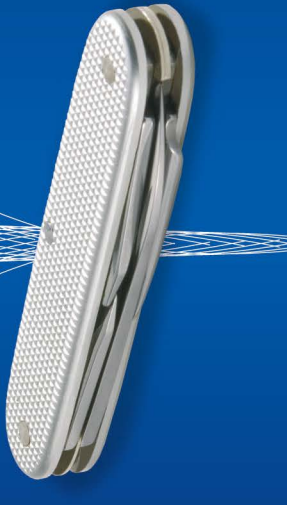
Microsoft

Microsoft Windows Server® 2012

Уильям Р. Станек



Справочник администратора

РУССКАЯ РЕДАКЦИЯ Microsoft BHV

Microsoft

Windows Server® 2012

Pocket Consultant

William R. Stanek
Author and Series Editor

Microsoft Windows Server® 2012

Справочник администратора

Уильям Р. Станек

РУССКАЯ РЕДАКЦИЯ

bhv

2014

УДК 004.451
ББК 32.973.26-018.2
С76

Станек У. Р.

С76 Microsoft Windows Server® 2012. Справочник администратора: Пер. с англ. — М.: Издательство «Русская редакция»; СПб.: «БХВ-Петербург», 2014. — 688 с.: ил. — (Справочник администратора)

ISBN 978-5-7502-0428-1 («Русская редакция»)
ISBN 978-5-9775-0940-4 («БХВ-Петербург»)

Данная книга — краткий и исчерпывающий справочник по администрированию Windows Server 2012. Здесь описаны: управление серверами на базе Windows Server 2012, мониторинг процессов, служб и событий, автоматизация административных задач, улучшение безопасности компьютера, использование и администрирование Active Directory, работа с учетными записями пользователя и группы, управление файловыми системами и дисками, настройка томов и RAID-массивов, общий доступ к данным, безопасность и аудит, резервное копирование и восстановление данных, управление сетью TCP/IP, запуск DCHP-клиентов и серверов, оптимизация DNS.

Для квалифицированных пользователей и системных администраторов

УДК 004.451
ББК 32.973.26-018.2

Уильям Р. Станек

Microsoft Windows Server® 2012. Справочник администратора

Перевод с английского языка Дениса Колисниченко

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

РУССКАЯ РЕДАКЦИЯ bhv®

Подписано в печать 30.09.13.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 55,47.
Тираж 1000 экз. Заказ №

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

ISBN 978-0-7356-6633-7 (англ.)
ISBN 978-5-7502-0428-1 («Русская редакция»)
ISBN 978-5-9775-0940-4 («БХВ-Петербург»)

Оглавление

Эта книга посвящается моей жене, которая на протяжении многих книг, многих миллионов слов и многих тысяч страниц была рядом со мной, предоставляя помощь и поддержку и создавая домашний уют в каждом месте, в котором мы жили.

Я также посвящаю эту книгу моим детям, за их помощь видеть мир по-новому, за их исключительное терпение и безграничную любовь, а также за то, что они делают каждый день приключением.

Также посвящается Карене, Мартину, Луанде, Джулиане и многим другим людям, которые помогали мне как в малом, так и в большом.

Уильям Р. Станек

Об авторе

Уильям Р. Станек (William R. Stanek, **http://www.williamstanek.com**) имеет за плечами более 20 лет практического опыта работы в области продвинутого программирования и разработки. Он один из ведущих экспертов по компьютерным технологиям, автор отмеченных наградами книг и довольно-таки хороший обучающий инструктор. На протяжении многих лет он своими практическими советами помогал миллионам программистов, разработчиков и сетевых инженеров по всему миру.

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

Уильям обладает степенью магистра информационных систем и дипломом бакалавра информатики. Он гордится своей службой в армии во время военных действий в Персидском заливе в качестве члена экипажа самолета радиоэлектронного противоборства. Он участвовал во многих боевых операциях в Ираке и был награжден девятью медалями за свою военную службу, включая одну из наград военно-воздушных сил США — крест "За лётные боевые заслуги". В настоящее время он проживает со своей женой и детьми на тихоокеанском северо-западе США.

Недавно Уильям снова увлекся природным туризмом. Когда он не работает над очередной книгой, то совершает пешие прогулки, 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

Введение

За эти годы я написал много книг о серверных технологиях и продуктах, но больше всего мне нравится писать о Microsoft Windows Server. Для всех, кто переходит на Windows Server 2012, замечу, что это самое существенное обновление Windows Server, начиная с Windows Server 2000. Хотя пользовательский интерфейс сильно изменился, но все-таки главные изменения существенно более глубокие — в основной архитектуре.

Хорошая новость заключается в том, что операционная система Windows Server 2012 построена на той же базе, что и Microsoft Windows 8. Это означает, что можно применить большую часть знаний о Windows 8 к Windows Server 2012, в том числе и то, как Windows работает с сенсорным пользовательским интерфейсом. Вряд ли Windows Server 2012 будет устанавливаться на компьютеры с сенсорным интерфейсом, но можно управлять Windows Server 2012 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.

Поскольку я написал много бестселлеров по Windows Server, в этой книге собран уникальный опыт, полученный при работе с технологиями на протяжении многих лет. Задолго до того, как продукт получил название Windows Server 2012, я работал с его бета-версией. И вот уже существует окончательная версия Windows Server 2012, доступная сегодня в виде готового продукта.

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

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. Она не только рекомендует, как настроить Windows Server 2012, 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, эта 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.

Для кого предназначена эта книга

Книга охватывает все редакции Windows Server 2012 и предназначена для:

- действующих системных администраторов Windows;
- опытных пользователей, выполняющих некоторые обязанности администратора;
- администраторов, выполняющих обновление систем с предыдущих версий до Windows Server 2012;
- 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-сервера, 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 интерфейсом пользователя этой ОС. Если есть необходимость в изучении основ Windows, нужно обратиться к другим ресурсам.

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. Эта книга состоит из 16 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.

Как и другие книги данной серии, эта книга призвана быть кратким и удобным в использовании ресурсом для управления Windows-серверами. Она станет удобным настольным руководством, поскольку охватывает все необходимое для осуществления основных административных задач для Windows-серверов. Читателю не придется листать сотни страниц с посторонней информацией, чтобы найти необходимое — он быстро найдет то, что ищет.

Книга написана так, чтобы стать единым ресурсом, к которому читатель будет обращаться каждый раз, когда у него появятся вопросы относительно администрирования Windows Server. С этой целью в книге приводятся ежедневные административные процедуры, часто выполняемые задачи, документированные примеры и альтернативные варианты решений разных проблем. Одна из моих задач — сделать повествование максимально кратким и легким, но при этом предоставить максимум информации.

Типографские соглашения

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

> ***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**.

Остальные соглашения выглядят так:

- **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**. Следите за мной на Твиттере на WilliamStanek и на Facebook на **www.facebook.com/William.Stanek.Author**.

Другие ресурсы

Не существует какого-то волшебного способа изучить все, что есть по Windows Server 2012. 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 эту книгу по назначению — в качестве краткого и удобного в работе ресурса. Он охватывает основные задачи администратора Windows-сервера, 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 и обновления для книги.

Опечатки и поддержка книги

Мы приложили все усилия для обеспечения точности информации в этой книге и сопровождающего ее содержимого. Список всех ошибок, обнаруженных после издания этой книги, выложен на странице издательства "Microsoft Press" веб-сайта издательства O'Reilly по адресу:

http://go.microsoft.com/FWLink/?Linkid=258651

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

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

Обратите внимание, что поддержка программного обеспечения корпорации Microsoft по данного 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://www.microsoft.com/learning/booksurvey

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**.

часть I

Основы администрирования Windows Server 2012

ГЛАВА 1

Обзор администрирования Windows Server

Microsoft Windows Server 2012 — мощная, универсальная и полнофункциональная операционная система, основанная на расширениях, которые Microsoft внедрила в Windows Server 2008 Release 2. Windows Server 2012 и Windows 8 имеют много общего, поскольку обе системы являются частью одного и того же проекта. Благодаря этому работа с этими операционными системами во многом схожа, в том числе в управлении, настройке средств безопасности, сети и средств хранения данных. Поэтому большую часть информации о Windows 8 можно применить и к Windows Server 2012.

В этой главе рассказано, с чего начать работу в Windows Server 2012, и дан обзор основных архитектурных изменений в Windows Server 2012. В этой главе, как и в других главах книги, представлены советы по улучшению безопасности вашего сервера. Данные советы касаются всех аспектов компьютерной безопасности, в том числе физической, информационной и сетевой безопасности. Хотя книга посвящена Windows Server 2012, эти советы и техники применимы для других версий Windows Server.

Windows Server 2012 и Windows 8

Перед установкой Windows Server 2012 необходимо тщательно спланировать архитектуру сервера. Нужно внимательно проанализировать конфигурацию программного обеспечения, которое будет использоваться, а также модифицировать аппаратную конфигурацию, чтобы она соответствовала системным требованиям. Для большей гибкости можно развернуть сервер, используя один из трех типов установки.

- **Сервер с графическим интерфейсом пользователя** (Server With A GUI installation) — этот тип установки предоставляет полную функциональность, поэтому он также называется *полной установкой*. Можно настроить сервер на любую допустимую комбинацию ролей, сервисов ролей и функций, а полноценный интерфейс пользователя пригодится для управления сервером. Этот тип установки предоставляет более динамическое решение и рекомендуется для развертывания Windows Server 2012 в местах, где роль сервера будет часто меняться.
- **Установка основных серверных компонентов (Server Core)** (Server Core installation) — минимальная установка, которая подразумевает фиксированный набор ролей, но не содержит графическую оболочку сервера (Server Graphical Shell), Консоль управления Microsoft (Microsoft Management Console), а также компонент **Возможности рабочего стола** (Desktop Experience). Эту установку можно настроить с ограниченным набором ролей. Для управления сервером предоставляется ограниченный интерфейс пользо-

вателя. Большая часть управления осуществляется локально в командной строке или удаленно с помощью инструментов управления. Этот тип установки идеально подходит для решений, когда нужен сервер определенной роли или конкретной комбинации ролей.

- **Сервер с минимальным графическим интерфейсом пользователя** (Server With Minimal Interface installation) — промежуточный вариант установки, при котором выполняется полная установка, а затем удаляется графическая оболочка сервера (Server Graphical Shell). В этом случае будет доступен минимальный интерфейс пользователя, консоль управления Microsoft (MMC), диспетчер серверов (Server Manager) и Панель управления (Control Panel) для локального управления. Этот тип установки идеален в ситуациях, когда нужно тщательно контролировать задачи, выполняемые сервером, например роли и функции, но не нужен графический интерфейс пользователя.

Выбор типа установки происходит при установке операционной системы. В отличие от предыдущих выпусков Windows Server, теперь можно изменить тип установки только при установке. Основное отличие между инсталляционными типами заключается в присутствии графических инструментов управления и графической оболочки. В установке основных серверных компонентов (Server Core) вообще нет ни того, ни другого; в полной установке есть обе возможности; в третьем типе установки — только графические инструменты управления.

> ***Дополнительная информация***
>
> Некоторые функции и роли сервера требуют наличия графической оболочки: Факс-сервер (Fax Server), Службы удаленных рабочих столов (Remote Desktop Session Host), Службы развертывания Windows (Windows Deployment Services) и Клиент печати через Интернет (Internet Printing user interface). Также графический интерфейс нужен для средства Просмотр событий и Брандмауэра Windows.

Подобно Windows 8, Windows Server 2012 обладает следующими возможностями.

