в меню **Управление** выберите команду **Добавить роли и компоненты**. Будет запущен мастер добавления ролей и компонентов (Add Roles and Features Wizard). Если мастер отобразит страницу **Перед началом работы**, прочитайте вступительный текст и затем нажмите кнопку **Далее**.
2. На странице **Выбор типа установки** по умолчанию выбран переключатель **Установка ролей или компонентов**. Нажмите кнопку **Далее**.
3. На странице **Выбор целевого сервера** можно указать, где нужно установить роли и компоненты — на сервере или на виртуальном жестком диске. Выберите либо сервер из пула серверов, либо сервер, на котором можно смонтировать виртуальный жесткий диск (VHD). Если добавляете роли и компоненты на VHD, нажмите кнопку **Обзор**, а затем используйте окно **Обзор виртуальных жестких дисков** (Browse for virtual hard disks) для выбора VHD. Когда будете готовы продолжить, нажмите кнопку **Далее**.

4. На странице **Выбор компонентов** установите флажок **Система архивации данных Windows Server** (Windows Server Backup). Нажмите кнопку **Далее**.
5. Нажмите кнопку **Установить**. Когда мастер закончит установку выбранных компонентов, нажмите кнопку **Закрыть**. Начиная с этого момента, будет доступна утилита **Система архивации данных Windows Server**, а также соответствующие утилиты командной строки.

Введение в *Систему архивации данных Windows Server*

Для запуска утилиты **Система архивации данных Windows Server** выберите соответствующую опцию из меню **Средства** в диспетчере серверов. Альтернативно, можно также запустить исполнимый файл Wbadmin.msc.

После запуска утилиты будет отображено сообщение об оперативном резервном копировании. Если желаете использовать оперативное (онлайн) резервное копирование, нужно подписаться на этот сервис, зарегистрировать сервер и загрузить агента службы Microsoft Online Backup. Запустить этот процесс можно, нажав кнопку **Продолжить** (Continue) в узле **Система архивации данных Windows Server**.

В утилите **Система архивации данных Windows Server** (рис. 11.1) выберите узел **Локальная архивация** (Local Backup) для работы с резервными копиями. При первом использовании утилиты будет отображено предупреждение, что для данного компьютера не настроена архивация. Чтобы избавиться от этого предупреждения, создайте однократную резервную копию, используя команду **Однократная архивация** (Backup Once) из меню **Действие** (Action), или запланируйте создание архивации с помощью функции **Расписание архивации** (Backup Schedule).

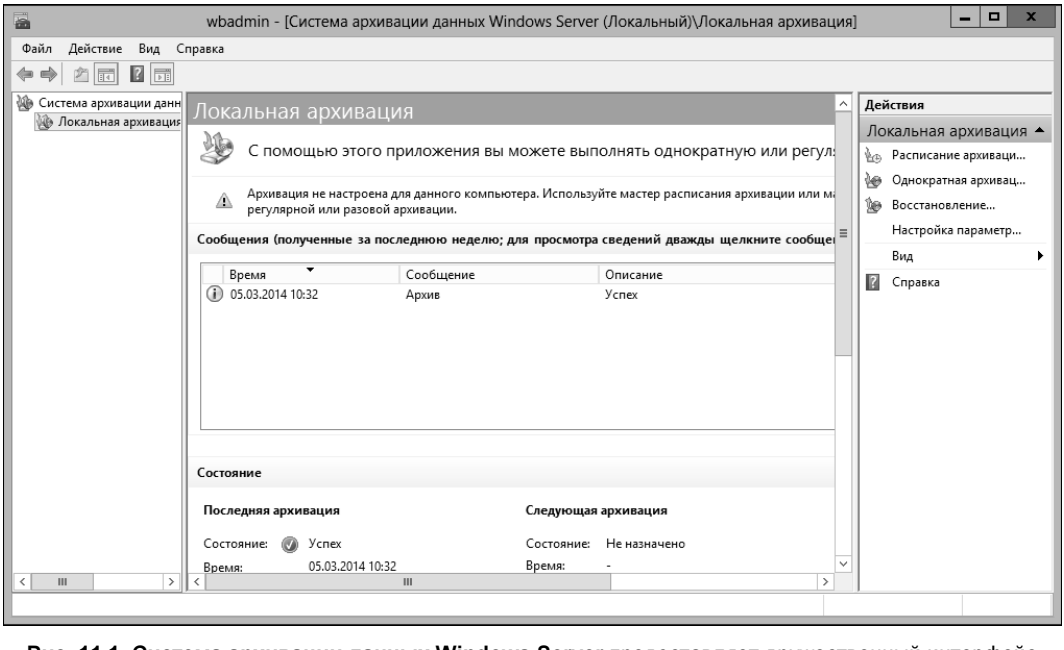


Рис. 11.1. Система архивации данных Windows Server предоставляет дружественный интерфейс для резервного копирования и восстановления

Чтобы выполнить резервное копирование и операции восстановления, у пользователя должны быть определенные разрешения и права. Такие разрешения есть у групп **Администраторы** и **Операторы архива**: пользователи этих групп имеют право резервировать и восстанавливать файлы любого типа, независимо от того, кому они принадлежат и какие права установлены на файле. Владельцы файла и те, кому был дан контроль над файлами, также могут архивировать файлы, но они могут архивировать только свои файлы и те, для которых у них есть разрешения **Чтение**, **Чтение и выполнение**, **Изменение** или **Полный доступ**.

> ***Примечание***
>
> Помните, что хотя локальные учетные записи могут работать только с локальными системами, у учетных записей домена есть привилегии, распространяющиеся на весь домен. Поэтому члены локальной группы **Администраторы** могут работать лишь с файлами на локальной системе, а члены группы **Администраторы домена** — с файлами по всему домену.

Система архивации данных Windows Server предоставляет расширения для работы со следующими специальными типами данных.

- **Данные состояния системы** — содержит важные системные файлы, необходимые для восстановления локальной системы. У всех компьютеров есть системные данные, которые должны архивироваться в дополнение к другим файлам для восстановления работы системы.
- **Данные приложений** — содержит файлы данных приложений. Нужно архивировать данные, если необходимо полностью восстановить приложения в случае сбоя. Система архивации данных создает резервные копии данных приложений, используя VSS.

Система архивации данных Windows Server позволяет осуществлять полное резервное копирование, архивирование путем копирования и добавочное резервное копирование. Хотя можно запланировать полное резервное или добавочное копирование, которое будет выполняться один или несколько раз в день, нельзя использовать эту функцию, чтобы создать отдельные расписания для выполнения и полного, и добавочного резервного копирования. Нельзя выбрать день или дни недели для выполнения резервного копирования. Это происходит потому, что у каждого сервера есть единственное главное расписание, которое настроено на запуск один или несколько раз ежедневно. Если у администрируемых серверов есть основное расписание, можно обойти это ограничение, настроив утилиту **Система архивации данных Windows Server**, чтобы выполнить ежедневное добавочное резервное копирование, а затем создать задачу планировщика Windows, который запустит Wbadmin для создания полной резервной копии в нужный день недели или месяца.

При использовании утилиты **Система архивации данных Windows Server** первая резервная копия сервера — это всегда полная копия. Это происходит потому, что процесс создания полной резервной копии сбрасывает бит "архивный" на файлах, так что потом утилита может отслеживать файлы, которые были обновлены. Какое резервное копирование (полное или добавочное) будет выполнено, зависит от настроек производительности.

Настроить параметры производительности можно с помощью следующих действий:

1. Запустите утилиту **Система архивации данных Windows Server**. На панели **Действия** или в меню **Действие** выберите команду **Настройка параметров производительности** (Configure Performance Settings). Откроется окно **Оптимизация производительности архивации** (Optimize Backup Performance), показанное на рис. 11.2.

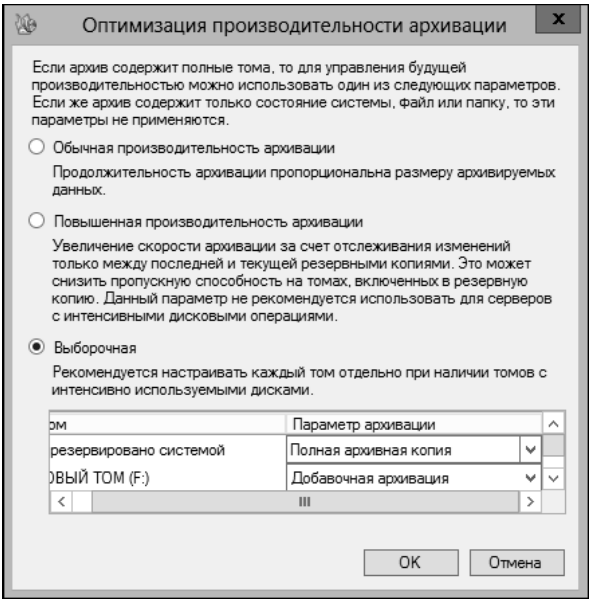


Рис. 11.2. Настройка параметров резервного копирования

2. Выберите одну из следующих опций и нажмите кнопку **OK**:
   - **Обычная производительность архивации** (Normal backup performance) — для осуществления полного резервного копирования всех присоединенных дисков;
   - **Повышенная производительность архивации** (Faster backup performance) — для добавочного резервного копирования всех присоединенных дисков;
   - **Выборочная** (Custom). В предоставленном списке укажите, какую архивацию нужно производить — полную или добавочную для отдельных дисков.
3. После настройки параметров производительности можно начать архивацию, выбрав команду **Однократная архивация** (Backup Once) из меню **Действие** или из панели **Действия**.

Знакомство с утилитами резервного копирования командной строки

Программа Wbadmin — аналог утилиты **Система архивации данных Windows Server** для командной строки. Можно использовать Wbadmin для управления всеми аспектами резервного копирования, которые можно осуществить в утилите **Система архивации**

данных Windows Server. Это означает, что можно использовать эту утилиту для управления резервным копированием и восстановлением.

После установки утилит командной строки для резервного копирования и восстановления, как было описано ранее, можно использовать Wbadmin для управления архивацией и восстановлением. Wbadmin находится в каталоге *%SystemRoot%*\System32\. Этот каталог используется командной строкой по умолчанию, поэтому при вызове Wbadmin не нужно добавлять его. Можно запустить Wbadmin так:

1. Откройте командную строку с правами администратора. Один из способов сделать это — ввести `cmd` в поле поиска приложений, щелкнуть правой кнопкой мыши на элементе **Командная строка** (Command Prompt) в списке и выбрать команду **Запустить от имени администратора** (Run as administrator).
2. В окне **Командная строка** (Command Prompt) введите текст команды или запустите сценарий Wbadmin.

У Wbadmin есть множество связанных команд, представленных в табл. 11.2.