- **Модуляризация для языковой независимости и образы дисков для аппаратной независимости.** Каждый компонент операционной системы разработан как независимый модуль, который можно легко добавить или удалить. Такая функциональность является базовой для конфигурации архитектуры в Windows Server 2012. Microsoft распространяет Windows Server 2012 на носителях в формате Windows Imaging Format (WIM), который использует сжатие и позволяет резко уменьшить размер файлов.
- **Преинсталляционная и предзагрузочная среда.** Преинсталляционная среда (она же среда предустановки), Windows Preinstallation Environment (Windows PE 4.0), заменяет MS-DOS как среду предустановки и обеспечивает самозагружаемую среду запуска для установки, развертывания, восстановления и решения проблем. Предзагрузочная среда предоставляет загрузочное окружение с менеджером загрузки, позволяющим выбрать загрузочное приложение для запуска операционной системы. На компьютерах с несколькими операционными системами доступ к старым системам (до Windows 7) осуществляется с помощью традиционного (устаревшего) загрузчика.
- **Контроль учетных записей пользователей и повышение привилегий.** Контроль учетных записей пользователей (User Account Control, UAC) повышает компьютерную безопасность, гарантируя истинное разделение стандартных учетных записей пользователя и администратора. Благодаря UAC, все приложения запускаются либо с правами стандартного пользователя, либо с правами администратора. Если приложение требует привилегий администратора, будет отображено предупреждение безопасности (по умолчанию). Предупреждение безопасности можно настроить с помощью групповой полити-

ки. А если вход осуществляется с помощью встроенной учетной записи **Администратор**, какие-либо предупреждения не отображаются.

Поскольку у Windows 8 и Windows Server 2012 общая база кода, то обе системы имеют идентичные интерфейсы управления. Каждая утилита Панели управления, доступная в Windows Server 2012, почти (или полностью) идентична аналогичной утилите в Windows 8. Конечно, есть исключения, связанные со стандартными настройками по умолчанию. Так как Windows Server 2012 не использует рейтинги производительности, в Windows Server нет индекса производительности Windows. Поскольку операционная система Windows Server 2012 не может перейти в режим сна, в ней нет режимов сна и гибернации. Так как обычно на Windows-серверах не используется расширенное управление питанием, в Windows Server 2012 довольно ограниченный набор параметров по управлению питанием.

В ОС Windows Server 2012 нет Windows Aero, боковой панели, гаджетов и других расширений пользовательского интерфейса, поскольку Windows Server 2012 разработан для обеспечения максимальной производительности задач сервера и не предназначен для расширенной персонализации пользовательского интерфейса. Однако, если выбрана полная установка, можно добавить компонент **Возможности рабочего стола** (Desktop Experience) для включения некоторых функций Windows 8 на сервере.

Компонент **Возможности рабочего стола** предоставляет функциональность рабочего стола Windows на вашем сервере. А именно будут доступны следующие компоненты: Проигрыватель Windows Media (Windows Media Player), темы оформления рабочего стола, Видео для Windows (поддержка AVI) (Video for Windows), Защитник Windows (Windows Defender), Очистка диска (Disk Cleanup), Центр синхронизации (Sync Center), Звукозапись (Sound Recorder), Таблица символов (Character Map), Ножницы (Snipping Tool). Хотя все эти функции позволяют использовать сервер как настольный компьютер, они отрицательно сказываются на его общей производительности.

Поскольку основные функции Windows 8 и Windows Server 2012 во многом подобны, в книге не будут рассматриваться отличия от интерфейсов предыдущих выпусков операционной системы, не будет рассказано, как работает UAC, и т. д. Все это легко найти в книге "Microsoft® Windows 8. Справочник администратора"[1], которую можно использовать в качестве дополнения к этой книге. В той книге рассматриваются не только задачи администрирования, но и показано, как персонализировать операционную систему и среду Windows, настроить аппаратные средства и сетевые устройства, управлять доступом пользователей и глобальными настройками, настраивать ноутбуки, использовать возможности удаленного управления, описано решение проблем с системой и многое другое. А эта книга ориентирована на управление службами каталогов, администрирование данных и сети.

Знакомство с Windows Server 2012

Существуют различные выпуски Windows Server 2012. Все они поддерживают многоядерные процессоры. Важно указать, что компьютер может иметь всего лишь один процессор (будем называть его физическим процессором), но у него может быть восемь ядер (так называемые логические процессоры).

Windows Server 2012 — строго 64-разрядная операционная система. В этой книге 64-битными системами называются системы, разработанные для архитектуры *x*64. Поскольку раз-

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

личные выпуски Windows Server поддерживают те же самые базовые компоненты и обладают одинаковыми инструментами управления, допускается использовать методы, обсуждаемые в этой книге, независимо от используемого выпуска Windows Server 2012.

После установки ОС Windows Server 2012 нужно настроить систему в соответствии с ее ролью в сети:

- *серверы* — обычно являются частью рабочей группы или домена;
- *рабочие группы* — группы компьютеров, в которых каждый компьютер управляется (администрируется) отдельно;
- *домены* — группы компьютеров, которыми можно управлять коллективно посредством контроллеров доменов, в роли которых может выступать система на базе Windows Server 2012. Такие системы управляют доступом к сети, базе данных каталога и общим ресурсам.

> ***Примечание***
>
> В этой книге упоминание "Windows Server 2012" и "семейство Windows Server 2012" относится ко всем выпускам Windows Server 2012. Различные выпуски сервера поддерживают одинаковые базовые компоненты и инструменты управления.

В отличие от Windows Server 2008, в Windows Server 2012 есть экран **Пуск** (Start). Экран **Пуск** — это окно, а не меню. Помимо всего прочего, в этом окне могут быть плитки программ. Нажатие пальцем (или щелчок мышью) приводит к запуску программы. При нажатии и удерживании плитки пальцем (или щелчке по плитке правой кнопкой мыши) открывается панель команд. Панель **Charms** (она же боковая панель) — это панель опций для экрана **Пуск**, рабочего стола и параметров компьютера. При использовании сенсорного экрана можно отобразить панель **Charms** путем скольжения от правого края экрана к центру. Чтобы отобразить панель **Charms** с помощью мыши, подведите указатель мыши к скрытой кнопке в правом верхнем или правом нижнем углу экрана **Пуск**, рабочего стола или параметров компьютера. Также можно воспользоваться комбинацией клавиш <Windows>+<C>.

Нажмите или щелкните по кнопке **Поиск** (Search) на панели **Charms** для отображения панели **Поиск** (Search). Поиск может быть произведен по приложениям, параметрам и файлам. Когда выбран поиск по приложениям, можно использовать панель **Поиск** для быстрого нахождения установленных программ. Когда поиск производится по параметрам, можно быстро найти настройки и опции в Панели управления. Когда же в поле **Поиск** (Search) выбрана опция **Файлы** (Files), можно быстро найти файлы.

Один из способов быстрого запуска программы заключается в следующем: нажмите клавишу <Windows> и введите название программы, а затем нажмите клавишу <Enter>. Появится панель поиска, содержащая результаты поиска по приложениям (по умолчанию).

Нажатие клавиши <Windows> позволяет переключаться между экраном **Пуск** и рабочим столом (при работе с параметрами компьютера — между экранами **Пуск** и **Параметры компьютера** (PC Setings)). На экране **Пуск** также есть плитка **Рабочий стол** (Desktop), нажатие которой приводит к переключению на рабочий стол. Также можно перейти на рабочий стол, нажав комбинацию клавиш <Windows>+<D>. Нажмите комбинацию клавиш <Windows>+<,>, чтобы получить возможность выбора элементов рабочего стола (данная комбинация работает, когда активен рабочий стол и позволяет выбрать его элементы без использования мыши). Запустить Панель управления проще всего с экрана **Пуск** — нажмите плитку **Панель управления** (Control Panel) (пальцем или мышью). С рабочего стола можно отобразить Панель управления через панель **Charms**: откройте ее, потом выберите команду **Параметры** (Settings), а затем — команду **Панель управления**. Поскольку Про-

водник (File Explorer) прикреплен к панели задач рабочего стола по умолчанию, можно также добраться до Панели управления таким способом:

1. Откройте Проводник, нажав его значок на панели задач.
2. Нажмите (или щелкните мышью) стрелку вверх слева от списка адресов.
3. Выберите элемент **Панель управления**.

У экрана **Пуск** и рабочего стола есть удобное меню, которое можно отобразить, щелкнув правой кнопкой мыши (или используя нажатие и удержание при работе с сенсорным экраном) по левому нижнему углу экрана **Пуск** или рабочего стола. В этом меню[1] находятся команды **Командная строка** (Command Prompt), **Командная строка (администратор)** (Command Prompt (Admin)), **Диспетчер устройств** (Device Manager), **Просмотр событий** (Event Viewer), **Система** (System), **Диспетчер задач** (Task Manager). На экране **Пуск** скрытая кнопка в левом нижнем углу экрана показывает миниатюру рабочего стола. Нажатие пальцем или мышью этой кнопки приведет к переключению на рабочий стол. На рабочем столе такая же скрытая кнопка в левом нижнем углу экрана показывает миниатюру экрана **Пуск**, при ее нажатии происходит переключение на экран **Пуск**. Нажатие пальцем и удерживание (или щелчок правой кнопкой мыши) этой миниатюры и приводит к отображению того самого меню.

Теперь **Завершение работы** (Shutdown) и **Перезагрузка** (Reboot) — это опции параметра **Выключение** (Power). Это означает, что для завершения работы или перезагрузки сервера нужно выполнить следующие шаги:

1. Откройте боковую панель **Charms** с помощью скольжения от правой стороны экрана к центру или переместив указатель мыши в верхний или нижний угол экрана.
2. Нажмите (или щелкните мышью) кнопку **Параметры** (Settings), а затем нажмите кнопку **Выключение**.
3. Нажмите кнопку **Завершение работы** или кнопку **Перезагрузка**.

Альтернативно можно нажать физическую кнопку питания на сервере, чтобы инициировать "вежливое" завершение работы — сначала будет произведен выход пользователя из системы, а затем завершение работы. На корпусах компьютеров настольного класса обычно есть кнопка сна (Sleep), по умолчанию она отключена, как и реакция на закрытие крышки для портативных компьютеров. Дополнительно серверы настроены на выключение после 10 минут неактивности.

Операционные системы Windows 8 и Windows Server 2012 поддерживают спецификацию APCI 5.0 (Advanced Configuration and Power Interface, усовершенствованный интерфейс конфигурации и управления питанием). Windows использует интерфейс ACPI для управления питанием системы и отдельно взятых устройств, переводя устройства из рабочего состояния в состояние низкого энергопотребления, чтобы уменьшить потребление энергии.

Настройки питания для компьютера берутся из схемы управления питанием. Изменить схемы управления питанием можно в Панели управления: щелкните по ссылке **Система и безопасность** (System and Security), а затем — по ссылке **Электропитание** (Power Options).

В ОС Windows Server 2012 также есть утилита Power Configuration (powercfg.exe), используемая для управления параметрами питания из командной строки. В командной строке можно просмотреть доступные схемы управления питанием, введя команду `powercfg /l`.

[1] Это меню можно также открыть с помощью комбинации клавиш <Windows>+<X>. — *Прим. пер.*

Активная схема питания будет отмечена звездочкой. По умолчанию активная схема управления питанием называется **Сбалансированная** (Balanced) и настроена так:

- жесткие диски никогда не выключаются (при желании можно настроить выключение жестких дисков по прошествии некоторого времени неактивности);
- отключены любые события пробуждения компьютера (при желании можно включить события пробуждения);
- разрешено временное отключение USB-порта (можно его отключить);
- используется умеренное энергосбережение при простое связей PCI Express;
- используется активная политика охлаждения системы, которая повышает скорость вентиляторов перед замедлением процессоров (можно использовать пассивную систему охлаждения, которая замедляет процессоры перед увеличением скорости вентиляторов);
- если поддерживается, используются минимальные и максимальные состояния процессоров (в противовес можно использовать фиксированное состояние).

> ***Примечание***
>
> Управление электропитанием — важный вопрос, тем более что в последнее время большое внимание уделяется экологии. Экономия электроэнергии также может экономить деньги предприятия, а в некоторых случаях позволяет установить больше серверов в центрах данных. Если установить Windows Server 2012 на ноутбук — для тестирования или персонального использования — параметры питания будут немного отличаться: появятся параметры, относящиеся к работе от батареи.

Параметры управления питанием

Для управления питанием важно сфокусироваться на следующем:

- режимы охлаждения;
- состояния устройств;
- состояния процессора.

Интерфейс ACPI определяет активные и пассивные модели охлаждения. Эти модели связаны друг с другом обратно пропорционально.

- Пассивное охлаждение понижает производительность системы, но оно более тихое, поскольку меньше шума от вентиляторов. Используя пассивное охлаждение, Windows уменьшает потребляемую мощность, чтобы снизить рабочую температуру компьютера, но за счет производительности системы. Windows уменьшает скорость процессора в попытке охладить компьютер, а потом уже увеличивает скорость работы вентилятора, которая бы увеличила потребление энергии.
- Активное охлаждение позволяет достичь максимальной производительности. При активном охлаждении Windows увеличивает потребление энергии для снижения температуры машины. В этом случае Windows увеличивает скорость вентиляторов для охлаждения компьютера перед попыткой снизить скорость процессора.

Политика управления питанием ограничивает состояние процессора верхним и нижним пределами, называемыми *максимальным* и *минимальным состояниями процессора* соответственно. Эти состояния реализованы с использованием функции ACPI 3.0 (и более поздними версиями) и называются регулировкой процессора. Состояния ACPI 3.0 определяют диапазон допустимой производительности процессора, который может использоваться опе-

рационной системой Windows. При установке максимальных и минимальных значений определяются границы для разрешенных состояний производительности или же используется одно и то же значение, чтобы система оставалась в одном состоянии производительности. Операционная система Windows уменьшает потребляемую энергию, регулируя скорость процессора. Например, если верхняя граница равна 100%, а нижняя граница — 5%, Windows может отрегулировать работу процессора в этом диапазоне для уменьшения потребляемой энергии. В компьютере, оснащенном процессором с частотой 3 ГГц, Windows может установить частоты процессора в диапазоне от 0,15 до 3 ГГц.

Регулировка процессора и связанные состояния производительности впервые появились в Windows XP и не являются новинкой, но ранние реализации были разработаны для одноядерных, а не многоядерных процессоров. В результате они неэффективно снижали потребляемую энергию на компьютерах с логическими процессорами. Windows 7 и более поздние версии Windows снижают потребление энергии на компьютерах с многоядерными процессорами, используя функцию ACPI 4.0, называемую *логическим бездействием процессора*, и обновляя функции регулировки процессора для работы с несколькими его ядрами.

Логическое бездействие процессора разработано для того, чтобы удостовериться, что Windows использует наименьшее число ядер процессора для данной рабочей нагрузки. Windows объединяет рабочие нагрузки и распределяет их на наименьшем возможном количестве ядер, приостанавливая неактивные ядра процессора. Когда требуется дополнительная вычислительная мощность, Windows активирует неактивные ядра процессора. Такая функциональность работает в сочетании с управлением состояниями производительности на уровне ядра.

Интерфейс ACPI определяет состояния производительности процессора, называемые *p*-состояниями, и состояния сна процессора, называемые *c*-состояниями. Состояния производительности процессора: P0 (процессор/ядро настроено на максимальную производительность и максимально потребляет энергию), P1 (процессор/ядро работает на частоте чуть ниже максимума и использует меньше энергии, чем максимальная мощность), P*n* (где состояние *n* — максимальное число, зависимое от процессора; процессор/ядро работает на минимально возможной частоте и потребляет минимальную энергию, оставаясь в активном состоянии).

Состояния сна процессора: C0 (процессор/ядро могут выполнять инструкции), C1 (у процессора/ядра минимальная задержка, и они находятся в невыполняемом состоянии), C2 (более длинная задержка, чтобы улучшить экономию электропитания по сравнению с состоянием C1), C3 (самая длинная задержка и самая большая экономия электроэнергии по сравнению с состояниями C1 и C2).

Дополнительная информация

Интерфейс ACPI 4.0 вышел в июне 2009 г., а ACPI 5.0 — в декабре 2011 г. У компьютеров, созданных до этого времени, вероятно, не будет полностью совместимого встроенного микропрограммного обеспечения (BIOS), и вам, вероятно, придется обновить его. Для некоторых компьютеров, особенно старых, вообще нет возможности обновить микропрограммное обеспечение, чтобы сделать компьютер полностью совместимым с ACPI 4.0 или ACPI 5.0. Например, если при настройке питания отсутствуют опции, задающие минимальное и максимальное состояния процессора, используемое микропрограммное обеспечение не полностью совместимо с ACPI 3.0, следовательно, оно не полностью совместимо и с более поздними модификациями (ACPI 4.0 и ACPI 5.0). Однако на всякий случай проверьте веб-сайт производителя оборудования на предмет доступных обновлений.

Переключения между состояниями (между любыми *p*-состояниями и из состояния C1 в C0) происходят практически мгновенно (за доли миллисекунд). Состояния глубокого сна не используются Windows, поэтому можно не беспокоиться относительно потери производи-

тельности при пробуждении процессора/ядра. Процессор/ядро будут доступны сразу же, как только понадобятся. Это означает, что самый простой способ ограничить управление питанием процессора — модифицировать активную схему питания и установить минимальное и максимальное состояния процессора равными 100%.

Бездействие логического процессора используется, чтобы уменьшить потребляемую мощность. При этом удаляется логический процессор из списка процессоров, используемых для неаффинизированной работы. Однако эффективность этой функции снижается процессор-аффинизированной работой[1]. Поэтому нужно тщательно спланировать параметры аффинизации приложений. Менеджер системных ресурсов Windows (Windows System Resource Manager) позволяет управлять ресурсами процессора путем установки процента использования процессора и правил аффинизации процессора. Оба метода уменьшают эффективность бездействия логического процессора.

Операционная система Windows экономит электроэнергию, переводя ядра процессора в надлежащие *p*- и *c*-состояния. На компьютере с четырьмя логическими процессорами Windows могла бы использовать *p*-состояния от 0 до 5, где P0 — 100%-е использование, P1 — 90%-е использование, P2 — 80%-е использование, P3 — 70%-е использование, P4 — 60%-е, P5 — 50%-е использование. Когда компьютер активен, логический процессор 0, скорее всего, тоже активен в *p*-состоянии от 0 до 5, а другие процессоры, вероятно, будут в соответствующем *p*-состоянии или в состоянии сна. На рис. 1.1 показано, что логический процессор 1 достигает производительности в 90%, логический процессор 2 — 80%, логический процессор 3 — 50%, а логический процессор 4 находится в состоянии сна.

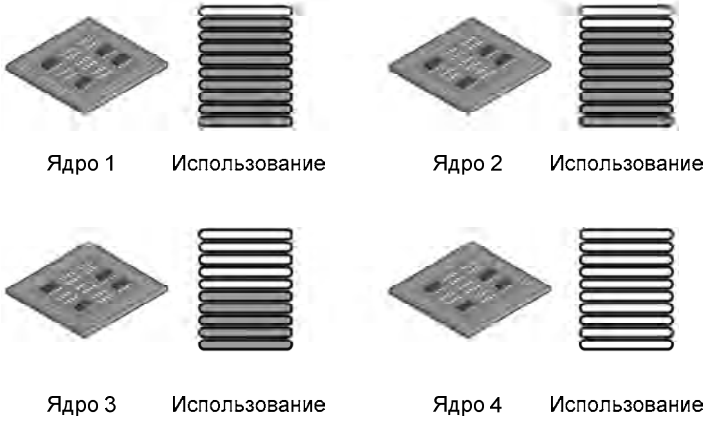


Рис. 1.1. Понимание состояний процессоров

Практический совет

Интерфейсы ACPI 4.0 и ACPI 5.0 определяют четыре глобальных состояния питания. Состояние G0 — рабочее состояние, в котором выполняется программное обеспечение, наивысшее потребление энергии и наименьшая латентность. Состояние G1 — состояние сна, в этом состоянии программное обеспечение не выполняется, латентность варьируется

[1] Речь идет об аффинизированной и неаффинизированной работе. При аффинизированной работе каждый поток должен работать только на строго определенном наборе процессоров/ядер или только на одном определенном процессоре/ядре. При неаффинизированной работе поток может выполняться на любом процессоре/ядре. Процессор-аффинизированная работа снижает эффективность экономии энергии, поскольку может найтись поток, который должен работать на том процессоре/ядре, который система могла бы перевести в спящее состояние и тем самым сэкономить энергию. — *Прим. пер.*

в зависимости от состояния сна, а потребление энергии меньше, чем в состоянии G0. Состояние G2 (также называется состоянием сна S5) — "мягкое" выключение, когда операционная система не выполняется, задержка длинная, а потребляемая энергия близка к нулю. Состояние G3, состояние механического выключения, операционная система не работает, задержка огромная, потребление энергии равно 0. Есть также специальное глобальное состояние, известное как S4 (энергонезависимый сон), в котором операционная система записывает весь системный контекст в файл на носителе энергонезависимой памяти, благодаря этому системный контекст может быть сохранен и восстановлен.

В глобальном состоянии сна, в G1, есть разные варианты сна. S1 — состояние сна, в котором сохраняется весь системный контекст. S2 — состояние сна, подобное S1 за исключением того, что контексты центрального процессора и системного кэша потеряны, управление запускается со сброса. S3 — состояние сна, где потеряны контексты процессора, кэша и чипсета, аппаратные средства поддерживают контекст памяти и восстанавливают некоторые контексты конфигурации процессора и L2-кэша. S4 — состояние сна, в котором предполагается, что аппаратные средства выключили все устройства, чтобы уменьшить использование питания до минимума, сохраняется только контекст платформы. S5 — состояние сна, в котором предполагается, что аппаратные средства находятся в состоянии "мягкого" отключения, никакой контекст не сохраняется, при пробуждении требуется полная начальная загрузка.

Устройства также имеют состояния питания. D0 — устройство потребляет максимум энергии. D1 и D2 — промежуточные состояния, которые не используются многими устройствами. D3hot — состояние экономии электроэнергии, при котором сохраняется контекст устройства. D3 — состояние выключения, при котором контекст устройства потерян полностью, а система должна повторно инициализировать устройство, чтобы снова использовать его.

Сетевые утилиты и протоколы

В Windows Server 2012 есть целый набор сетевых утилит: Обозреватель сети (Network Explorer), Центр управления сетями и общим доступом (Network and Sharing Center), Диагностика сети (устранение неполадок). На рис. 1.2 изображен Центр управления сетями и общим доступом.

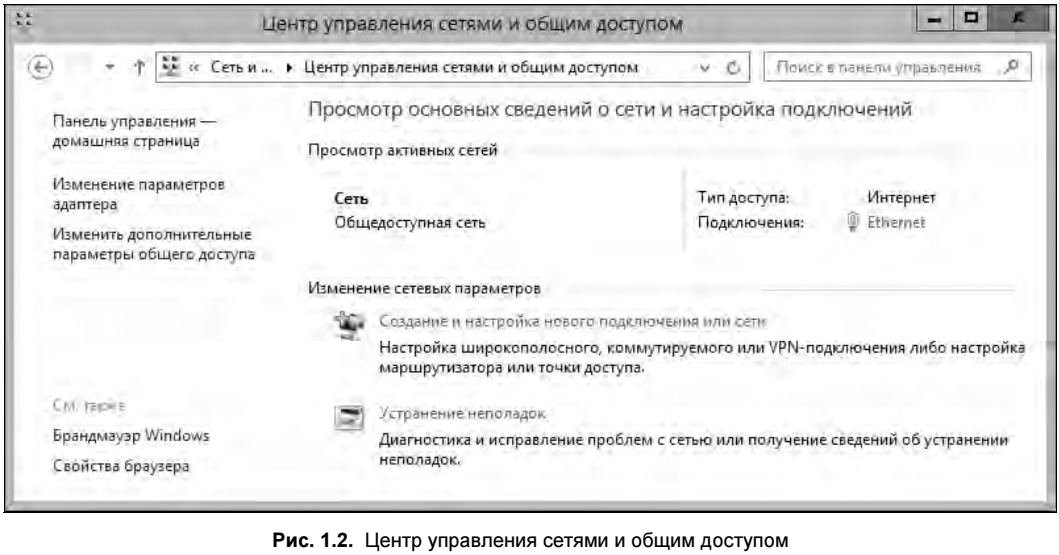


Рис. 1.2. Центр управления сетями и общим доступом предоставляет быстрый доступ к различным сетевым функциям

Сетевые настройки

Предоставление общего доступа и сетевое обнаружение — базовые параметры Центра управления сетями и общим доступом. Если сетевое обнаружение включено и сервер подключен к сети, то сервер может видеть остальные компьютеры сети и другие сетевые устройства. При этом сам сервер тоже виден в сети. Если общий доступ включен или выключен, доступны различные параметры, которые могут быть разрешены или запрещены. Как будет показано в *главе 12*, доступны опции предоставления общего доступа к файлам и папкам, принтеру, а также общий доступ с защитой паролем.