Таблица 11.2. *Команды управления Wbadmin*

Команда	Описание
`DELETE SYSTEMSTATEBACKUP`	Удаляет один или несколько архивов состояния системы
`DISABLE BACKUP`	Отключает выполнение архивации по расписанию
`ENABLE BACKUP`	Включает или изменяет расписание ежедневной архивации
`GET DISKS`	Выдает список активных дисков локального компьютера. Выводится название производителя, тип, номер диска, GUID, общее пространство, использованное пространство и связанные тома
`GET ITEMS`	Отображает список элементов, содержащихся в архиве
`GET STATUS`	Отображает состояния текущей операции
`GET VIRTUAL MACHINES`	Выводит список настроенных в данный момент виртуальных машин
`GET VERSIONS`	Выводит сведения о резервных копиях, которые можно восстановить из указанного расположения, в том числе время резервной копии и ее назначение
`START BACKUP`	Запускает выполнение однократной архивации. Если не заданы параметры и включено расписание создания резервных копий, процесс резервного копирования использует параметры, заданные для запланированной архивации
`START RECOVERY`	Запускает восстановление томов, приложений или файлов с помощью определенных параметров
`START SYSTEMSTATEBACKUP`	Запускает создание архива состояния системы, используя заданные параметры
`START SYSTEMSTATERECOVERY`	Запускает восстановление состояния системы, используя указанные параметры
`STOP JOB`	Останавливает текущую задачу по архивированию или восстановлению. Остановленные задачи не могут быть продолжены с места остановки

При работе с Wbadmin можно получить справку по доступным командам:

- для просмотра всех команд управления введите `wbadmin /?` в командной строке;
- для просмотра синтаксиса определенной команды введите `wbadmin` *команда* `/?`, где *команда* — имя интересующей команды управления, например, `wbadmin stop job /?`.

Почти каждая команда Wbadmin принимает параметры и конкретные значения параметров, которые определяют то, с чем нужно работать. Чтобы понять, как это работает, рассмотрим следующий пример:

```
wbadmin get versions [-backupTarget:{VolumeName | NetworkSharePath}]
[-machine:BackupMachineName]
```

Параметры, заключенные в квадратные скобки (`-backupTarget` и `-machine`), являются необязательными. Поэтому для получения информации о резервных копиях локального компьютера можно ввести команду:

```
wbadmin get versions
```

Для получения информации о резервных копиях, хранящихся на диске F:, введите эту команду:

```
wbadmin get versions -backupTarget:f:
```

Или же можно получить информацию о резервных копиях, хранящихся на диске F: компьютера Server96:

```
wbadmin get versions -backupTarget:f: -machine:server96
```

Множество команд Wbadmin использует параметры `-backupTarget` и `-machine`. Первый параметр задает хранилище резервных копий, с которым нужно работать, и может быть выражен как имя локального тома (F:) или сетевой путь (\\FileServer32\backups\Server85). Параметр `-machine` определяет компьютер, который используется для архивирования и восстановления.

Работа с командами Wbadmin

Команды Wbadmin применяются для управления конфигурацией резервного копирования администрируемых серверов. Эти команды работают с определенным набором параметров. В следующих разделах представлен обзор доступных команд и их наиболее часто используемый синтаксис.

Команды общего назначения

Следующие команды общего назначения предоставляют информацию о резервных копиях и системе.

- `GET DISKS` — выводит диски, подключенные в данный момент к локальному компьютеру. Выводится название производителя, тип, номер диска, GUID, общее пространство, использованное пространство и связанные тома.

  ```
  wbadmin get disks
  ```

- **GET ITEMS** — отображает список элементов, содержащихся в определенном архиве.

```
wbadmin get items -version:VersionIdentifier [-backupTarget:{VolumeName |
NetworkSharePath}] [-machine:BackupMachineName]
```

- **GET STATUS** — отображает состояние текущей операции.

```
wbadmin get status
```

- **GET VERSIONS** — выводит сведения о резервных копиях, которые можно восстановить из указанного расположения, в том числе время резервной копии и ее назначение.

```
wbadmin get versions [-backupTarget:{ VolumeName | NetworkSharePath}]
[-machine:BackupMachineName]
```

Команды управления резервной копией

Можно управлять резервными копиями и их конфигурацией, используя следующие команды.

- **DELETE SYSTEMSTATEBACKUP** — удаляет один или несколько архивов состояния системы.

```
wbadmin delete systemstateBackup [-backupTarget:{VolumeName}]
[-machine:BackupMachineName]
[-keepVersions:NumberOfBackupsToKeep | -version:VersionIdentifier |
-deleteOldest]
[-quiet]
```

- **DISABLE BACKUP** — отключается выполнение архивации по расписанию.

```
wbadmin disable backup [-quiet]
```

- **ENABLE BACKUP** — включает или изменяет расписание ежедневной архивации.

```
wbadmin enable backup [-addTarget:{ BackupTargetDisk}]
[-removeTarget:{BackupTargetDisk}]
[-schedule:TimeToRunBackup]
[-include:VolumesToInclude]
[-allCritical]
[-quiet]
```

- **START BACKUP** — запускает выполнение однократной архивации. Если не заданы параметры и включено расписание создания резервных копий, процесс резервного копирования использует параметры, заданные для запланированной архивации.

```
wbadmin start backup [-backupTarget:{ TargetVolume | TargetNetworkShare}]
[-include:VolumesToInclude]
[-allCritical]
[-noVerify]
[-user:username]
[-password:password]
[-inheritAcl:InheritAcl]
[-vssFull]
[-quiet]
```

- **STOP JOB** — останавливает текущую задачу по архивированию или восстановлению. Остановленные задачи не могут быть продолжены с места остановки.

```
wbadmin stop job [-quiet]
```

Команды управления восстановлением

Можно восстановить компьютеры и данные, используя следующие команды.

- **START RECOVERY** — запускает восстановление томов, приложений или файлов с использованием определенных параметров.

```
wbadmin start recovery -version:VersionIdentifier
-items: VolumesToRecover | AppsToRecover | FilesOrFoldersToRecover
-itemType:{volume | app | file}
[-backupTarget:{VolumeHostingBackup | NetworkShareHostingBackup}]
[-machine:BackupMachineName]
[-recoveryTarget:TargetVolumeForRecovery | TargetPathForRecovery]
[-recursive]
[-overwrite:{Overwrite | CreateCopy | skip}]
[-notRestoreAcl]
[-skipBadClusterCheck]
[-noRollForward]
[-quiet]
```

- **START SYSTEMSTATEBACKUP** — запускает создание архива состояния системы, используя заданные параметры.

```
wbadmin start systemstateBackup -backupTarget:{VolumeName} [-quiet]
```

- **START SYSTEMSTATERECOVERY** — запускает восстановление состояния системы, используя указанные параметры.

```
wbadmin start systemstateRecovery -version:VersionIdentifier
-showSummary
[-backupTarget:{VolumeName | NetworkSharePath}]
[-machine:BackupMachineName]
[-recoveryTarget:TargetPathForRecovery]
[-authSysvol]
[-quiet]
```

Резервное копирование сервера

Для каждого сервера, резервное копирование которого планируется осуществлять, нужно определить, какие тома будут архивироваться и будут ли в резервные копии включаться данные состояния системы и данные приложений (или оба типа данных). Хотя можно вручную архивировать на общие тома и DVD-носители, нужен отдельный, выделенный диск для выполнения запланированных резервных копий. После настройки диска для запланированных заданий, утилиты резервного копирования автоматически управляют использованием дискового пространства и автоматически удаляют старые резервные копии при создании новых. Необходимо периодически проверять этот диск и убедиться, что резервные копии создаются, как и ожидалось, а расписание резервного копирования соответствует текущим потребностям.

При создании или планировании резервных копий нужно определить, какие тома следует архивировать, и выбрать способы, которыми можно будет восстановить серверы и данные. Есть следующие варианты.

- **Весь сервер (все тома с данными приложений).** Выполняет резервное копирование всех томов с данными приложений, что позволяет полностью восстановить сер-

вер, включая его состояние системы и данные приложений. Поскольку архивируются файлы, системное состояние и данные приложений, можно будет полностью восстановить сервер только с использованием инструментов резервного копирования Windows.

- **Весь сервер (все тома, но без данных приложений).** Архивируются все тома без данных приложений, если нужно восстановить сервер и его приложения отдельно. Средства резервного копирования Windows выполняют архивацию сервера, но при этом исключаются расположения, содержащие сами приложения и данные приложений. Создать резервную копию приложений и их данных можно с помощью сторонних инструментов или инструментов, встроенных в приложения. Можно полностью восстановить сервер посредством утилит резервного копирования Windows, а затем использовать стороннюю утилиту для восстановления приложений и их данных.
- **Критические тома/восстановление исходного состояния системы.** Выполняет резервное копирование только критических томов, если нужно восстановить лишь операционную систему.
- **Некритические тома.** Резервное копирование отдельных томов, если нужно восстановить файлы, приложения и их данные только из этих томов.

Также нужно указать место назначения архивации. Помните следующее при выборе места назначения.

- При использовании внутреннего жесткого диска для хранения резервных копий существуют ограничения в способе восстановления системы. Можно восстановить данные из тома, но нельзя восстановить всю структуру диска.
- При использовании внешнего жесткого диска для хранения резервных копий диск будет выделен для хранения резервных копий и больше не будет виден в Проводнике. При выборе этой опции диск (или диски) будет отформатирован с удалением всех записанных на нем данных.
- При использовании удаленной общей папки для хранения резервных копий имеющаяся резервная копия будет перезаписана каждый раз при создании новой резервной копии. Не выбирайте эту опцию, если нужно хранить несколько резервных копий для каждого сервера.
- При использовании съемного носителя или DVD для хранения резервных копий можно архивировать тома только полностью, нельзя архивировать приложения или отдельные файлы. Минимальный размер носителя должен быть 1 Гбайт.

В следующих разделах мы рассмотрим техники резервного копирования. Процедуры архивирования с помощью утилит **Системы архивации данных Windows Server** и Wbadmin аналогичны.

Настройка запланированных резервных копий

Настроить автоматическое запланированное резервное копирование в **Системе архивации данных Windows Server** можно с помощью следующих действий:

1. В утилите **Система архивации данных Windows Server** выберите команду **Расписание архивации** из меню **Действие** или панели **Действия**. Будет запущен мастер расписания архивации (Backup Schedule Wizard). Нажмите кнопку **Далее**.
2. На странице **Конфигурация архивации** (Backup Configuration) обратите внимание на размер резервной копии под опцией **Весь сервер** (Full server), как показано на рис. 11.3. Это место, необходимое для архивации данных сервера, приложений и состояния системы. Для архивации всех томов на сервере выберите переключатель **Весь сервер** и нажмите кнопку **Далее**. Чтобы выбрать тома для архивации, установите переключатель **Настраиваемый** (Custom) и нажмите кнопку **Далее**.