В Windows 8 и Windows Server 2012 доступны сети следующих типов:

- *домен* — сеть, в которой компьютеры подключены к корпоративному домену;
- *рабочая сеть* — частная сеть, в которой компьютеры настроены как члены рабочей группы и не подключены напрямую к Интернету;
- *домашняя сеть* — частная сеть, в которой компьютеры настроены как члены домашней группы и не подключены напрямую к Интернету;
- *общедоступная (публичная) сеть* — публичная сеть, в которой компьютеры подключены к сети в публичном месте, например в кафе или аэропорту, но это не внутренняя сеть.

Эти типы сетей организованы в три категории: домашняя или рабочая, домен и общедоступная. У каждой категории есть связанный сетевой профиль. Поскольку компьютер сохраняет параметры общего доступа и брандмауэра отдельно для каждой категории сети, можно использовать различные настройки блокировки/разрешения. При подключении к сети появится диалоговое окно, предлагающее выбрать категорию сети. Если выбрать вариант **Частная** (Private) и компьютер определит, что сеть подключена к корпоративному домену, устанавливается категория сети **Домен** (Domain Network).

В зависимости от категории сети, Windows Server включает или отключает обнаружение сети. Состояние **Включено** (On) означает, что компьютер может обнаружить другие компьютеры и сетевые устройства в сети и что остальные компьютеры сети могут увидеть этот компьютер. Состояние **Отключено** (Off) означает, что ни компьютер, ни другие устройства сети или компьютеры не могут обнаружить друг друга.

Используя окно **Сеть** (Network) или **Дополнительные параметры общего доступа** (Advanced Sharing Settings), открываемые из Центра управления сетями и общим доступом, можно включить сетевое обнаружение и общий доступ к файлам. Однако из соображений безопасности сетевое обнаружение и общий доступ по умолчанию блокируются для публичной сети. Когда сетевое обнаружение и общий доступ отключены, общие файлы и принтеры недоступны другим компьютерам сети. Вдобавок и некоторые программы могут не получить доступ к сети.

Работа с сетевыми протоколами

Чтобы разрешить серверу доступ к сети, нужно установить поддержку TCP/IP и сетевой адаптер. По умолчанию Windows Server использует TCP/IP как протокол глобальной сети (Wide Area Network, WAN). Поддержка TCP/IP устанавливается при инсталляции операционной системы. Можно также использовать TCP/IP в локальной сети.

Протоколы TCP и IP позволяют компьютерам взаимодействовать по различным сетям и Интернету с помощью сетевых адаптеров. Windows 7 и более поздние версии Windows обладают двухуровневой архитектурой уровня IP, в которой реализованы и разделяют транспортный и сетевой уровни обе версии протокола IP — IPv4 и IPv6.

Протокол IPv4 использует 32-разрядные адреса и является основной версией протокола IP для большинства сетей, в том числе Интернета. Протокол IPv6 использует 128-разрядные адреса и является следующим поколением протокола IP.

Примечание

DirectAccess-клиенты передают только IPv6-трафик по DirectAccess-соединению на DirectAccess-сервер. Благодаря поддержке NAT64/DNS64 на Windows Server 2012 DirectAccess-сервере, DirectAccess-клиенты могут теперь инициировать связь с IPv4-узлами в корпоративной сети. NAT64/DNS64 работают вместе для трансляции трафика входящего соединения от узла IPv6 в трафик IPv4. NAT64 транслирует входящий IPv6-трафик в IPv4-трафик и осуществляет обратное преобразование трафика. DNS64 разрешает имя узла IPv4-узла в IPv6-адрес.

Практический совет

Функция Разгрузка TCP Chimney (TCP Chimney Offload) была представлена с Windows Vista и Windows Server 2008. Она позволяет сетевой подсистеме разгрузить обработку TCP/IP-соединения с центрального процессора компьютера на его сетевой адаптер, если сетевой адаптер поддерживает процесс TCP/IP-разгрузки. Разгрузить можно оба типа соединений — TCP/IPv4 и TCP/IPv6. В Windows 7 и более поздних версиях Windows по умолчанию разгружаются TCP-соединения на 10-гигабитных (10 Гбит/с) сетевых адаптерах, 1-гигабитные сетевые адаптеры по умолчанию не разгружаются. Чтобы разгрузить TCP-соединения на адаптере со скоростью передачи данных 1 или 10 Гбит/с, нужно сначала включить TCP-разгрузку с помощью следующей команды, введенной в командной строке с правами администратора: `netsh int tcp set global chimney=enabled`. Проверить статус TCP-разгрузки можно путем ввода команды `netsh int tcp show global`. Хотя TCP-разгрузка работает с Брандмауэром Windows, TCP-разгрузка не может быть использована с IPsec, виртуализацией Windows (Hyper-V), балансировкой сетевой нагрузки и с сервисом NAT. Чтобы определить, работает ли TCP-разгрузка, введите команду `netstat -t` и проверьте статус разгрузки. Состояние разгрузки будет указано в колонке **Состояние разгрузки**: offloaded (разгружено) или InHost (не разгружено). Windows также использует технологии Receive-side Scaling (RSS) и Net-DMA (Network Direct Memory Access). Включить или отключить RSS можно с помощью команды `netsh int tcp set global rss=enabled` или `netsh int tcp set global rss=disabled` соответственно. Для проверки статуса RSS введите команду `netsh int tcp show global`. Включить или выключить Net-DMA можно путем установки ключа реестра `DWord`-значения `EnableTCPA` в `1` или `0` соответственно. Этот ключ находится в разделе `HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\ Tcpip\Parameters`.

32-битные IPv4-адреса обычно представлены четырьмя отдельными десятичными значениями, например 127.0.01 или 192.168.10.52. Четыре десятичных значения также называются *октетами*, поскольку каждое представляет 8 бит в 32-битном числе. В IPv4-адресации часть IP-адреса представляет идентификатор сети, а другая часть — идентификатор компьютера. IPv4-адрес узла и внутренний адрес машины (MAC-адрес) сетевого адаптера никак не связаны друг с другом.

При IPv6-адресации используются 128-битные адреса, которые делятся на восемь 16-битных блоков, разделенных двоеточиями. Каждый 16-битный блок представлен в шестнадцатеричной форме, например, FEC0:0:0:02BC:FF:BECB:FE4F:961D. В обычной одноадресной IPv6-адресации первые 64 бита представляют идентификатор сети, а последние 64 бита — сетевой интерфейс. Поскольку многие блоки в IPv6-адресах равны 0, последовательность нулевых блоков может быть заменена символами "::" — так называемым двойным двоеточием. С помощью двойного двоеточия нулевые блоки в предыдущем адресе можно сжать так: FEC0::02BC:FF:BECB:FE4F:961D. Три и более нуля сжимаются так же, например, FFE8:0:0:0:0:0:0:1 превратится в FFE8::1.

Если при установке операционной системы будет обнаружено сетевое оборудование, по умолчанию будет включена поддержка и IPv4, и IPv6. Не нужно отдельно устанавливать компонент для обеспечения поддержки IPv6. В Windows 7 и более поздних версиях Windows применяется измененная IP-архитектура, она называется *следующим поколением TCP/IP-стека* (Next Generation TCP/IP) и содержит множество улучшений использования IPv4 и IPv6.

Контроллеры домена, рядовые серверы и службы домена

При установке Windows Server 2012 на новую систему можно настроить сервер как рядовой сервер, контроллер домена или автономный сервер. Важно понимать разницу между этими типами серверов. Рядовые серверы являются частью домена, но не хранят информацию каталога. Контроллеры домена отличаются от рядовых серверов тем, что хранят информацию каталога, производят аутентификацию и предоставляют сервисы для домена. Автономные серверы не являются частью домена. Поскольку у автономных серверов собственные базы данных, они требуют отдельной аутентификации.

Работа с Active Directory

Операционная система Windows Server 2012 поддерживает модель репликации с несколькими хозяевами (multi-master). В этой модели любой контроллер домена может обрабатывать изменения каталога, затем эти изменения могут реплицироваться между остальными контроллерами домена автоматически. Windows Server распространяет всю информацию каталога, называемую *хранилищем данных*. Внутри хранилища находятся наборы объектов, представляющих учетные записи пользователя, группы, компьютера, а также информация об общих ресурсах — серверах, файлах и принтерах.

Домены, которые используют ActiveDirectory, также называются ActiveDirectory-доменами. Хотя эти домены могут работать только на одном контроллере домена, обычно в сети есть несколько контроллеров. В этом случае если один контроллер будет недоступен, остальные контроллеры домена смогут обрабатывать аутентификации и выполнять другие критические задачи.

По сравнению с Windows Server 2008 Microsoft внесла некоторые фундаментальные изменения в Active Directory. В результате Microsoft перестроила функциональность каталога и создала целое семейство связанных служб.

- **Службы сертификатов Active Directory (Active Directory Certificate Services, AD CS).** Предоставляют функциональность, необходимую для выпуска и освобождения цифровых сертификатов пользователей, клиентских компьютеров и серверов. Служба AD CS использует центры сертификации (CA), ответственные за подтверждение идентификации пользователей и компьютеров, а также за выпуск сертификатов подтверждения этих идентификационных данных. У доменов есть корпоративные корневые сертификационные центры, которые являются сертификационными серверами на вершине сертификационной иерархии для доменов и пользуются наибольшим доверием в корпоративной сети, и подчиненные центры сертификации, которые являются членами существующей корпоративной сертификационной иерархии. У рабочих групп есть свои автономные корневые сертификационные центры, которые являются сертификационными серверами

на вершине некорпоративной сертификационной иерархии, а также автономные подчиненные центры сертификации, которые являются членами существующей некорпоративной сертификационной иерархии.

- **Доменные службы Active Directory (Active Directory Domain Services, AD DS).** Обеспечивают службы каталогов, необходимые для установки домена, включая хранилище данных, в котором содержится информация об объектах в сети. Эта же служба делает всю данную информацию доступной для пользователей домена. AD DS использует контроллеры домена для управления доступом к сетевым ресурсам. Как только пользователи аутентифицировали себя при входе в домен, их учетные записи используются для доступа к ресурсам сети. Поскольку AD DS — основа Active Directory, необходимая для работы каталогозависимых приложений и технологий, в книге эта служба будет называться просто Active Directory, а не Active Directory Domain Services или AD DS.
- **Службы федерации Active Directory (Active Directory Federation Services, AD FS).** Дополняют функции аутентификации и управления доступом AD DS, расширяя их до WWW. AD FS использует веб-агенты для предоставления пользователям доступа к внутренним (внутри корпоративной сети) веб-приложениям, для управления доступом клиентов используются прокси. Как только служба AD FS настроена, пользователи могут использовать свои цифровые идентификационные данные для аутентификации в веб. Доступ к внутренним веб-приложениям осуществляется с помощью веб-браузера, например Internet Explorer.
- **Службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services, AD LDS).** Предоставляют хранилище данных для каталогозависимых приложений, которые не требуют AD DS и которые не должны размещаться на контроллерах доменов. AD LDS не выполняется как служба операционной системы и может использоваться как в домене, так и в рабочей группе. Каждое приложение, которое работает на сервере, может иметь свое хранилище данных, реализованное с помощью AD LDS.
- **Службы управления правами Active Directory (Active Directory Right Management Services, AD RMS).** Предоставляют уровень защиты информации организации, которая может распространяться за пределы корпоративной сети, например, сообщения e-mail, документы, веб-страницы интрасети — все это может быть защищено от несанкционированного доступа. AD RMS использует: сервис сертификации для выпуска правильных сертификатов учетных записей, позволяющих идентифицировать пользователей, группы и сервисы; службу лицензирования, предоставляющую авторизированным пользователям, группам и сервисам доступ к защищенной информации; сервис протоколирования, чтобы контролировать и обслуживать службу управления правами. Как только доверие будет установлено, пользователи с правильным сертификатом учетной записи смогут получить права на доступ к информации. Эти права определяют, какие пользователи могут получить доступ к информации и что они смогут с ней сделать. Пользователи с подтвержденными сертификатами учетной записи также могут получить доступ к защищенному контенту. Шифрование гарантирует, что доступ к информации контролируется с обеих сторон — изнутри и снаружи предприятия.

Microsoft представила дополнительные изменения в Windows Server 2012: новый функциональный уровень домена (называемый *функциональным уровнем домена Windows Server 2012*), новый функциональный уровень леса *(функциональный уровень леса Windows Server 2012)*. Другие изменения рассматриваются в *главе 6*.

Контроллеры домена только для чтения

ОС Windows Server 2008 и более поздние версии поддерживают так называемые контроллеры домена только для чтения и перезапускаемые доменные службы Active Directory (Restartable Active Directory Domain Services). Контроллер домена только для чтения (read-only domain controller, RODC) — дополнительный контроллер домена, содержащий копию хранилища данных Active Directory, доступную только для чтения. RODC идеально подходит для филиалов, где не гарантирована физическая безопасность контроллера домена. За исключением паролей, на RODC хранятся те же объекты и атрибуты, как и на обычном (перезаписываемом) контроллере домена. Эти объекты и атрибуты реплицированы в RODC посредством однонаправленной репликации от перезаписываемого контроллера домена, который работает как партнер по репликации.

Поскольку RODC по умолчанию не хранят пароли или учетные данные, кроме их собственной учетной записи компьютера и цели Kerberos (Kerberos Target, Krbtgt), RODC получает учетные записи пользователя и компьютера от перезаписываемого контроллера домена, который работает под управлением Windows Server 2008 или более новых версий. Если это разрешено политикой репликации пароля, заданной на перезаписываемом контроллере домена, RODC получает и кэширует учетные записи по мере необходимости, пока эти учетные данные не изменятся. Поскольку на RODC хранится только подмножество учетных записей, это существенно сужает число учетных данных, которые могут быть скомпрометированы.

> ***Совет***
>
> Любой пользователь домена может быть делегирован как локальный администратор RODC без других прав в домене. RODC может выступать в роли глобального каталога, но не может работать в роли мастера операций. Хотя RODC-серверы могут получать информацию от контроллеров домена, работающих под управлением Windows Server 2003, обновления раздела домена могут быть получены только от перезаписываемого контроллера домена, работающего под управлением Windows Server 2008 или более новых версий.

Перезапускаемые доменные службы Active Directory

Перезапускаемые доменные службы Active Directory (Restartable Active Directory Domain Services) — функция, позволяющая администратору запускать и останавливать AD DS. В консоли **Службы** (Services) на контроллерах домена доступна служба **Доменные службы Active Directory** (Active Directory Domain Services), позволяющая легко остановить и перезапустить AD DS, как и любую другую службу, которая локально запущена на сервере. Пока служба **Доменные службы Active Directory** остановлена, можно выполнить задачи по техническому обслуживанию, которые могут потребовать перезапуска сервера, например, оффлайн-дефрагментация базы данных Active Directory, применение обновлений операционной системы или инициирование авторитетного восстановления. При остановленной службе **Доменные службы Active Directory** на сервере другие контроллеры домена могут обрабатывать задачи аутентификации и входа в систему. Кэшируемые учетные данные, смарт-карты и биометрические методы входа в систему все еще будут работать. Если же в сети нет других доступных контроллеров домена, ни один из этих методов входа в систему работать не будет. Однако все еще можно будет войти в систему сервера, используя режим восстановления служб каталогов (Directory Services Restore Mode).

Все контроллеры домена, работающие под управлением Windows Server 2008 и более новых версий, поддерживают перезапускаемые доменные службы Active Directory, даже RODC.

Администратор имеет право запустить или остановить AD DS, используя запись **Контроллер домена** (Domain Controller) в утилите **Службы** (Services).

Учитывая перезапускаемые доменные службы Active Directory, контроллеры домена под управлением Windows Server 2008 (или более поздние версии) могут находиться в одном из трех состояний.

- **Active Directory запущен** (Active Directory Started) — у контроллера домена такое же состояние, как у Windows 2000 Server и Windows Server 2003. В этом состоянии контроллер домена может предоставлять услуги аутентификации и входа в систему для домена.
- **Active Directory остановлен** (Active Directory Stopped) — Active Directory остановлен, и контроллер домена больше не может предоставлять услуги аутентификации и входа для домена. В этом режиме сохраняются некоторые характеристики рядового сервера и контроллера домена в режиме DSRM (Directory Services Restore Mode). Как рядовой сервер, этот сервер может присоединяться к домену. Пользователи могут входить интерактивно с помощью кэшированных учетных данных, смарт-карт и биометрических методов входа. Пользователи также могут входить по сети с использованием других контроллеров домена. Как и в режиме DSRM, база данных Active Directory (Ntds.dit) на локальном контроллере домена находится в отключенном состоянии. Это означает, что можно выполнять оффлайн-операции AD DS, например, дефрагментацию базы данных, обновление приложений без необходимости перезагрузки контроллера домена.
- **Режим восстановления службы каталогов (Directory Services Restore Mode)** — Active Directory в режиме восстановления. Такое же состояние восстановления есть и в контроллере домена под управлением Windows Server 2003. В этом режиме разрешается проводить авторитетное или неавторитетное восстановление базы данных Active Directory.

При работе с AD DS в остановленном состоянии следует помнить, что зависимые сервисы также отключены (когда остановлена служба AD DS). Это означает, что **Служба репликации файлов** (File Replication Service, FRS), **Центр распределения ключей Kerberos** (Kerberos Key Distribution Center, KDC) и **Служба межсайтовых сообщений** (Intersite Messaging) будут остановлены перед остановкой Active Directory. Даже если они запущены, эти зависимые сервисы будут перезапущены при перезапуске Active Directory. Далее можно перезапустить контроллер домена в режиме DSRM, но нельзя запустить контроллер домена в остановленном состоянии. Чтобы остановить Active Directory, нужно сначала запустить контроллер домена, а затем остановить службу AD DS.

Сервисы разрешения имен

Операционная система Windows использует разрешение имен для более простого взаимодействия с другими компьютерами сети. Разрешение имен ставит в соответствие имена компьютеров числовым IP-адресам, которые используются для сетевого взаимодействия. Таким образом, вместо того чтобы использовать длинные последовательности цифр, пользователи могут получить доступ к компьютеру в сети при помощи дружественного имени.

Современные операционные системы Windows поддерживают три системы разрешения имен:

- систему доменных имен (Domain Name System, DNS);
- службу имен Интернета для Windows (Windows Internet Name Service, WINS);
- протокол LLMNR (Link-Local Multicast Name Resolution).

В следующих разделах мы рассмотрим все эти три системы.

Система доменных имен

Система доменных имен (Domain Name System, DNS) — сервис разрешения имен компьютеров в IP-адреса. С помощью DNS можно преобразовать полное имя узла, например **computer84.cpandl.com**, в IP-адрес. DNS работает по стеку протокола TCP/IP и может быть интегрирована с WINS, протоколом динамического конфигурирования узлов (DHCP) и Active Directory Domain Services. Как будет показано в *главе 15*, DHCP используется для динамической IP-адресации и конфигурации протокола TCP/IP.

Система DNS организует группы компьютеров в домены. Эти домены собраны в иерархическую структуру, которая служит основой для всего Интернета (для публичных сетей) и для корпоративных сетей (для частных сетей, известных так же как *intranets* и *extranets*). Для идентификации отдельных компьютеров, доменов организаций и доменов верхнего уровня используются различные уровни иерархии. Например, если полное имя узла **computer84.cpandl.com**, то **computer84** — имя компьютера, **cpandl** — домен организации, а **com** — домен верхнего уровня.

Домены верхнего уровня являются корневыми в DNS-иерархии, поэтому они также называются *корневыми доменами*. Эти домены организованы географически, по типу организации и по функции. Домены вроде **cpandl.com** также называются *родительскими доменами*, поскольку являются таковыми в организационной структуре. Родительские домены могут делиться на поддомены, которые используются для групп и департаментов в пределах организации.

Поддомены часто называют *дочерними доменами*. Например, пусть полное доменное имя (Fully Qualified Domain Name, FQDN) узла будет **jacob.hr.cpandl.com**. Здесь **jacob** — имя компьютера, **hr** — дочерний домен для группы отдела кадров (human resources), а **cpandl.com** — родительский домен.

Домены Active Directory используют DNS для реализации своей структуры имен и иерархии. Active Directory и DNS очень тесно интегрированы, поэтому перед установкой первичного контроллера домена нужно сначала установить DNS-сервер. Во время установки первого контроллера домена в ActiveDirectory-сети будет возможность установить DNS-сервер автоматически, если DNS-сервер не найден в сети. Также нужно указать, должны ли сервисы DNS и Active Directory быть полностью интегрированы. В большинстве случаев необходимо утвердительно ответить на оба запроса. При полной интеграции информация DNS хранится непосредственно в Active Directory, что позволяет использовать все возможности Active Directory.

Важно понимать разницу между полной и частичной интеграцией.

- При *частичной интеграции* домен использует стандартное файловое хранилище. DNS-информация хранится в текстовых файлах с расширением dns, по умолчанию они находятся в каталоге *%SystemRoot%*\System32\Dns. Обновления в DNS обрабатываются одним авторитетным DNS-сервером, который определяется как первичный DNS-сервер для определенного домена или области в пределах домена, называемой *зоной*. Клиенты, которые используют динамические обновления DNS по DHCP, могут быть настроены на использование первичного DNS-сервера в зоне. Если клиенты не настроены, то их DNS-информация не будет обновлена. Аналогично, динамические обновления по DHCP не могут быть выполнены, если первичный DNS-сервер недоступен (оффлайн).
- При *полной интеграции* домен использует хранилище, интегрированное в каталог. DNS-информация хранится непосредственно в Active Directory и доступна через контейнер для объекта dnsZone. Поскольку информация является частью Active Directory, любой

контроллер домена может получить доступ к данным. В результате любой контроллер домена с запущенным DNS-сервером может обрабатывать динамические обновления. Кроме того, клиенты, использующие динамические обновления DNS через DHCP, могут использовать любой DNS-сервер в зоне. Дополнительное преимущество интеграции каталога в том, что это возможность использовать безопасность каталога для контроля доступа к DNS-информации.

Если нужен способ репликации DNS-информации по всей сети, преимущество полной интеграции с Active Directory очевидны. При частичной интеграции DNS-информация хранится и распространяется отдельно от Active Directory. Наличие двух отдельных структур уменьшает эффективность и DNS, и ActiveDirectory, а также усложняет администрирование. Поскольку DNS менее эффективен при репликации, чем Active Directory, можно увеличить сетевой трафик и время, требуемые для репликации DNS-информации по сети.

Чтобы включить DNS в сети, необходимо настроить DNS-клиенты и DNS-серверы. При настройке DNS-клиентов нужно указать IP-адреса DNS-серверов сети. Используя эти адреса, клиенты могут взаимодействовать с DNS-серверами, даже если эти серверы находятся в разных подсетях.

Если сеть использует DHCP, администратор может настроить DHCP на работу с DNS. Чтобы сделать это, нужно установить DHCP-опции 006 DNS Servers и 015 DNS Domain Name *(см. главу 15)*. Дополнительно, если компьютеры в сети должны быть доступны из других доменов Active Directory, необходимо создать записи для них в DNS. DNS-записи организованы в зоны, зона — это просто область домена. Настройка DNS подробно описана в *главе 16*.