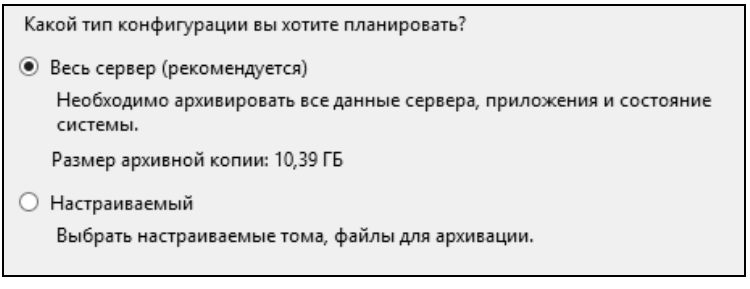


Рис. 11.3. Обратите внимание на размер резервной копии

Примечание

Тома, содержащие файлы операционной системы или приложений, включаются в состав резервной копии по умолчанию и не могут быть исключены. К сожалению, это означает, что если ОС Windows Server 2012 R2 установлена на диск D:, то будет архивироваться и диск C:, поскольку на нем находятся файлы диспетчера загрузки.

3. Если выбрать переключатель **Настраиваемый**, будет отображена страница **Объекты для архивации** (Select Items For Backup). Нажмите кнопку **Добавить элементы** (Add Items). Как показано на рис. 11.4, можно выбрать тома, которые нужно добавить в резервную копию. Если необходимо полностью восстановить систему, отметьте флажок **Восстановление исходного состояния системы** (Bare metal recovery). Выберите опцию **Состояние системы** (System state), если нужно восстановить состояние системы. Если сервер является узлом Hyper-V, выберите отдельные виртуальные серверы, которые вы хотите восстановить. Нажмите кнопку **OK**, а затем кнопку **Далее**.

Совет

После выбора элементов нужно нажать **Дополнительные параметры** (Advanced Settings). Затем можно использовать вкладку **Исключения** (Exclusions), чтобы указать расположения и файлы, которые не должны архивироваться. Также можно использовать параметры вкладки **Параметры VSS** (VSS Settings), чтобы указать тип резервной копии — полная архивация или копирование архива.

4. На странице **Время архивации** (Specify backup time) (рис. 11.5) можно указать, как часто и когда именно должны создаваться резервные копии. Для ежедневного резервного копирования в определенное время выберите переключатель **Раз в день** (Once a day), а затем укажите время начала резервного копирования. Чтобы выпол-

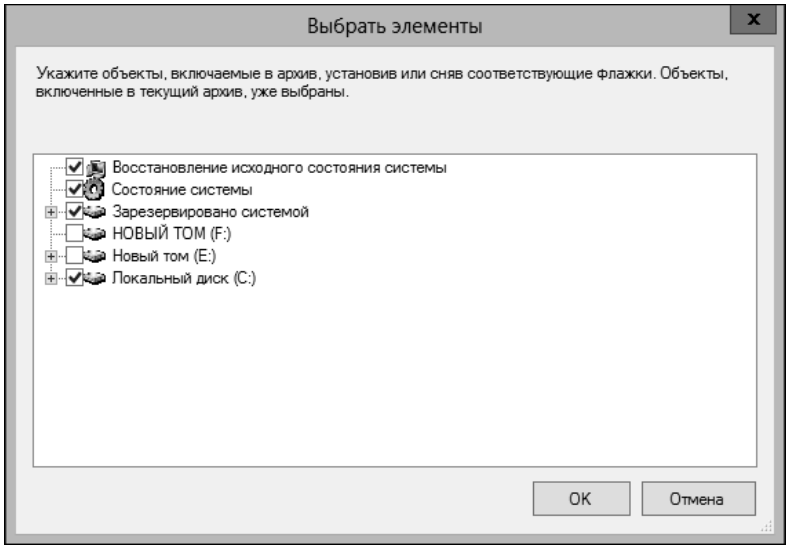


Рис. 11.4. Выберите элементы для включения в резервную копию

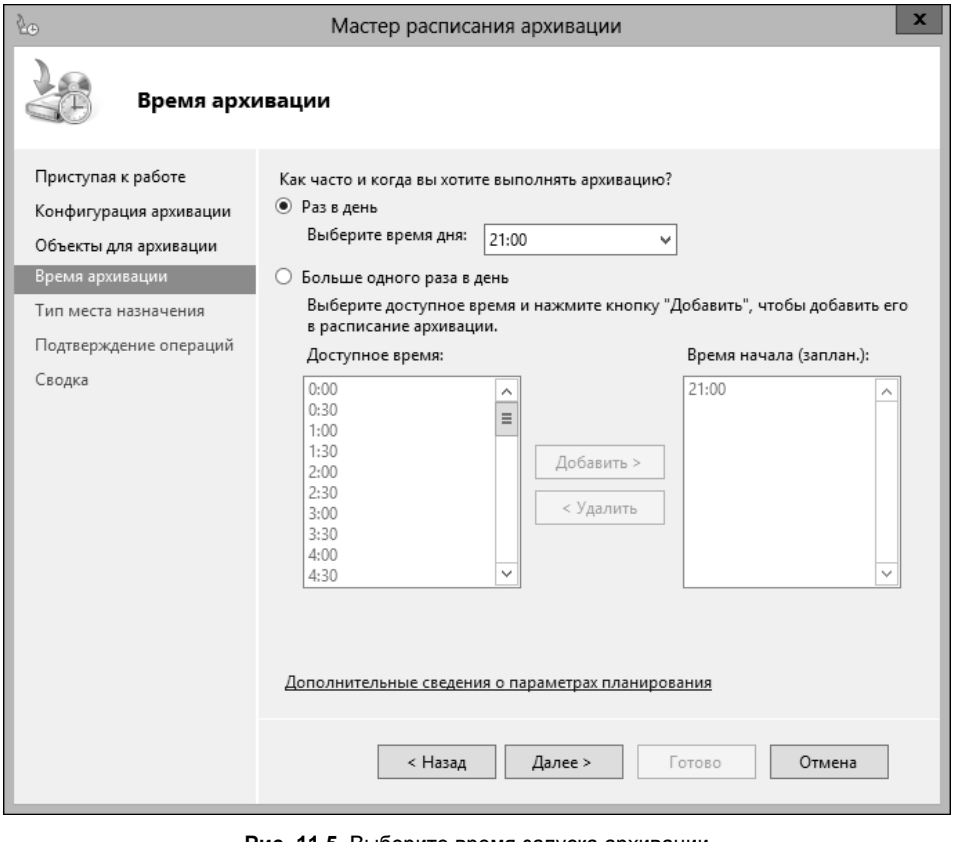


Рис. 11.5. Выберите время запуска архивации

нять резервное копирование несколько раз в день, установите переключатель **Больше одного раза в день** (More than once a day). Затем из списка **Доступное время** (Available time) выберите время и нажмите кнопку **Добавить**, чтобы добавить это время в список **Время начала (заплан.)** (Scheduled time). Повторите этот процесс для каждого времени начала архивации. Нажмите кнопку **Далее**, когда будете готовы продолжить.

5. На странице **Тип места назначения** (Specify destination type) есть следующие опции.
   - **Архивация на жесткий диск для архивов** (Back up to a hard disk that is dedicated for backups) позволяет указать выделенный жесткий диск для резервных копий. Хотя можно использовать несколько дисков для резервных копий, любой выбранный диск будет отформатирован и предназначен только для резервных копий. Эта опция рекомендуется, поскольку она обеспечивает наилучшую производительность. Если выбрали эту опцию, нажмите кнопку **Далее**, выберите диск или диски для использования, а затем нажмите кнопку **Далее** снова.
   - **Архивация на том** (Back up to a volume) позволяет записывать резервные копии на отдельные тома жесткого диска. Поскольку любой выбранный том не будет выделен для резервных копий, также можно использовать их для других нужд. Однако производительность любого выбранного тома будет снижена при создании резервной копии. Если выбрали эту опцию, нажмите кнопку **Далее**, потом с помощью кнопок **Добавить** и **Удалить** выберите тома, которые нужно использовать, а затем нажмите кнопку **Далее**.
   - **Архивация в общую сетевую папку** (Back up to a shared network folder) позволяет указать общую сетевую папку для хранения резервных копий. При выборе этой опции может быть создана только одна резервная копия, поскольку новая резервная копия перезаписывает предыдущую. Если выбрали эту опцию, нажмите кнопку **Далее**. При запросе нажмите кнопку **ОК**. Введите UNC-путь к сетевой папке, например, \\FileServer25\Backups\Exchange. Если нужно, чтобы резервная копия была доступна всем, у кого есть доступ к общей папке, выберите опцию **Наследовать** (Inherit) в области **Управление доступом**. Если нужно ограничить доступ к резервной копии только членам группы **Администраторы** и **Операторы архива**, выберите опцию **Не наследовать** (Not Inherit). Нажмите кнопку **Далее**. После этого введите имя пользователя и пароль для учетной записи, у которой есть право записи в общую папку.
6. На странице **Подтверждение операций** (Confirmation) просмотрите подробности и нажмите кнопку **Готово**. Мастер отформатирует диск. Процесс форматирования займет несколько минут или дольше, в зависимости от размера диска.
7. На странице **Сводка** (Summary) нажмите кнопку **Закрыть**. Теперь создание резервных копий запланировано на администрируемом сервере.

При использовании утилиты Wbadmin можно запланировать резервные копии командой `ENABLE BACKUP`. Эта команда принимает следующие параметры:

- `-addTarget` — устанавливает место хранения резервных копий. Нужно указать GUID диска, который должен использоваться. GUID диска можно узнать с помощью команды `GET DISDKS`;

- `-removeTarget` — указывает место хранения, которое требуется удалить из существующего расписания архивации. Нужно указать GUID диска, который должен использоваться. GUID диска можно узнать с помощью команды `GET DISDKS`;
- `-include` — указывает список включаемых в резервную копию элементов, элементы перечисляются через запятую. Можно задать буквы дисков, точки монтирования томов и идентификаторы GUID;
- `-allCritical` — создает резервную копию всех критических томов операционной системы;
- `-quiet` — указывает, что нужно выполнить команду в "тихом" режиме, без запросов пользователю.

Давайте рассмотрим несколько примеров использования `ENABLE BACKUP`:

- запланированное резервное копирование дисков C: и D: в 18:00 каждый день:

```
wbadmin enable backup -addTarget:{06d88776-0000-0000-0000-000000000000}
-schedule:18:00 -include:c:,d:
```

- запланированное резервное копирование всех томов операционной системы в 6:00 и 18:00:

```
wbadmin enable backup -addTarget:{06d88776-0000-0000-0000-000000000000}
-schedule:06:00,18:00 -allCritical
```

Изменение или остановка запланированного резервного копирования

Изменить или остановить запланированные задания можно так:

1. Запустите утилиту **Система архивации данных Windows Server** и выберите команду **Расписание архивации** из меню **Действие** или панели **Действия**. Будет запущен мастер расписания архивации (Backup Schedule Wizard). Нажмите кнопку **Далее**.
2. На странице **Параметры архивации** (Modify scheduled backup settings) выберите переключатель **Изменить архив** (Modify backup), если нужно добавить или удалить элементы резервной копии, время или цели, а затем выполните действия 3–7 процедуры, описанной в *разд. "Настройка запланированных резервных копий" ранее в этой главе*. Если нужно остановить запланированное задание архивации, выберите переключатель **Остановить архивацию** (Stop backup) и нажмите кнопку **Далее**, а затем нажмите кнопку **Готово**. Для подтверждения действия нажмите кнопку **Да**, а затем кнопку **Закрыть**.

> ***Примечание***
>
> После остановки расписания резервного копирования диски, использующиеся ранее для резервных копий, станут доступными для нормальной эксплуатации. Резервные копии не удаляются с дисков и доступны для восстановления.

Воспользовавшись утилитой Wbadmin, можно изменить запланированные резервные копии с помощью команды `ENABLE BACKUP`. Например, можно использовать ключи `-addTarget` и `-removeTarget` для изменения целевых дисков.

Рассмотрим следующие примеры:

- добавление нового целевого диска для запланированного резервного копирования:

```
wbadmin enable backup -addTarget:{41cd2567-0000-0000-0000-000000000000}
```

- удаление целевого диска из запланированного резервного копирования:

```
wbadmin enable backup -removeTarget:{06d88776-0000-0000-0000-000000000000}
```

- изменение времени запуска и включаемых томов:

```
wbadmin enable backup -schedule:03:00 -include:c:,d:,e:
```

Организация запланированного резервного копирования с помощью Wbadmin

Один из способов создания резервных копий вручную — использовать команду `START BACKUP`. Этой команде нужно передать следующие параметры:

- `-backupTarget` — устанавливает место хранения для резервной копии. Можно указать букву диска или UNC-путь к общей папке на удаленном сервере;
- `-include` — список элементов, разделенных запятыми и включаемых в резервную копию (буквы диска, точки монтирования томов, GUID);
- `-allCritical` — создает резервную копию всех критических томов операционной системы;
- `-inreritAcl` — архивная папка в удаленной общей папке будет наследовать права доступа общей папки. Если не определить этот параметр, архивируемая папка будет доступна только пользователю, заданному параметром `-user`, администраторам и операторам архива;
- `-noVerify` — определяет, нужно ли проверять резервные копии, записанные на съемные носители. Если не указать этот параметр, резервные копии, записанные на сменный носитель, будут проверяться;
- `-password` — позволяет указать пароль, который будет использоваться при подключении к удаленной общей папке;
- `-quiet` — указывает, что нужно выполнить команду в "тихом" режиме, без запросов пользователю;
- `-user` — позволяет указать пароль, который будет использоваться при подключении к удаленной общей папке;
- `-vssFull` — указывает, что нужно выполнить полную резервную копию с использованием VSS. Это действие позволяет убедиться, что все данные сервера и приложений будут заархивированы. Не указывайте этот параметр, если используется стороннее приложение для архивирования данных приложений.

Чтобы понять, как применяется команда `START BACKUP`, рассмотрим следующие примеры:

- создание полной резервной копии сервера:

```
wbadmin start backup -backupTarget:f: -vssfull
```

- создание резервной копии дисков C:, D: на диск F:

```
wbadmin start backup -backupTarget:f: -include:c:,d:
```

- архивирование всех критических томов:

```
wbadmin start backup -backupTarget:f: -allCritical
```

- архивирование томов C:, D: в удаленную общую папку:

```
wbadmin start backup -backupTarget:\\fileserver27\backups -include:c:,
d: -user:williams
```

Если нужно создать расписание для запуска резервного копирования в разное время в разные дни, можно использовать Планировщик заданий (Task Scheduler) для создания нужных задач по выполнению команд для резервного копирования в необходимое время. Чтобы запланировать запуск команд Wbadmin с помощью Планировщика заданий, выполните эти действия:

1. В оснастке **Управление компьютером** выберите узел **Планировщик заданий** (Task Scheduler). По умолчанию оснастка подключается к локальному компьютеру. При необходимости подключитесь к другому компьютеру.
2. Щелкните правой кнопкой мыши на узле **Планировщик заданий** и выберите команду **Создать задачу** (Create task). Будет открыто окно **Создание задачи** (Create Task).
3. На вкладке **Общие** введите имя задачи и установите параметры безопасности для запуска задачи.
   - Если задачу нужно выполнить от имени другого пользователя, нажмите кнопку **Изменить** (Change user or group). В окне **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"** укажите пользователя или группу, от имени которых должна быть выполнена задача, а затем предоставьте необходимые учетные данные.
   - Установите другие параметры запуска. По умолчанию задание запускается только, когда пользователь вошел в систему. Если нужно запустить задачу независимо от того, зарегистрирован пользователь или нет, выберите опцию **Выполнять для всех пользователей** (Run whether user is logged on or not). Также можно запустить задачу с наивысшими привилегиями и настроить ее для предыдущих выпусков Windows.
4. На вкладке **Триггеры** (Triggers) нажмите кнопку **Создать**. В окне **Создание триггера** (New Trigger) выберите вариант **По расписанию** (On a schedule) из списка **Начать задачу** (Begin the task). Используйте предоставленные опции для настройки запуска задачи и затем нажмите кнопку **OK**.
5. На вкладке **Действия** (Actions) выберите действие **Создать** (New). В окне **Создание действия** (New Action) выберите элемент **Запуск программы** (Start a program) из списка **Действие** (Action).
6. В поле **Программа или сценарий** (Program/Script) введите `%windir%\System32\wbadmin.exe`.

7. В поле **Добавить аргументы** (Add arguments) введите команду `START BACKUP` с необходимыми параметрами, например,

```
start backup -backupTarget:f: -include:c:,d:,
e:\mountpoint, \\?\volume{be345a23-32b2-432d-43d2-7867ff3e3432}\
```

8. Нажмите кнопку **OK** для закрытия окна **Создание действия**.
9. На вкладке **Условия** (Conditions) укажите любые условия, ограничивающие запуск или остановку задачи.
10. На вкладке **Параметры** (Settings) выберите дополнительные параметры задачи.
11. Нажмите кнопку **OK** для создания задачи.

Создание резервных копий вручную

Утилита **Система архивации данных Windows Server** может использоваться для создания резервных копий вручную. Для этого выполните следующие действия:

1. Запустите утилиту **Система архивации данных Windows Server**. Из меню **Действие** или из панели **Действия** выберите команду **Однократная архивация** (Backup Once). Будет запущен мастер однократной архивации (Backup Once Wizard).
2. Если нужно архивировать сервер, используя те же опции, что и для запланированного расписания, выберите переключатель **Параметры архивации по расписанию** (Scheduled Backup Options) и нажмите кнопку **Далее**. Затем нажмите кнопку **Архивировать** (Backup), чтобы выполнить архивирование, пропустив последующие шаги.
3. Если нужно использовать другие параметры, выберите переключатель **Другие параметры** и нажмите кнопку **Далее**.
4. На странице **Конфигурация архивации** обратите внимание на размер резервной копии под опцией **Весь сервер**. Это место необходимо для архивирования данных сервера, приложений и состояния системы. Для архивирования всех томов на сервере установите переключатель **Весь сервер** и нажмите кнопку **Далее**. Для архивации выбранных томов на сервере выберите переключатель **Настраиваемый**, а затем нажмите кнопку **Далее**.
5. Если выбран переключатель **Настраиваемый**, будет отображена страница **Объекты для архивации**. Нажмите кнопку **Добавить элементы**. Выберите тома, которые нужно добавить в резервную копию, установите флажки возле томов, которые нужно исключить из резервной копии. Если необходимо полностью восстановить систему, выберите опцию **Восстановление исходного состояния системы**. Нажмите кнопку **OK**, а затем кнопку **Далее**.

> ***Совет***
>
> После выбора элементов нужно нажать кнопку **Дополнительные параметры**. Затем можно использовать вкладку **Исключения**, чтобы указать расположения и файлы, которые не должны архивироваться. Также можно использовать параметры вкладки **Параметры VSS**, чтобы указать тип резервной копии — полная архивация или копирование архива.

6. На странице **Тип места назначения** выполните следующее.
   - Если необходимо архивировать локальные диски, выберите переключатель **Локальные диски** (Local drives) и нажмите кнопку **Далее**. На странице **Место назначения архива** (Backup destination) выберите внутренний или внешний диск или DVD-привод, который будет использоваться в качестве места назначения архива. Когда информация сохраняется на DVD, резервные копии сжимаются, и можно будет восстановить только тома целиком. В результате размер резервной копии на DVD должен быть меньше, чем размер тома сервера.
   - Если нужно записать резервную копию в удаленную общую папку, выберите переключатель **Удаленная общая папка** (Remote Shared Folder) и затем нажмите кнопку **Далее**. На странице **Выбор удаленной папки** (Specify Remote Folder) введите UNC-путь к удаленной папке, например, \\FileServer43\Backups. Если нужно, чтобы резервная копия была видна всем, у кого есть доступ к общей папке, выберите переключатель **Наследовать**. Если нужно ограничить доступ к общей папке текущему пользователю, администраторам и операторам архива, выберите переключатель **Не наследовать**. Нажмите кнопку **Далее**. Затем введите имя пользователя и пароль для учетной записи, имеющей право записи в удаленную папку.
7. Нажмите кнопку **Далее**, а затем **Архивировать** (Backup). Откроется окно **Ход архивации** (Backup Progress), показывающее этот процесс. Если нажать кнопку **Закрыть**, архивация будет продолжена в фоновом режиме.

Восстановление сервера после сбоя оборудования или процесса запуска

Операционная система Windows Server 2012 R2 содержит средства расширенной диагностики и решения проблем. Эти функции помогут восстановить работу системы после множества разных проблем с оборудованием, памятью, решить проблемы производительности. Также они помогают пользователям решать всяческие проблемы, связанные со сбоем оборудования.

Операционная система Windows Server 2012 R2 содержит более надежные и более высокопроизводительные драйверы устройств, позволяющие предотвратить много разных причин зависаний и отказов. Улучшенная отмена ввода-вывода (I/O) для драйверов устройств гарантирует, что операционная система сможет восстановиться после блокирования вызовов, и теперь возникает меньше блокирующих операций дискового ввода-вывода.