Если сервис **DNS-сервер** (DNS Server) устанавливается на RODC, RODC в состоянии получить реплику (только для чтения) всех разделов каталога приложения, которые используются DNS, включая ForestDNSZones и DomainDNSZones. Клиенты могут обращаться к RODC для разрешения имен, как будто это обычный DNS-сервер. Однако, как и с обновлениями каталога, DNS-сервер на RODC не поддерживает прямые обновления. Это означает, что RODC не регистрирует записи NS (Name Server) ни для одной зоны Active Directory, которую он размещает. Когда клиент пытается обновить его DNS-записи, RODC возвращает ссылку на DNS-сервер, который клиент может использовать для обновления. DNS-сервер на RODC должен получить обновленную запись от сервера DNS, который получит информацию об обновлении с использованием специального единичного объекта репликации, работающего в качестве фонового процесса.

Операционная система Windows 7 и более поздние версии поддерживают расширения безопасности DNS (DNS Security Extensions, DNSSEC). DNS-клиент, работающий на этих операционных системах, отправляет запросы, свидетельствующие о поддержке DNSSEC, обрабатывать связанные записи и определять, проверил ли DNS-сервер лично эти записи. На Windows-серверах это позволяет безопасно подписывать зоны и размещать уже DNSSEC-подписанные зоны. Это также позволяет DNS-серверам обрабатывать связанные записи и выполнять проверку допустимости и аутентификацию.

Службы имен Интернета для Windows

Windows Internet Name Service (WINS) — это служба, разрешающая имена компьютеров в IP-адреса. Используя WINS, можно разрешить имя компьютера в сети Microsoft, например COMPUTER84, в соответствующий ему IP-адрес. Служба WINS необходима для поддержки старых систем (до Windows 2000) и старых приложений, которые используют NetBIOS по TCP/IP, например, утилиты командной строки .NET. Если на компьютере нет старых систем

(до Windows 2000) и не используются старые сетевые приложения, нет никакой необходимости в WINS.

WINS лучше всего работает в окружении "клиент/сервер", в котором WINS-клиенты отправляют запросы на разрешение доменного имени WINS-серверам, WINS-серверы разрешают запросы и отвечают серверам. Когда все ваши DNS-серверы работают под управлением Windows Server 2008 или более поздней версии, развертывание зоны Global Names создает статические, глобальные записи одноуровневых доменных имен без использования WINS. Это позволяет пользователям получать доступ к узлам с помощью одноуровневых имен, а не FQDN, и избавляет от WINS. Для передачи WINS-запросов и другой информации компьютеры используют NetBIOS. NetBIOS предоставляет программный интерфейс (API), позволяющий компьютерам взаимодействовать в сети. NetBIOS-приложения используют WINS или файл LMHOSTS для разрешения имен компьютеров в IP-адреса. В старых сетях (до Windows 2000) WINS — это первичный сервис разрешения имен. В Windows 2000 и более поздних версиях в качестве первичного сервиса разрешения имен используется DNS, а у WINS несколько другая функция, которая заключается в разрешении старым компьютерам (до Windows 2000) просматривать список ресурсов сети и в предоставлении возможности Windows 2000 и более новым системам находить NetBIOS-ресурсы.

Чтобы включить в сети разрешение имен средствами WINS, необходимо настроить клиенты и серверы. При настройке WINS-клиентов нужно указать IP-адреса WINS-серверов сети. Используя IP-адреса, клиенты смогут связаться с WINS-серверами, даже если серверы находятся в других подсетях. Также WINS-клиенты могут взаимодействовать широковещательным способом, запрашивая IP-адреса с помощью широковещательных сообщений. Поскольку сообщения широковещательные, WINS-серверы не используются. Любые неWINS-клиенты, поддерживающие этот тип широковещательных сообщений, могут также использовать данный метод для разрешения имен компьютеров в IP-адреса.

Когда клиенты взаимодействуют с WINS-серверами, они устанавливают сеансы. Вот три основных ключевых момента таких сеансов:

- *регистрация имени* — при регистрации имени клиент передает серверу свое имя и свой IP-адрес, а также просит добавить его в базу данных WINS. Если указанное имя и IP-адрес не используются в сети, WINS-сервер принимает запросы и регистрирует клиента в базе данных WINS;
- *обновление имени* — имя регистрируется не навсегда. Вместо этого клиент может использовать это имя ограниченное время, называемое *временем аренды*. Через некоторое время (интервал обновления) клиент должен обновить имя на WINS-сервере;
- *освобождение имени* — если клиент не может обновить аренду, регистрация имени аннулируется, и другой компьютер может использовать это же имя и/или IP-адрес. Освобождение имени также происходит при закрытии WINS-клиента.

После установки клиентом сеанса с WINS-сервером он (клиент) может использовать службы разрешения имен. Метод разрешения имени компьютера зависит от настройки сети. Доступны четыре метода определения имен.

- *B-узел (широковещательный)* — для преобразования имен компьютеров в IP-адреса используются широковещательные сообщения. Компьютеры, которым необходимо разрешить имя, отправляют широковещательное сообщение каждому узлу сети, запрашивая IP-адрес компьютера с определенным именем. В больших сетях с сотнями или тысячами компьютеров широковещательные запросы могут израсходовать ценную пропускную способность сети.

- *P-узел (одноранговый)* — для разрешения имен используются WINS-серверы. Как было показано ранее, сессии клиента делятся на три этапа: регистрация имени, обновление имени и освобождение имени. В этом режиме, когда клиенту требуется преобразовать имя компьютера в IP-адрес, он отправляет запрос серверу, сервер его обрабатывает и отвечает клиенту.
- *M-узел (смешанный)* — комбинируются *B*- и *P*-узел. Сначала WINS-клиент пытается использовать *B*-узел для разрешения имен. Если попытка проваливается, тогда клиент пытается использовать *P*-узел. Поскольку сначала используется *B*-узел, то этот метод порождает те же самые проблемы с пропускной способностью, что и *B*-узел.
- *H-узел (гибридный)* — также является комбинацией *B*- и *P*-узлов. Но в этом случае клиент сначала обращается к WINS-серверу, а если эта попытка не удалась, тогда используются широковещательные сообщения (*B*-узел). Поскольку одноранговый метод — первичный, *H*-узел гарантирует лучшую производительность в большинстве сетей. *H*-узел является методом по умолчанию для WINS.

Если WINS-серверы доступны в сети, Windows-клиенты используют метод *P*-узла для определения имен. Если WINS-серверы недоступны, Windows-клиенты используют метод *B*-узла. Компьютеры под управлением Windows также используют DNS и локальные файлы LMHOSTS и HOSTS для разрешения сетевых имен. Работа с DNS подробно описана в *главе 16*.

Когда используете DHCP для автоматического назначения IP-адресов, нужно установить метод разрешения имен для DHCP-клиентов. Чтобы сделать это, нужно установить DHCP-опции для узла типа 046 WINS/NBT *(см. главу 15)*. Лучший метод — *H*-узел. Он обеспечивает лучшую производительность и уменьшает трафик в сети.

Протокол LLMNR

Протокол LLMNR (Link-Local Multicast Name Resolution) подходит для одноранговых служб разрешения имен для устройств с IP-адресами IPv4 и IPv6, позволяет IPv4- и IPv6-устройствам, находящимся в одной подсети с отсутствующими серверами WINS/DNS, разрешать имена друг друга — сервис, который не могут полностью предоставить ни WINS, ни DNS.

Несмотря на то, что WINS может предоставить разрешение имен как в одноранговых, так и в сетях типа "клиент-сервер", он не поддерживает адреса IPv6. DNS, с другой стороны, поддерживает и IPv4, и IPv6, но это зависит от определенных серверов, предоставляющих услуги разрешения имен.

Операционная система Windows 7 и более поздние версии поддерживают LLMR. Протокол LLMNR разработан для клиентов IPv4/IPv6 и случаев, когда другие системы разрешения имен недоступны, например:

- в домашних сетях или в сетях небольших офисов;
- в сетях ad hoc;
- корпоративных сетях, в которых недоступны DNS-серверы.

Протокол LLMNR разработан в дополнение к протоколу DNS, он позволяет разрешать имена в сценариях, в которых стандартное определение имен (DNS) невозможно. Несмотря на то, что LLMNR может заменить WINS в случаях, когда NetBIOS не требуется, протокол LLMNR нельзя рассматривать как полноценную замену DNS, т. к. он работает только в локальных сетях. Поскольку LLMNR-трафик блокируется маршрутизаторами, он не может использоваться в глобальных сетях.

Как в случае с WINS, LLMNR используется для разрешения имени узла, например **COMPUTER84**, в IP-адрес. По умолчанию LLMNR включен на всех компьютерах, работающих под управлением Windows 7 и более поздних версий, эти компьютеры будут использовать LLMNR только в случаях, когда все попытки найти имя узла через DNS тщетны. В результате процесс разрешения имен в Windows 7 (и более поздних версиях) работает примерно так:

1. Узел отправляет запрос к первичному (предпочитаемому) DNS-серверу. Если узел не получает ответ или возникает ошибка, он обращается к вторичному (альтернативному) DNS-серверу. Если DNS-серверы не сконфигурированы или не получается к ним подключиться без ошибок, компьютер пытается разрешить имя с помощью LLMNR.
2. Узел отправляет широковещательный запрос по протоколу UDP (User Datagram Protocol), запрашивающий IP-адрес искомого компьютера. Этот запрос ограничивается только локальной сетью (также называется *local link*).
3. Каждый компьютер в локальной сети, поддерживающий LLMNR и настроенный на ответ на входящие запросы, принимает этот запрос и сравнивает искомое имя со своим именем. Если имена узлов не совпадают, узел отправляет отрицательный ответ. При совпадении имен компьютер передает исходному узлу одиночное (не широковещательное) сообщение, содержащее IP-адрес этого узла.

Также можно использовать LLMNR для обратного преобразования. При этом компьютер отправляет одноадресный запрос указанному IP-адресу с целью узнать имя узла. Компьютер, поддерживающий LLMNR, получив такой запрос, отправит ответ запрашивающему узлу.

Компьютерам с поддержкой LLMNR нужно убедиться, что их имена уникальные в пределах локальной подсети. В большинстве случаев компьютер проверяет уникальность при запуске, при пробуждении из состояния сна и при изменении параметров сетевого интерфейса. Если компьютер еще не определил, что его имя является уникальным, он должен указать это при ответе на запрос разрешения имени.

> ***Практический совет***
>
> По умолчанию LLMNR включен на компьютерах, работающих под управлением Windows 7 и более поздних версий. Отключить LLMNR можно с помощью реестра. Для этого установите следующий параметр реестра в 0: `HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\EnableMulticast`.
>
> Для отключения LLMNR для определенного сетевого интерфейса создайте и установите в 0 следующий параметр реестра: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\AdapterGUID\EnableMulticast`.
>
> Здесь `AdapterGUID` — глобальный уникальный идентификатор сетевого адаптера, для которого нужно отключить LLMNR. Чтобы включить LLMNR снова, установите это значение в 1. Также можно управлять LLMNR с помощью групповой политики.

Часто используемые инструменты

Для администрирования системы Windows Server 2012 доступно много инструментов. Большинство утилит входит в состав следующих инструментов.

- *Панель управления (Control Panel)* содержит набор утилит для управления конфигурацией системы. Организовать список этих утилит можно разными способами. Для этого используется список **Просмотр** (View By). По умолчанию просмотр организован по кате-

гориям, которые предусматривают доступ к утилитам в зависимости выполняемой задачи. Представления **Крупные значки** (Large Icons) и **Мелкие значки** (Small Icons) являются альтернативными и позволяют найти утилиту по имени.

- *Графические инструменты администратора* — ключевые утилиты для управления сетевыми компьютерами и их ресурсами. Получить доступ к этим утилитам можно через программную группу **Администрирование** (Administrative Tools).
- *Административные мастера* — утилиты, предназначенные для автоматизации ключевых задач администратора. Доступ к большинству таких утилит можно получить с помощью диспетчера серверов (Server Manager) — основной административной консоли Windows Server 2012.
- *Утилиты командной строки* — большинство утилит администратора можно запустить из командной строки. В дополнение к этим утилитам Windows Server 2012 предоставляет другие полезные утилиты, доступные в системах Windows Server 2012.