Чтобы уменьшить время простоя и число перезапусков, необходимых для установки приложений и обновлений, Windows Server 2012 R2 может использовать процесс обновления, чтобы отметить файлы для обновления и затем автоматически заменить файлы при следующем запуске приложения. В некоторых случаях Windows Server 2012 R2 может сохранить данные приложения, закрыть приложение, обновить файлы и затем перезапустить приложение. Чтобы улучшить общую производительность системы и скорость отклика, Windows Server 2012 R2 более эффективно использует память, осуществляет упорядоченное выполнение групп потоков и предоставляет несколько меха-

низмов диспетчеризации процессов. Благодаря оптимизации памяти и использованию процесса, в Windows Server 2012 R2 фоновые процессы оказывают меньше влияния на производительность системы.

Операционная система Windows Server 2012 R2 предоставляет дополнительные подробности в сообщениях об ошибке, что в конечном счете упрощает идентификацию и решение проблемы. ОС Windows Server 2012 R2 использует политики восстановления после сбоя служб более эффективно, чем ее предшественники. Восстанавливая отказавшую службу, Windows Server 2012 R2 автоматически обрабатывает зависимости. Любые необходимые службы и системные компоненты будут запущены перед запуском отказавшей службы.

В более ранних версиях Windows при отказе или зависании приложение отмечалось как не отвечающее, и пользователь должен был выйти из него и заново запустить приложение. ОС Windows Server 2012 R2 содержит диспетчер перезапуска (Restart Manager), позволяющий автоматически перезапустить приложения, не отвечающие на запросы системы. Благодаря этому диспетчеру, возможно, не придется вмешиваться в процесс решения проблемы зависшего приложения.

Сбои при инсталляции, зависания приложений и драйверов также отслеживаются через Центр поддержки, и встроенная диагностика отобразит предупреждение. Щелкнув по значку **Центр поддержки** из области уведомлений, можно увидеть последние сообщения. Если щелкнуть на сообщении, Windows Server 2012 R2 откроет страницу Центра поддержки, предоставляющую решение проблемы.

Можно также просмотреть список текущих проблем с помощью этих действий:

1. В Панели управления щелкните по ссылке **Проверка состояния компьютера** (Review your computer's status) в категории **Система и безопасность** (System and security).
2. Центр поддержки предоставляет список текущих проблем. Для некоторых проблем есть возможность нажать кнопку **Показать сведения о сообщении** (View message details) для отображения страницы **Сведения о сообщении** (Message details). Если доступно решение, щелкните по предоставленной ссылке для загрузки решения или посещения надлежащего сайта с целью получения подробной информации.

При работе с Центром поддержки для поиска решений проблемы можно воспользоваться ссылкой **Поиск решений** (Check for solutions) на панели **Обслуживание** (Maintenance).

Операционная система Windows Server 2012 R2 пытается решить проблемы, связанные с исчерпыванием виртуальной памяти, предоставляя **Средство обнаружения и устранения нехватки ресурсов** (Resource Exhaustion Detection and Recovery, RADAR). Эта функция контролирует лимит виртуальной памяти системы и предупреждает пользователя, если компьютер испытывает нехватку виртуальной памяти. Для решения проблемы она также обнаруживает процессы, использующие самый большой объем памяти, позволяя закрыть любые из них в окне **Закрыть программы для предотвращения потери информации** (Close Programs To Prevent Information Loss). Предупреждение о нехватке ресурсов также записывается в системный журнал.

В ранних версиях Windows поврежденные системные файлы относились к одной из наиболее частых причин сбоя запуска. ОС Windows Server 2012 R2 содержит встроен-

ную диагностику и автоматически обнаруживает поврежденные системы файлов во время запуска и позволяет произвести автоматическое или ручное восстановление. Для решения проблемы запуска Windows Server 2012 R2 использует утилиту StR (Startup Repair Tool), которая автоматически устанавливается и запускается, когда система не может загрузиться. После запуска StR пытается определить причину сбоя запуска, анализируя журналы загрузки и отчеты об ошибках, а затем пытается решить проблему автоматически. Если StR не может решить проблему, она восстанавливает последнее рабочее состояние и затем предоставляет информацию диагностики и опции для решения проблемы.

Проблемы с оборудованием, выявляемые встроенной диагностикой, связаны с обнаружением ошибок и дисковыми сбоями. Если есть проблема с устройством, диагностика оборудования обнаружит условия ошибки и затем устранит проблему автоматически или же предоставит инструкции процесса восстановления. В случае с дисками диагностика оборудования может использовать отчеты отказа для обнаружения потенциальных отказов и предупреждать перед тем, как они произойдут. Диагностика оборудования также поможет с резервным копированием на случай, если диск откажет.

Встроенная диагностика может обнаружить и проблемы с производительностью, в том числе медленный запуск приложения, медленную загрузку, медленный переход в состояние сна и восстановления и медленное завершение работы. Диагностика производительности способна выявить проблему и предоставить возможные решения для ее устранения. Для сложных проблем можно отслеживать производительность и данные надежности с помощью консоли диагностики производительности (Performance Diagnostics console), состоящей из Монитора производительности (Performance Monitor) и Монитора стабильности работы (Reliability Monitor).

Проблемы с памятью также обнаруживаются встроенной диагностикой и включают как утечки памяти, так и сбои памяти. Утечки памяти происходят, если приложение или системный компонент не полностью освободили области физической памяти после работы с ними. Если есть подозрения, что у компьютера возникает проблема с памятью, которая не обнаруживается автоматически, можно запустить процедуру диагностики памяти вручную при запуске системы. Если при запуске системы нельзя запустить диагностику памяти, тогда можно запустить эту программу так:

1. Запустите **Средство проверки памяти** (Windows Memory Diagnostics). Один из способов это сделать — ввести `mdsched.exe` в поле поиска приложений и нажать клавишу <Enter>.
2. Выберите, нужно ли перезапустить компьютер прямо сейчас для проверки памяти или запланировать запуск утилиты при следующем запуске компьютера.
3. Средство диагностики памяти Windows будет запущено автоматически после перезапуска компьютера. По умолчанию используется стандартный тест и два его прохода.

Изменить параметры диагностики можно, нажав клавишу <F1>. Доступны три уровня тестирования памяти: **Базовый** (Basic), **Обычный** (Standard) и **Широкий** (Extended). Используйте базовый тест для быстрого тестирования памяти. Обычный тест применяется для стандартного тестирования памяти. Широкий тест выполняется, когда нужно

произвести расширенное тестирование. Установите число проходов теста, выбрав опцию **Число проходов** (Pass Count).

Для обнаружения отказов системы, вызванных, возможно, отказом памяти, диагностика памяти работает вместе с Microsoft Online Crash Analysis. Если сбой произошел из-за памяти, диагностика памяти определит это и запланирует тест памяти при следующей перезагрузке компьютера.

Восстановление после сбоя запуска

Если произойдет сбой запуска Windows, операционная система Windows Server 2012 R2 автоматически перейдет в режим восстановления. В этом режиме появится экран восстановления со следующими опциями:

- **Продолжить** (Continue) — выйти из меню восстановления и продолжить загрузку операционной системы;
- **Использовать другую операционную систему** (Use Another Operating System) — выйти из меню восстановления и выбрать другую операционную систему для загрузки (если установлено несколько операционных систем);
- **Диагностика** (Troubleshoot) — отображает расширенное меню **Дополнительные параметры** (Advanced Options);
- **Выключить компьютер** (Turn Off Your PC) — выйти из меню восстановления и завершить работу сервера.

Меню **Дополнительные параметры** содержит три опции:

- **Восстановление образа системы** (System Image Recovery) — позволяет восстановить сервер, используя файл образа системы. Файл образа может быть получен с удаленного компьютера;
- **Командная строка** (Command Prompt) — предоставляет доступ к командной строке, и можно работать с командами и утилитами, доступными в среде восстановления;
- **Параметры загрузки** (Startup Settings) — позволяет изменить поведение запуска и запустить сервер в безопасном режиме. Здесь можно выбрать опцию **Перезагрузить** (Restart) для перезапуска компьютера в безопасном режиме так, что можно будет отключить применение подписей драйверов, автоматический перезапуск системы в случае ошибки и т. д. Также позволяет включить видеорежим с низким разрешением, режим отладки, протоколирование загрузки и пр.

Запуск сервера в безопасном режиме

Множество проблем может произойти, если что-то в системе было изменено. Например, устройство было неправильно установлено. Конфигурация системы или реестр могли быть некорректно обновлены, что вызвало конфликт. Часто проблемы с загрузкой можно решить, используя безопасный режим для диагностики проблем или восстановления. Когда закончите использовать безопасный режим, перезапустите сервер для его загрузки в обычном режиме. После этого можно использовать сервер как обычно.

В безопасном режиме Windows Server 2012 R2 загружает только базовые файлы, службы и драйверы. Загружаются драйверы для мыши, монитора, клавиатуры, носителей данных и базовый видеодрайвер. Драйвер монитора устанавливает базовые параметры и режимы для монитора сервера; базовый видеодрайвер устанавливает основные параметры для графической карты сервера. Если сервер не был запущен в безопасном режиме с поддержкой сети, сетевые драйверы не загружаются. Поскольку в безопасном режиме загружается ограниченный набор конфигурационной информации, это помогает диагностировать проблемы.

Запустить сервер в безопасном режиме можно так:

1. Если компьютер не будет запущен нормально, появится экран восстановления. Выберите команду **Диагностика**.
2. На экране **Дополнительные параметры** нажмите кнопку **Параметры загрузки** (Startup settings). Далее на экране **Параметры загрузки** (Startup settings) нажмите кнопку **Перезагрузить** (Restart).
3. Нажимая клавиши-стрелки, выберите безопасный режим, который нужно использовать, и нажмите клавишу <Enter>. Необходимый безопасный режим зависит от типа проблемы.

   - **Устранение неполадок компьютера** (Repair your computer) — загружает утилиту устранения неполадок. Выберите эту опцию для перезапуска сервера и возвращения к экрану восстановления.
   - **Безопасный режим** (Safe mode) — загружает только базовые файлы, службы и драйверы. Будут загружены драйверы для мыши, монитора, видеокарты, носителей информации, клавиатуры. Сетевые службы и драйверы не загружаются.
   - **Безопасный режим с загрузкой сетевых драйверов** (Safe mode with networking) — загружает базовые файлы, службы, драйверы, в том числе службы и драйверы, необходимые для запуска сети.
   - **Безопасный режим с поддержкой командной строки** (Safe mode with command prompt) — загружаются базовые файлы, службы, драйверы, а затем запускается командная строка вместо графического интерфейса Windows. Сетевые службы и драйверы не загружаются.

     Совет

     В **Безопасном режиме с поддержкой командной строки** можно запустить оболочку Проводника из командной строки: нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc>, а из меню **Файл** диспетчера задач можно выбрать команду **Новая задача**, ввести `explorer.exe` и нажать клавишу <Enter>.

   - **Ведение журнала загрузки** (Enable boot logging) — позволяет создать и записать все события запуска в журнал загрузки.
   - **Включение видеорежима с низким разрешением** (Enable low-resolution video) — позволяет запускать систему в видеорежиме с низким разрешением 640×480, что полезно, если был установлен режим, который не поддерживается текущим монитором.

- **Последняя удачная конфигурация** (Last known good configuration) — запускает компьютер в безопасном режиме, используя информацию реестра, которую Windows сохранила при последнем завершении работы, в том числе куст `HKEY_CURRENT_CONFIG` (`HKCC`). Этот куст реестра хранит информацию о конфигурации оборудования, при которой компьютер был ранее удачно загружен.
- **Режим отладки** (Debugging mode) — запускает систему в режиме отладки, что полезно при диагностике ошибок операционной системы.
- **Режим восстановления служб каталогов** (Directory services restore mode) — запускает систему в безопасном режиме и позволяет восстановить службу каталогов. Эта опция доступна на контроллерах домена под управлением Windows Server 2008 R2 и более поздних версий Windows.
- **Отключить автоматическую перезагрузку при отказе системы** (Disable automatic restart on system failure) — запрещает Windows Server автоматически перезагружать компьютер после сбоя системы.
- **Отключение обязательной проверки подписи драйверов** (Disable driver signature enforcement) — запускает компьютер в безопасном режиме без обязательной проверки подписи драйверов. Если цифровая подпись драйвера некорректна или отсутствует, это может вызвать проблему с запуском. Данная опция временно решает проблему, поэтому можно запустить компьютер и получить новый драйвер или изменить цифровую подпись драйвера.
- **Отключение раннего запуска антивредоносного драйвера** (Disable early launch anti-malware driver) — запускает компьютер в безопасном режиме без загрузки антивредоносного драйвера. Если антивредоносный драйвер препятствует запуску системы, нужно проверить сайт разработчика программного обеспечения на предмет обновлений, которые решают проблему с загрузкой, или отключить защиту загрузки в настройках программного обеспечения.
- **Обычная загрузка Windows** (Start Windows normally) — запускает компьютер с обычными настройками.

4. Если проблема не проявляется в безопасном режиме, можно исключить настройки по умолчанию и базовые драйверы из списка возможных проблем. Если проблема заключается в недавно добавленном устройстве или обновленном драйвере, можно использовать безопасный режим, чтобы деинсталлировать устройство или сделать откат обновления.

Резервное копирование и восстановление состояния системы

В операционной системе Windows Server 2012 R2 примерно 50 000 файлов системного состояния, которые занимают около 4 Гбайт дискового пространства в обычной инсталляции 64-разрядного компьютера. Самый быстрый и самый простой способ заархивировать и восстановить состояние системы сервера — применить утилиту Wbadmin. С помощью Wbadmin можно использовать команду `START SYSTEMSTATEBACKUP` для создания резервной копии системы и команду `START SYSTEMSTATERECOVERY` для восстановления системного состояния компьютера.

Совет

При выборе восстановления системного состояния на контроллере домена нужно быть в **Режиме восстановления служб каталога** (Directory Services Restore mode). В следующем разделе будет показано, как восстановить Active Directory.

Для архивирования состояния системы сервера введите следующую команду в командной строке:

```
wbadmin start systemstatebackup -backupTarget:VolumeName
```

Здесь *VolumeName* — имя хранилища резервной копии, например, F:.

Для восстановления состояния системы введите эту команду:

```
wbadmin start systemstaterecovery -backupTarget:VolumeName
```

Здесь *VolumeName* — имя хранилища, содержащего резервную копию, которую нужно восстановить, например, F:. Дополнительно можно сделать следующее:

- используйте параметр `-recoveryTarget` для восстановления системы в альтернативное размещение;
- используйте параметр `-machine` для указания имени восстанавливаемого компьютера, если в хранилище есть резервные копии для разных компьютеров;
- используйте параметр `-authSysvol` для осуществления принудительного восстановления SYSVOL.

Также можно восстановить состояние системы, используя резервную копию, содержащую состояние системы.

Восстановление Active Directory

При восстановлении данных состояния системы на контроллере домена нужно выбрать, какое восстановление будет использоваться: авторитарное (принудительное) или неавторитарное (обычное). По умолчанию используется обычное восстановление. В этом режиме Active Directory и другие реплицируемые данные восстанавливаются из резервной копии, а любые изменения реплицируются с другого контроллера домена. Таким образом, можно безопасно восстановить отказавший контроллер домена без перезаписи последней информации Active Directory. С другой стороны, при попытке восстановить Active Directory по сети, используя резервные копии, нужно выбрать принудительное восстановление. При этом данные восстанавливаются на текущем контроллере домена и затем тиражируются на другие контроллеры домена.

Осторожно!

Принудительное восстановление перезаписывает все данные Active Directory по всему домену. Перед выполнением этого восстановления нужно убедиться, что в резервной копии содержатся корректные данные, которые будут распространены по всему домену, а текущие данные на других контроллерах домена неточные, устарели или повреждены.

Для восстановления Active Directory на контроллере домена и репликации всех восстановленных данных по всей сети выполните следующие действия:

1. Убедитесь, что сервер контроллера домена выключен.
2. Перезагрузите сервер контроллера домена и войдите в безопасный режим.

3. Выберите **Режим восстановления служб каталогов** (Directory Services Restore Mode).
4. Когда система запустится, используйте утилиту Backup для восстановления системного состояния и других важных файлов.
5. После восстановления данных, но до перезапуска сервера, используйте утилиту Ntdsutil.exe, чтобы отметить объекты как принудительно восстанавливаемые. Убедитесь, что тщательно проверили данные Active Directory.
6. Перезагрузите сервер, когда система закончит загрузку, данные Active Directory должны быть реплицированы по всему домену.

Восстановление операционной системы и всего сервера

Как было упомянуто ранее, ОС Windows Server 2012 R2 содержит функции восстановления запуска, которые могут восстановить сервер в случае повреждения или отсутствия системных файлов. Процесс восстановления запуска также может избавить и от других проблем загрузки, связанных с диспетчером загрузки. Если эти процедуры не помогли и диспетчер загрузки не в состоянии запустить сервер, можно использовать инсталляционный диск Windows Server 2012 R2 или восстановление системы для восстановления диспетчера загрузки и запуска системы.

Восстановление системы доступно только на серверах с полной установкой и недоступно на инсталляциях Server Core. Если используется инсталляция Server Core (основные компоненты сервера), нужно воспользоваться установочным диском для запуска процесса восстановления.

Восстановление системы содержит следующие утилиты.

- **Восстановление образа системы** (System Image Recovery) позволяет восстановить операционную систему сервера или выполнить восстановление всей системы. Убедитесь, что данные резервной копии доступны и можно войти с использованием учетной записи с надлежащими правами. При восстановлении всей системы помните, что данные, которые не были включены в резервную копию, будут удалены после восстановления системы, в том числе любые тома, которых нет в резервной копии.
- **Средство диагностики памяти Windows** (Windows Memory Diagnostics Tools) позволяет диагностировать проблемы с физической памятью сервера. Доступны три уровня тестирования памяти: базовый, обычный и широкий.

Также можно получить доступ к командной строке. Командная строка позволяет запустить утилиты командной строки, доступные во время инсталляции, а также дополнительные программы:

- X:\Sources\Recovery\StartRep.exe — обычно эта утилита запускается автоматически при сбое загрузки, если Windows обнаруживает проблему с загрузочным сектором, диспетчером загрузки или хранилищем BCD (Boot Configuration Data);
- X:\Sources\Recovery\Recenv.exe — позволяет запускать Startup Recovery Options Wizard. Если ранее были введены неправильные параметры восстановления, можно указать другие параметры.

Администратор может выполнить диагностику в командной строке:

1. Если компьютер не загружается как обычно, будет отображен экран восстановления. Выберите команду **Диагностика**.
2. В меню **Дополнительные параметры** выберите опцию **Командная строка**.
3. Выберите учетную запись **Администратор**. Далее введите пароль для этой учетной записи и нажмите кнопку **Продолжить** (Continue).
4. Используйте командную строку для диагностики. Например, можно запустить Startup Repair Wizard командой `x:\sources\recovery\startrep.exe`.

Можно восстановить операционную систему сервера или выполнить полное восстановление системы, используя резервный образ, созданный ранее с помощью утилиты **Система архивации данных Windows Server**. При восстановлении операционной системы восстанавливаются все критические тома, но не восстанавливаются несистемные тома. При восстановлении всей системы утилита **Система архивации данных Windows Server** заново разобьет и отформатирует все диски, подключенные к серверу. Поэтому нужно использовать этот метод только тогда, когда необходимо восстановить данные сервера на отдельное оборудование или когда все попытки восстановить сервер на существующем оборудовании не увенчались успехом.

> ***Примечание***
>
> При восстановлении операционной системы или всей системы убедитесь, что архивные данные доступны, и можно войти в систему с учетной записью, обладающей необходимыми правами. При полном восстановлении помните, что существующие данные, которые не были включены в резервную копию, будут удалены при восстановлении системы, в том числе это касается и томов, которые в данный момент используются сервером, но не включены в резервную копию.

Восстановить операционную систему, используя резервный образ, можно с помощью следующих действий:

1. Если компьютер не загружается, как обычно, будет отображен экран восстановления. Выберите команду **Диагностика**.
2. В меню **Дополнительные параметры** выберите команду **Восстановление образа системы**.
3. При запросе выбрать учетную запись укажите запись **Администратор** и введите пароль для нее. Нажмите кнопку **Продолжить**. Будет запущен мастер восстановления компьютера из образа (Re-Image Your Computer Wizard).
4. На странице **Выбор архивного образа** (Select A System Image Backup) системы отметьте переключатель **Использовать последний доступный образ системы (рекомендуется)** (Use the latest available system image (recommended)) и нажмите кнопку **Далее**. Или выберите вариант **Выберите образ системы** (Select a system image) и нажмите кнопку **Далее**.
5. Если нужно выбрать образ для восстановления, на странице **Выберите расположение резервной копии** (Select The Location Of The Backup), которую нужно использовать для восстановления, выберите один из следующих вариантов.