Чтобы узнать, как использовать утилиты командной строки .NET, введите команду `NET HELP <имя команды>` в командной строке, например, `NET HELP SHARE`. ОС Windows Server 2012 отобразит краткую справку по команде.

Windows PowerShell 3.0

Для дополнительной гибкости при написании сценариев в командной строке можно использовать Windows PowerShell 3.0. Это полноценная командная оболочка со своими встроенными командами (называемыми *командлетами* — cmdlets), встроенными функциями и стандартными утилитами командной строки. Также доступно графическое окружение и командная консоль.

Хотя консоль Windows PowerShell и графическое окружение устанавливаются по умолчанию, некоторые функции PowerShell по умолчанию отсутствуют: движок Windows PowerShell 2.0, используемый для обратной совместимости с уже существующими PowerShell-приложениями; Windows PowerShell WebAccess, который позволяет серверу работать как веб-шлюз для удаленного управления сервером с использованием PowerShell и веб-клиента.

> ***ПРАКТИЧЕСКИЙ СОВЕТ***
>
> Эти дополнительные компоненты Windows PowerShell можно установить с помощью мастера добавления ролей и компонентов (Add Roles and Features Wizard). Нажмите кнопку **Диспетчер серверов** (Server Manager) на панели задач. В диспетчере серверов (Server Manager) выберите меню **Управление** (Manage), а затем — команду **Добавить роли и компоненты** (Add roles and features). Так будет запущен мастер добавления ролей и компонентов, который можно использовать для добавления этих компонентов. Заметьте, однако, что в Windows Server 2012 не только можно отключить роль или компонент, но и удалить бинарные файлы, необходимые для этой роли или компонента. Эти файлы называются *полезными данными* (payloads).

Консоль Windows PowerShell (Powershell.exe) — это 32- или 64-разрядное окружение для работы с Windows PowerShell в командной строке. В 32-разрядных версиях Windows исполняемый файл находится в каталоге *%SystemRoot%*\System32\WindowsPowerShell\v1.0. На 64-разрядных версиях Windows 32-разрядный исполняемый файл находится в каталоге *%SystemRoot%*\SysWow64\WindowsPowerShell\v1.0, а 64-разрядный — в *%SystemRoot%*\System32\WindowsPowerShell\v1.0.

На рабочем столе можно открыть консоль Windows PowerShell, нажав кнопку **PowerShell** на панели задач. Эта возможность имеется по умолчанию. На 64-разрядных системах по умол-

чанию запускается 64-битная версия PowerShell. Если необходимо использовать 32-битную версию PowerShell на 64-разрядной системе, нужно выбрать опцию **Windows PowerShell (x86)**.

Из командной строки Windows (cmd.exe) можно запустить Windows PowerShell с помощью команды:

```
powershell
```

> ***Примечание***
>
> Путь к каталогу для Windows PowerShell должен быть в пути поиска команд. Поэтому перед запуском Windows PowerShell из командной строки сначала перейдите в нужный каталог.

После запуска Windows PowerShell можно ввести имя командлета в приглашении, командлет будет запущен, как и обычная команда в командной строке. Можно также запустить командлеты в сценариях. Имена командлетов обычно составляются из пары слов "глагол-существительное". Глаголы говорят о том, что перед нами командлет. А существительное указывает, с каким командлетом происходит работа. Например, командлет Get-Variable получает все переменные окружения Windows PowerShell и возвращает их значения. Глаголы могут быть следующими:

- Get — получает указанный объект или набор объектов какого-то типа, например, счетчик производительности или все счетчики производительности;
- Set — модифицирует настройки указанного объекта;
- Enable — включает опцию или функцию;
- Disable — отключает опцию или функцию;
- New — создает новый экземпляр элемента, например, новое событие или сервис;
- Remove — удаляет экземпляр объекта, например, событие или журнал событий.

В приглашении Windows PowerShell можно получить полный список командлетов с помощью команды `get-help *-*`. Для получения справки по конкретному командлету введите `get-help` и укажите имя командлета, например `get-help get-variable`.

Все командлеты имеют преднастроенные псевдонимы, которые используются как ярлыки для быстрого запуска командлета. Чтобы вывести все доступные псевдонимы, введите `get-item -path alias:` в приглашении Windows PowerShell. Создать псевдоним любой команды можно, используя следующий синтаксис:

```
new-item –path alias:AliasName –value:FullCommandPath
```

Здесь *AliasName* — имя создаваемого псевдонима, а *FullCommandPath* — полный путь к запускаемой команды, например:

```
new-item –path alias:sm –value:c:\windows\system32\compmgmtlauncher.exe
```

Этот пример создает псевдоним `sm` для запуска диспетчера серверов. Для использования этого псевдонима просто введите `sm` и нажмите клавишу <Enter> при работе в оболочке Windows PowerShell.

> ***Практический совет***
>
> Вообще говоря, все, что вводится в командной строке, может быть введено в приглашении Windows PowerShell. Это возможно, поскольку PowerShell ищет внешние команды и утилиты, и это является частью нормальной обработки. Внешняя команда или утилита может

быть найдена в каталоге, указанном в переменной окружении `PATH`. Однако нужно учитывать порядок выполнения команд PowerShell:

1. Встроенные или определенные в профиле псевдонимы.
2. Встроенные или определенные в профиле функции.
3. Командлеты или ключевые слова.
4. Сценарии с расширением ps1.
5. Внешние команды, утилиты и файлы.

Если любой элемент в пунктах 1—4 порядка выполнения имеет то же самое имя, что и запускаемая внешняя команда, то он будет выполнен вместо этой внешней команды.

Служба удаленного управления Windows

Функции удаленного управления Windows PowerShell поддерживаются протоколом WS-Management, а сервис **Служба удаленного управления Windows** реализует WS-Management в Windows. Компьютеры, работающие под управлением Windows 7 и более поздних версий, а также Windows Server 2008 R2 (и более поздние) уже содержат WinRM 2.0 (или более позднюю версию). Если необходимо управлять Windows-сервером с рабочей станции, убедитесь, что на ней установлены WinRM 2.0 и Windows PowerShell 3.0, а на сервере включен слушатель WinRM. Расширение IIS, устанавливаемое как Windows-функция, называемая WinRM IIS Extension, позволяет серверу работать как веб-шлюз для удаленного управления сервером с использованием WinRM и веб-клиента.

Включение и использование WinRM

Проверить доступность WinRM 2.0 и настроить Windows PowerShell можно с помощью следующих шагов:

1. Запустите Windows PowerShell от имени администратора. Для этого щелкните правой кнопкой мыши на значке Windows PowerShell (или используйте нажатие и удержание) и в контекстном меню выберите команду **Запуск от имени администратора** (Run as administrator).
2. По умолчанию сервис WinRM настраивается на запуск вручную. Необходимо изменить тип запуска на **Авто** (Automatic) и запустить сервис на каждом компьютере, с которым планируется работа. В приглашении Windows PowerShell можно проверить, что сервис WinRM запущен, с помощью команды:

   ```
   get-service winrm
   ```

   Как показано в следующем примере, свойство **`Status`** в выводе должно быть установлено в `Running`:

   ```
   Status   Name      DisplayName
   ------   ----      -----------
   Running  WinRM     Служба удаленного управления Windows
   ```

   Если сервис остановлен, введите следующую команду для запуска сервиса и его настройки на автоматический запуск в будущем:

   ```
   set-service –name winrm –startuptype automatic –status running
   ```

3. Чтобы настроить Windows PowerShell для удаленной работы, введите команду:

   ```
   Enable-PSRemoting –force
   ```

Включить удаленное управление можно только, когда компьютер подключен к домену или к частной сети. Если компьютер подключен к общедоступной (публичной) сети, нужно отключиться от этой сети и подключиться к домену или частной сети, а затем повторить этот шаг. Если у одного или более соединений вашего компьютера тип **Общедоступная сеть** (Public Network), но на самом деле компьютер подключен к домену или частной сети, нужно изменить тип соединения в Центре управления сетями и общим доступом, а затем повторить этот шаг.

В большинстве случаев возможна работа с удаленными компьютерами в других доменах.

Однако, если удаленный компьютер не находится в доверенном домене, удаленный компьютер не сможет аутентифицировать ваши учетные записи. Для включения аутентификации нужно добавить удаленный компьютер в список доверенных узлов для локального компьютера в настройках WinRM. Для этого введите следующую команду:

```
winrm set winrm/config/client '@{TrustedHosts"RemoteComputer"}'
```

Здесь *RemoteComputer* — имя удаленного компьютера, например:

```
winrm set winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

При работе с компьютерами в рабочей или домашней группе необходимо использовать HTTPS в качестве транспортного протокола или же добавлять удаленную машину в параметр `TrustedHosts`. Если невозможно подключиться к удаленному узлу, проверьте, какой сервис запущен на удаленном узле и принимает запросы, с помощью команды (ее нужно ввести на удаленном узле):

```
winrm quickconfig
```

Эта команда анализирует и настраивает сервис WinRM. Если сервис WinRM настроен корректно, вывод будет примерно такой:

```
WinRM already is set up to receive requests on this machine.
WinRM already is set up for remote management on this machine.
```

Если сервис WinRM не настроен корректно, будут отображены сообщения об ошибках, при этом необходимо утвердительно ответить на несколько подсказок, позволяющих автоматически настроить удаленное управление. По завершению этого процесса сервис WinRM будет настроен правильно.

Независимо от того, используются ли удаленные функции Windows PowerShell, необходимо запустить Windows PowerShell от имени администратора (щелкните правой кнопкой мыши на ярлыке Windows PowerShell и в контекстном меню выберите команду **Запуск от имени администратора**). Когда запускаете Windows PowerShell из другой программы, например из командной строки, нужно запустить эту программу с правами администратора.

Настройка WinRM

При работе с командной строкой, запущенной от имени администратора, можно использовать утилиту командной строки WinRM для просмотра и настройки конфигурации удаленного управления. Введите `winrm get winrm/config` для получения подробной информации о конфигурации удаленного управления.

При исследовании листинга конфигурации легко обнаружить, что информация выводится иерархически. Основа этой иерархии, уровень `Config`, соотносится с путем winrm/config. Затем идут подуровни для клиента, сервиса и WinRS: winrm/config/client, winrm/config/

service и winrm/config/winrs соответственно. Изменить значения большинства параметров конфигурации можно с помощью команды:

```
winrm set ConfigPath @{ParameterName="Value"}
```

Здесь *ConfigPath* — путь конфигурации, *ParameterName* — имя параметра, с которым нужно работать, а *Value* — устанавливаемое для параметра значение, например:

```
winrm set winrm/config/winrs @{MaxShellsPerUser="10"}
```

Здесь мы устанавливаем параметр `MaxShellsPerUser` в winrm/config/winrs. Этот параметр управляет максимальным числом соединений к удаленному компьютеру от одного пользователя. (По умолчанию каждый пользователь может изменить только 5 активных соединений.) Учтите, что некоторые параметры предназначены только для чтения, и их значения не могут быть изменены таким способом.

WinRM требует, чтобы по крайней мере один слушатель указал транспорты и IP-адреса, на которых могут быть приняты запросы управления. В качестве транспортного протокола можно использовать HTTP или HTTPS (или оба протокола). При использовании протокола HTTP сообщения могут быть зашифрованы посредством шифрования Kerberos или NTLM. В случае с протоколом HTTPS для шифрования используется Secure Socket Layers (SSL). Для просмотра списка настроенных слушателей введите команду `winrm enumerate winrm/config/listener`. Как показано в листинге 1.1, эта команда отображает детали конфигурации для сконфигурированных слушателей.

Листинг 1.1. Пример конфигурации слушателей

```
Listener
    Address = *
    Transport = HTTP
    Port = 80
    Hostname Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.1.225
```

По умолчанию компьютер, возможно, настроен на прослушивание любого IP-адреса. Если это так, пользователь не увидит никакого вывода. Чтобы ограничить WinRM определенными IP-адресами, адрес локальной петли компьютера (127.0.0.1) и назначенные компьютеру IPv4- и IPv6-адреса могут быть явно сконфигурированы для прослушивания. Можно настроить компьютер для прослушивания запросов по HTTP на всех сконфигурированных IP-адресах, выполнив следующую команду:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
```

Здесь звездочка (`*`) обозначает все настроенные IP-адреса. Заметьте, что свойство `CertificateThumbprint` должно быть пустое для разделения SSL-конфигурации с другим сервисом.