- Выберите расположение, содержащее образ системы, который необходимо использовать, и нажмите кнопку **Далее**. Затем выберите образ системы и нажмите кнопку **Далее**.
- Для поиска системного образа в сети выберите команду **Дополнительно** (Advanced), а затем команду **Искать образ системы в сети** (Search For A System Image On The Network). Нажмите кнопку **Да** для подтверждения подключения к сети. В окне **Восстановление компьютера из образа** (Re-Image Your Computer) укажите сервер и общую папку, в которой хранится образ системы, например \\FileServer22\\Backups, и нажмите кнопку **OK**.
- Для установки драйвера устройства резервного копирования, которого нет в списке, выберите команду **Дополнительно**, а затем команду **Установить драйвер** (Install A Driver). Вставьте инсталляционный носитель с драйвером устройства и нажмите кнопку **OK**. После этого Windows установит драйвер устройства, и оно будет отображено в списке расположений.

6. На странице **Выберите дополнительные параметры восстановления** (Choose Additional Restore Options) задайте дополнительные параметры и нажмите кнопку **Далее**.
   - Установите флажок **Форматировать и разбивать диски** (Format and repartition disks) для удаления существующих разделов и повторного форматирования дисков назначения так, чтобы все соответствовало резервной копии.
   - Установите флажок **Восстановить только системные диски** (Only restore system drives) для восстановления из резервной копии только дисков, необходимых для запуска Windows: загрузочный, системный тома и том восстановления. Если на сервере есть диски с данными, они не будут восстановлены.
   - Отметьте флажок **Установить драйверы** (Install drivers) с целью установки драйверов устройств для оборудования, на котором производится процесс восстановления.
   - Выберите флажок **Дополнительно** (Advanced), чтобы указать, нужно ли перезагрузить компьютер и проверить диски на наличие ошибок немедленно после завершения операции восстановления.
7. На странице **Подтверждение** просмотрите детали восстановления и нажмите кнопку **Готово**. Мастер восстановит операционную систему или весь сервер, в зависимости от установленных вами параметров.

Восстановление приложений, несистемных томов, файлов и папок

Операционная система Windows Server 2012 R2 предоставляет отдельные процессы для восстановления системного состояния, всего сервера и отдельных томов, файлов и папок. Можно использовать мастер восстановления (Recovery Wizard) в утилите **Система архивации данных Windows Server** для восстановления несистемных томов, файлов и папок из резервной копии. Перед тем как начать, убедитесь, что компьютер, на котором восстанавливаются файлы, работает под управлением Windows Server 2012 R2.

Если нужно восстановить отдельные файлы и папки, убедитесь, что как минимум одна резервная копия существует на внутреннем или внешнем диске или в удаленной папке. Нельзя восстановить файлы и папки из резервных копий, сохраненных на DVD или сменных носителях.

Восстановить несистемные тома, файлы и папки или данные приложений можно так:

1. Запустите утилиту **Система архивации данных Windows Server**. Из меню **Действие** или панели **Действия** выберите команду **Восстановить** (Recover). Будет запущен мастер восстановления.
2. На странице **Приступая к работе** укажите, нужно ли восстановить данные с локального компьютера или из другого расположения, а затем нажмите кнопку **Далее**.
3. Если данные восстанавливаются из другого расположения, определите, нужно ли восстановить резервную копию с локальных дисков или удаленной общей папки, а затем нажмите кнопку **Далее** и укажите параметры, специфические для расположения. При восстановлении с локального диска на странице **Расположение архива** (Select backup location) выберите расположение резервной копии из выпадающего списка. При восстановлении из удаленной общей папки на странице **Выбор удаленной папки** (Specify remote folder) введите путь к папке, содержащей архив. В удаленной папке резервная копия должна быть сохранена в папке *сервер*\ WindowsImageBackup*ИмяКомпьютера*.
4. Если архив восстанавливается из другого расположения, на странице **Выберите сервер** (Select server) нужно указать, данные какого сервера следует восстановить. Нажмите кнопку **Далее**.
5. На странице **Выбор даты архивации** (Select backup date) выберите дату и время архивации, используя календарь и список времени. Если для даты доступна резервная копия, дата будет выделена жирным начертанием. Нажмите кнопку **Далее**.
6. На странице **Тип восстановления** (Select recovery type) выберите, что нужно восстановить.
   - Для восстановления отдельных файлов и папок выберите переключатель **Файлы и папки** (Files and folders), а затем нажмите кнопку **Далее**. На странице **Восстанавливаемые элементы** (Select items to recover) раскройте список **Доступные элементы** (Available Items) (нажав значок +). Щелкните на папке в списке **Доступные элементы**, чтобы отобразить ее содержимое в области **Восстанавливаемые элементы**. Выберите каждый элемент, который нужно восстановить, и нажмите кнопку **Далее**.
   - Для восстановления некритических томов выберите **Тома** (Volumes) и нажмите кнопку **Далее**. На странице **Выбор тома** (Select volumes) отображается список томов-источников и томов-назначений. Установите переключатели тех исходных томов, которые нужно восстановить, и затем выберите размещение, в которое нужно восстановить тома, используя список томов-назначений. Нажмите кнопку **Далее**. Если мастер попросит подтвердить операцию восстановления, нажмите кнопку **Да** и пропустите действия 7 и 8.
   - Для восстановления данных приложений выберите **Приложения** (Applications) и нажмите кнопку **Далее**. На странице **Выбор приложения** (Select application)

в списке **Приложения** (Applications) отметьте приложения, которые нужно восстановить. Если восстанавливается самая последняя резервная копия, будет отображен флажок **Не выполнять восстановление базы данных приложений с повтором всех завершенных транзакций** (Do not perform a roll-forward recovery of the application database). Если требуется, чтобы система архивации данных Windows Server не повторяла все завершенные транзакции в восстанавливаемой базе данных, установите этот флажок. Нажмите кнопку **Далее**. Поскольку все данные на томе назначения будут потеряны при осуществлении восстановления, убедитесь, что том назначения пуст или хотя бы не содержит важной информации.

7. Далее можно указать, нужно ли восстанавливать данные в их исходное расположение (только для несистемных файлов) или в альтернативное расположение. В случае с альтернативным расположением введите путь для восстановления данных или выберите его, нажав кнопку **Обзор**. В случае с приложениями можно скопировать данные приложения в альтернативное расположение. Однако нельзя восстановить приложения на другой компьютер.
8. Для восстановления файлов и каталогов выберите метод восстановления, который будет применяться, если в расположении восстановления уже существуют восстанавливаемые файлы и папки. Можно либо создавать копии так, чтобы присутствовали обе версии файла или папки, либо перезаписывать существующие файлы восстановленными, либо пропускать уже существующие файлы. Также можно восстановить исходные права доступа к восстановленным файлам и папкам.
9. На странице **Подтверждение** просмотрите подробности и нажмите кнопку **Восстановить** для восстановления указанных элементов.

Управление политикой восстановления шифрования

Если используется шифрованная файловая система EFS (Encrypting File System), план резервного копирования должен содержать дополнительные процедуры и подготовительные операции. Нужно рассмотреть, как обрабатывать проблемы, связанные с персональными сертификатами шифрования, агентами восстановления EFS и политикой восстановления EFS. Все эти проблемы описаны в следующих разделах.

Сертификаты шифрования и политики восстановления

Шифрование поддерживается на уровне файла и на уровне папки. Любой файл, помещенный в папку, отмеченную для шифрования, автоматически зашифровывается. Файлы в зашифрованном формате могут быть прочитаны только тем лицом, которое зашифровало их. Чтобы другие пользователи смогли прочитать зашифрованный файл, его нужно сначала расшифровать.

У каждого зашифрованного файла есть свой уникальный ключ шифрования. Это означает, что файлы могут быть скопированы, перемещены и переименованы — как и лю-

бые другие файлы, и в большинстве случаев эти операции никак не повлияют на шифрование данных. Пользователь, зашифровавший файл, всегда имеет доступ к файлу, поскольку приватный ключ находится в профиле пользователя на локальном компьютере или получен с помощью перемещаемого профиля посредством DIMS (Digital Identification Management Service). Для этого пользователя процесс шифрования и расшифровки обрабатывается автоматически и абсолютно прозрачно.

EFS — это процесс, обрабатывающий шифрование и расшифровку. Установка EFS по умолчанию дает возможность пользователю шифровать файлы без необходимости наличия специальных разрешений. Файлы шифруются с использованием публичного/приватного ключа, который автоматически генерируется для каждого пользователя. По умолчанию используется алгоритм AES (Advanced Encryption Standard) для шифрования файлов в EFS. Internet Information Services 7 (и более поздние версии) может использовать AES-провайдера для шифрования паролей по умолчанию.

Сертификаты шифрования хранятся как часть данных в профилях пользователей. Если пользователь работает с несколькими компьютерами и хочет применять шифрование, администратору нужно настроить для него перемещаемый профиль. Перемещаемый профиль гарантирует, что данные профиля пользователя и сертификаты публичного ключа доступны с других компьютеров. Без этого пользователи не смогут получить доступ к своим зашифрованным файлам на других компьютерах.

> ***Совет***
>
> Вместо создания перемещаемого профиля можно скопировать сертификат шифрования пользователя на другие компьютеры, которые использует пользователь. Можно сделать это, используя процедуру резервного копирования и восстановления сертификата, которая будет описана далее в этой главе. Просто заархивируйте сертификат с исходного компьютера пользователя и затем восстановите его на каждом компьютере, за которым работает пользователь.

EFS имеет встроенную систему восстановления данных, защищающую данные от потери. Эта система восстановления гарантирует, что зашифрованные данные могут быть восстановлены, если сертификат публичного ключа пользователя потерян или удален. Наиболее вероятна ситуация, когда пользователь больше не работает в компании, и его учетная запись была удалена. Хотя менеджер может войти под учетной записью пользователя, проверить файлы и сохранить важные данные в другие папки, зашифрованные файлы станут доступны только после удаления шифрования. Для этого менеджеру нужно, работая от имени пользователя, который зашифровал файлы, скопировать файлы на том FAT или FAT32 (где шифрование не поддерживается).

Для доступа к зашифрованным файлам после удаления учетной записи пользователя нужно запустить агент восстановления. Агенты восстановления обладают доступом к ключу шифрования файла, который необходим для разблокирования данных в зашифрованных файлах. Однако для защиты важных данных у агентов восстановления нет доступа к приватному ключу пользователя или любой информации приватного ключа.

Агенты восстановления назначаются автоматически, также автоматически генерируются необходимые сертификаты восстановления. Это гарантирует, что зашифрованные файлы всегда можно расшифровать.

Агенты восстановления EFS настроены на двух уровнях.

- **Домен.** Агент восстановления для домена автоматически настраивается при установке первого контроллера домена Windows Server 2012. По умолчанию агент восстановления — это администратор домена. Средствами групповой политики администраторы домена могут назначить дополнительных агентов восстановления. Администраторы домена могут также делегировать привилегии агентов восстановления назначенным администраторам безопасности.
- **Локальный компьютер.** Когда компьютер — часть рабочей группы или используется в автономной конфигурации, по умолчанию агентом восстановления является администратор локального компьютера. Можно назначить дополнительных агентов восстановления. В будущем, если нужно на локальном компьютере использовать локальных агентов восстановления, а не агентов восстановления уровня домена, необходимо удалить политику восстановления из групповой политики для домена.

Можно удалить политики восстановления, если в них больше нет необходимости.

Настройка политики восстановления EFS

Политики восстановления настраиваются автоматически для контроллеров домена и рабочих станций. По умолчанию администраторы домена являются назначенными агентами восстановления для доменов, а локальный администратор — назначенный агент восстановления для автономной рабочей станции.

С помощью групповой политики можно просматривать, назначать и удалять агентов восстановления. Выполните следующие действия:

1. Откройте групповую политику для локального компьютера, сайта, домена или организационного подразделения, с которыми нужно работать. За более детальными сведениями обратитесь к *главе 4*.
2. Разверните узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики открытого ключа\ Шифрованная файловая система (EFS)** (Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System), чтобы получить доступ к настроенным агентам восстановления в групповой политике.
3. Панель справа содержит список назначенных сертификатов восстановления. Сообщается, для кого выданы сертификаты, кем выданы, дата окончания, назначение сертификата и т. д.
4. Чтобы назначить дополнительного агента восстановления, щелкните правой кнопкой мыши по узлу **Шифрованная файловая система (EFS)** и выберите команду **Добавить агент восстановления данных** (Add Data Recovery Agent). Будет запущен мастер добавления агента восстановления данных (Add Recovery Agent Wizard), который можно использовать для выбора ранее сгенерированного сертификата, назначенного пользователю в качестве сертификата восстановления. Нажмите кнопку **Далее**. На странице **Выбор агентов восстановления** (Select Recovery Agents) нажмите кнопку **Обзор каталога** (Browse Directory), а затем в окне **Поиск: Пользов., контакты и группы** (Find users, contacts, and groups) выберите пользователя, с ко-

торым нужно работать. Нажмите кнопку **OK**, а потом кнопку **Далее**. Нажмите кнопку **Готово** для добавления агента восстановления.

5. Для удаления агента восстановления выберите сертификат агента восстановления на правой панели, а затем нажмите клавишу <Delete>. Когда будет запрошено подтверждение действия, нажмите кнопку **Да** для безвозвратного удаления сертификата. Если политика восстановления пуста (означает, что нет больше назначенных агентов восстановления), EFS будет выключена, поэтому пользователи больше не смогут шифровать файлы.

Примечание

Перед назначением дополнительных агентов восстановления необходимо установить корневой центр сертификации в домене. После нужно использовать оснастку **Сертификаты** для создания персональных сертификатов, которые задействованы шаблоном агента восстановления EFS. Корневой центр сертификации должен затем одобрить запрос сертификата, чтобы сертификат можно было использовать. Также можно использовать программу Cipher.exe для генерирования агента восстановления EFS и сертификата.

Резервное копирование и восстановление зашифрованных данных и сертификатов

Можно заархивировать и восстановить зашифрованные данные подобно любым другим данным. Важно помнить, что нужно применять программное обеспечение для резервного копирования, понимающее EFS, например встроенные утилиты резервного копирования и восстановления. Однако необходимо быть осторожным при использовании этого типа программного обеспечения.

Процесс резервного копирования или восстановления не обязательно архивирует или восстанавливает сертификат, необходимый для работы с зашифрованными данными. Сертификат содержится в данных профиля. Если учетная запись пользователя существует, профиль все еще хранит необходимый сертификат, и пользователь все еще может работать с зашифрованными данными.

Если учетная запись пользователя существует и ранее был заархивирован профиль пользователя, а затем был восстановлен для восстановления сертификата, пользователь все еще может работать с зашифрованными данными. В противном случае нет никакого другого способа работы с данными, и необходим назначенный агент восстановления для доступа к файлам и удаления шифрования.

Возможность архивирования и восстановления сертификатов — важная часть плана восстановления. В следующих разделах мы рассмотрим методы выполнения этих задач.

Архивирование сертификата шифрования

Для резервного копирования и восстановления сертификатов используется оснастка **Сертификаты** (Certificates). Личные сертификаты хранятся в формате Personal Information Exchange (pfx).

Для архивирования персональных сертификатов выполните следующие действия:

1. Войдите на компьютер как пользователь, сертификат которого нужно заархивировать. Нажмите клавишу <Windows> (другое название <Start>), в поле поиска приложений введите `mmc` и нажмите клавишу <Enter>. Будет открыта консоль управления Microsoft (MMC, Microsoft Management Console).
2. В MMC выберите команду меню **Файл | Добавить или удалить оснастку** (File | Add/Remove Snap-In). Откроется окно **Добавление и удаление оснасток** (Add Or Remove Snap-Ins).
3. В списке **Доступные оснастки** (Available Snap-Ins) выберите **Сертификаты** (Certificates) и нажмите кнопку **Добавить**. Далее выберите **моей учетной записи пользователя** (My User Account) и нажмите кнопку **Готово**. Оснастка **Сертификаты** (Certificates) будет добавлена в список **Выбранные оснастки** (Selected Snap-Ins). Оснастка будет работать для текущей учетной записи пользователя.
4. Нажмите кнопку **OK** для закрытия окна **Добавление и удаление оснасток**.
5. Перейдите в раздел **Сертификаты — текущий пользователь | Личное | Сертификаты** (Certificates — Current User | Personal | Certificates). Щелкните правой кнопкой мыши на сертификате, который нужно сохранить, выберите команду **Все задачи | Экспорт** (All tasks | Export). Будет запущен мастер экспорта сертификатов (Certificate Export Wizard). Нажмите кнопку **Далее**.
6. Выберите параметр **Да**, **экспортировать закрытый ключ** (Yes, Export The Private Key). Нажмите кнопку **Далее** дважды.
7. На странице **Безопасность** (Security) используйте предоставленные опции для указания субъектов безопасности, которые должны иметь доступ к сертификату. Субъект безопасности по умолчанию — учетная запись **Администратор**. После этого введите и подтвердите пароль для открытия сертификата. Нажмите кнопку **Далее**.
8. Нажмите кнопку **Обзор**. Используйте предоставленное окно для указания расположения файла сертификата и затем нажмите кнопку **Сохранить**. Убедитесь, что расположение безопасно, поскольку никто не хочет скомпрометировать безопасность системы. Файл будет сохранен с расширением pfx.
9. Нажмите кнопку **Далее**, а затем кнопку **Готово**. Если процесс экспорта сертификата успешен, будет отображено соответствующее окно, свидетельствующее об этом. Нажмите кнопку **OK** для закрытия этого окна.

Восстановление сертификата шифрования

Если есть резервная копия сертификата, можно восстановить сертификат на любом компьютере сети, а не только на исходном компьютере. Процесс архивирования и восстановления — по сути, это процесс перемещения сертификатов с одного компьютера на другой.

Для восстановления личного сертификата воспользуйтесь следующими действиями:

1. Скопируйте pfx-файл на съемный носитель, например на флешку или дискету, а затем зарегистрируйтесь как пользователь на компьютере, где нужно использовать личный сертификат.

Примечание

Нужно зарегистрироваться на целевом компьютере как пользователь, чей сертификат пытаетесь восстановить. Если не сделать этого, пользователь не сможет работать с зашифрованными данными.

2. Получите доступ к оснастке **Сертификаты**, как было описано ранее.
3. Разверните узел **Сертификаты — текущий пользователь**. Далее щелкните правой кнопкой мыши на элементе **Личное** (Personal), выберите команды **Все задачи | Импорт** (All Tasks | Import). Будет запущен мастер импорта сертификатов (Certificate Import Wizard).
4. Нажмите кнопку **Далее** и вставьте сменный носитель.
5. Нажмите кнопку **Обзор** и в окне открытия файла найдите личный сертификат на сменном носителе. Убедитесь, что выбран формат **Файлы обмена личной информации (.pfx)** (Personal Information Exchange). Найдите файл, выберите его и нажмите кнопку **Открыть**.
6. Нажмите кнопку **Далее**. Введите пароль для личного сертификата и нажмите кнопку **Далее** снова.
7. Сертификат должен быть помещен в хранилище **Личное** по умолчанию. Примите настройки по умолчанию, нажав кнопку **Далее**. Нажмите кнопку **Готово**. Если процесс импорта окажется успешным, будет отображено соответствующее окно. Нажмите кнопку **OK**.

Предметный указатель

K

L

M

N

O

P

R

S

T

U

V

W

Z

А

В

Г

Д

З

И

К

М

О

П

Р

С

Т

У

Ф

Ц

Ч

Ш

Я

Microsoft Windows Server® 2012 R2

ХРАНЕНИЕ, БЕЗОПАСНОСТЬ, СЕТЕВЫЕ КОМПОНЕНТЫ

Справочник администратора

Практическое руководство для администраторов Windows Server 2012 R2!

Готовые решения для использования средств хранения, обеспечения безопасности и сетевых компонентов Windows Server 2012 R2 представлены в виде таблиц, инструкций и списков. Сконцентрируйте свое внимание только на нужной информации, экономьте время и выполняйте поставленные задачи, где бы вы ни находились.

В этой книге:

- администрирование файловых систем, дисков, RAID-массивов;
- управление пространствами хранения и настройка пулов хранения;
- настройка разрешений и общего доступа к файлам;
- аудит системных ресурсов и реализация квот;
- администрирование групповой политики и параметров безопасности;
- установка и настройка DNS в сети;
- управление TCP/IP и сетевыми подключениями;
- управление и диагностика служб печати;
- шифрование, резервное копирование и восстановление данных.

Об авторе

Уильям Р. Станек (William R. Stanek) — обладатель статуса Microsoft MVP, имеет 20-летний опыт в области системного администрирования и продвинутого программирования. Отмечен наградами, написал свыше 150 книг, включая «Microsoft Windows 8.1. Справочник администратора», «Microsoft SQL Server 2012. Справочник администратора». Редактор серии Справочник администратора.

Издательство
Русская редакция
125362, Москва,
ул. Свободы, д. 17, а/я 14
E-mail: info@rusedit.com
Internet: www.rusedit.com
Тел.: (495) 638-5-638

БХВ-ПЕТЕРБУРГ
191036, Санкт-Петербург,
Гончарная ул., 20
Тел.: (812) 717-10-50,
339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

Windows Server
Microsoft

ISBN 978-5-9775-3558-8

bhv®

РУССКАЯ РЕДАКЦИЯ