Для включения и отключения прослушивания определенных IP-адресов используются команды:

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=
HTTP @{Enabled="true"}
```

или

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=
HTTP @{Enabled="false"}
```

Следующие команды включают и отключают базовую аутентификацию клиента:

```
winrm set winrm/config/client/auth @{Basic="true"}
```

или

```
winrm set winrm/config/client/auth @{Basic="false"}
```

Можно включить или выключить аутентификацию Windows, используя NTLM или Kerberos путем ввода команды:

```
winrm set winrm/config/client @{TrustedHosts="<local>"}
```

или

```
winrm set winrm/config/client @{TrustedHosts=""}
```

В дополнение к управлению WinRM из командной строки можно также использовать групповую политику. В результате параметры групповой политики будут перезаписывать любые установленные вами параметры.

ГЛАВА 2

Управление серверами на базе Windows Server 2012

Серверы — сердце любой сети Microsoft Windows. Одна из основных обязанностей администратора — управлять этими ресурсами. В ОС Windows Server 2012 появилось несколько интегрированных инструментов управления. Для осуществления базовых задач системного администрирования необходимо использовать консоль **Диспетчер серверов** (Server Manager). Эта консоль (далее просто — диспетчер серверов) позволяет произвести общую настройку и задать параметры конфигурации локального сервера, управлять ролями, компонентами на любом удаленно управляемом сервере предприятия. Задачи, которые можно выполнить с помощью диспетчера серверов, таковы:

- добавление серверов для удаленного управления;
- инициирование удаленных соединений к серверам;
- настройка локального сервера;
- управление установленными ролями и компонентами;
- управление томами и общими ресурсами;
- настройка объединения сетевых адаптеров NIC (Network Interface Card);
- просмотр событий и предупреждений;
- перезапуск серверов.

Диспетчер серверов идеально подходит для общего администрирования, но также вам пригодится утилита для более точной настройки параметров и свойств окружения. Речь идет об утилите **Система** (System), которая используется для:

- изменения имени компьютера;
- настройки производительности приложений, виртуальной памяти и параметров реестра;
- управления переменными окружения пользователя и системы;
- настройки запуска системы и параметров восстановления.

Роли серверов, службы ролей и компоненты Windows Server 2012

Операционная система Windows Server 2012 использует ту же архитектуру конфигурации, что и Windows Server 2008 и Windows Server 2008 Release 2 (R2). Подготовка серверов для размещения происходит путем установки и настройки следующих компонентов.

- **Роли серверов.** Это связанный набор программных компонентов, позволяющих серверу осуществить определенные функции для пользователей и других компьютеров сети. Компьютер может быть выделен для какой-то определенной роли, например для роли **Доменные службы Active Directory** (Active Directory Domain Services, AD DS), или же обеспечивать несколько ролей.
- **Службы ролей** (или ролевые службы). Это программные компоненты, обеспечивающие функциональность роли сервера. У каждой роли есть одна или несколько ролевых служб. Некоторые роли, например DNS-сервер или DHCP-сервер, выполняют одну функцию, и добавление роли устанавливает эту функцию. Другие роли, например **Службы политики сети и доступа** (Network Policy and Access Services), а также **Службы сертификатов Active Directory** (Active Directory Certificate Services, AD CS), имеют несколько служб ролей, доступных для установки. Администратор может выбрать, какие службы ролей нужно установить.
- **Компоненты.** Это программные компоненты, предоставляющие дополнительную функциональность. Компоненты вроде **Шифрование диска Bit Locker** и **Система архивации данных Windows Server** устанавливаются отдельно от ролей и ролевых служб. В зависимости от конфигурации компьютера компоненты могут быть установлены или отсутствовать.

Роли, ролевые службы и компоненты настраиваются с помощью диспетчера серверов и Консоли управления Microsoft (Microsoft Management Console, MMC). Некоторые роли, службы ролей и компоненты зависят от других ролей, служб ролей и компонентов. При установке ролей, служб ролей и компонентов диспетчер серверов запрашивает у администратора подтверждение на выполнение этого действия. Аналогично, при попытке удалить компонент, диспетчер серверов предупреждает администратора, что нельзя удалить этот компонент, пока не будут удалены зависимая роль, служба роли или компонент.

Поскольку добавление или удаление ролей, служб ролей и компонентов может менять требования к аппаратным ресурсам, необходимо внимательно планировать любые изменения в конфигурации и определять, как они отобразятся на общей производительности сервера. Хотя обычно хочется комбинировать дополнительные роли, а это увеличивает нагрузку на сервер, поэтому придется, соответственно, оптимизировать аппаратные средства. В табл. 2.1 представлен обзор основных ролей и связанных с ними служб ролей, доступных для размещения на сервере под управлением ОС Windows Server 2012.

Таблица 2.1. *Основные роли и связанные ролевые службы для Windows Server 2012*

Роль	Описание
Службы сертификатов Active Directory (Active Directory Certificate Services, AD CS)	Предоставляют функции, необходимые для выпуска и отзыва цифровых сертификатов для пользователей, компьютеров клиентов и серверов. Службы роли: **Центр сертификации** (Certification Authority), **Веб-служба политик регистрации сертификатов** (Certificate Enrollment Policy Web Service), **Веб-служба регистрации сертификатов** (Certificate Enrollment Web Service), **Сетевой ответчик** (Online Responder), **Служба регистрации в центре сертификации через Интернет** (Certification AuthorityWeb Enrollment Support), **Служба регистрации на сетевых устройствах** (Network Device Enrollment Service)
Доменные службы Active Directory (Active Directory Domain Services, AD DS)	Предоставляют функции, необходимые для хранения информации о пользователях, группах, компьютерах и других объектах сети. Делает эту информацию доступной пользователям и объектам. Контроллеры домена Active Directory предоставляют пользователям и компьютерам сети доступ к запрашиваемым ресурсам сети

Таблица 2.1 *(продолжение)*

Роль	Описание
Службы федерации Active Directory (Active Directory Federation Services, AD FS)	Производят аутентификацию и управление доступом для AD DS путем расширения этих функций на WWW. Сервисы и подсервисы роли: **Службы федерации** (Federation Service), **Поддерживающий утверждение агент AD FS 1.1** (Claims-Aware Agent), **Агент Windows на основе токенов** (Windows Token-Based Agent), **Прокси-агент службы федерации** (Federation Service Proxy)
Службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services, AD LDS)	Предоставляют хранилище данных для каталогозависимых приложений, которые не требуют AD DS и размещения на контроллере домена. Не требует дополнительных служб ролей
Службы управления правами Active Directory (Active Directory Rights Management, AD RMS)	Предоставляют контролируемый доступ к защищенным сообщениям e-mail, документам, страницам интрасети и другим типам файлов. Требует наличие служб: **Сервер управления правами Active Directory** (Active Directory Rights Management Server) и **Поддержка федерации удостоверений** (Identity Federation Support)
Сервер приложений (Application Server)	Позволяет серверу размещать приложения, построенные с помощью ASP.NET, Enterprise Services и Microsoft .NET Framework 4.5. Требует более 10 служб ролей
DHCP-сервер (DHCP Server)	Предоставляет централизованное управление IP-адресацией. DHCP-серверы динамически назначают IP-адреса и другие TCP/IP-параметры другим компьютерам сети. Не требует дополнительных ролевых служб
DNS-сервер (DNS Server)	DNS — система разрешения имен, преобразующая имена компьютеров в IP-адреса. Наличие DNS-серверов обязательно в доменах Active Directory. Не требует дополнительных ролевых служб
Факс-сервер (Fax Server)	Предоставляет централизованный контроль над отправкой и приемом факсов на предприятии. Факс-сервер может работать как шлюз для факсов и позволяет управлять факс-ресурсами: заданиями и отчетами, факс-устройствами на сервере или в сети. Не требует дополнительных служб
Файловые службы и службы хранилища (File And Storage Services)	Предоставляют сервисы для управления файлами и хранилищем. Некоторые роли требуют дополнительные типы файловых служб. Службы роли: **BranchCache для сетевых файлов** (BranchCache for Network Files), **Дедупликация данных** (Data Deduplication), **Распределенная файловая система** (Distributed File System), **Пространства имен распределенной файловой системы** (DFS Namespaces), **Репликация DFS** (DFS Replication), **Файловый сервер** (File Server), **Диспетчер ресурсов файлового сервера** (File Server Resource Manager), **Services for Network File System (NFS)**, **Конечный iSCSI-сервер** (iSCSI Target Server), **Загрузка цели iSCSI** (iSCSI Target Storage Provider) и **Storage Services**

Таблица 2.1 *(окончание)*

Роль	Описание
Hyper-V	Предоставляет службы для создания и управления виртуальными машинами и эмулирования физических компьютеров. На виртуальные машины можно установить операционные системы, отличные от операционной системы сервера
Службы политики сети и доступа (NPAS, Network Policy and Access Services)	Предоставляют службы для управления политиками сетевого доступа. Ролевые сервисы: **Сервер политики сети** (Network Policy Server), **Протокол авторизации учетных данных узла** (Host Credential Authorization Protocol) и **Центр регистрации работоспособности** (Health Registration Authority)
Службы печати и документов (Print And Document Services)	Предоставляют службы для управления сетевыми принтерами, сетевыми сканерами и соответствующими драйверами. Ролевые сервисы: **Сервер печати** (Print Server), **Печать через Интернет** (Internet Printing), **Сервер распределенного сканирования** (Distributed Scan Server), **Служба LPD** (LPD Service)
Удаленный доступ (Remote Access)	Обеспечивает сервисы для управления маршрутизацией и удаленным доступом к сетям. Используйте эту роль, если необходимо настроить виртуальную частную сеть (VPN), трансляцию сетевых адресов (NAT) и другие сервисы маршрутизации. Службы: **DirectAccess и VPN (RAS)** (DirectAccess and VPN (RAS)), **Маршрутизация** (Routing)
Службы удаленных рабочих столов (Remote Desktop Services)	Предоставляют службы, позволяющие пользователям запускать Windows-приложения, установленные на удаленном сервере. При запуске пользователем приложения на терминальном сервере весь процесс выполнения происходит на сервере, по сети передаются только данные от приложения
Volume Activation Services	Предоставляет службы для автоматического управления лицензионными ключами томов и активацией ключей томов
Веб-сервер (IIS) (Web Server (IIS))	Используется для размещения веб-сайтов и веб-приложений. Веб-сайты, размещаемые на веб-сервере, могут иметь статический и/или динамический контент. Некоторые веб-приложения, которые будут размещены на веб-сервере, используют ASP.NET и .NET Framework 4.5. При установке веб-сервера можно управлять конфигурацией сервера с помощью модулей и утилит администратора IIS 8. Содержит около 10 служб ролей
Служба развертывания Windows (Windows Deployment Services, WDS)	Предоставляет сервисы для размещения Windows-компьютеров на предприятии. Службы ролей: **Сервер развертывания** (Deployment Server), **Транспортный сервер** (Transport Server)
Службы Windows Server Update Services (WSUS)	Предоставляют сервисы для Microsoft Update, разрешая предоставлять обновления для определенных серверов

В табл. 2.2 представлен обзор основных компонентов, доступных для размещения на сервере под управлением операционной системы Windows Server 2012. В отличие от ранних версий Windows, в ОС Windows Server 2012 автоматически не устанавливаются некоторые важные компоненты. Например, для использования встроенных средств резервного копирования и восстановления необходимо добавить компонент **Система архивации данных Windows Server** (Windows Server Backup).

Таблица 2.2. *Основные компоненты ОС Windows Server 2012*

Компонент	Описание
Фоновая интеллектуальная служба передачи (BITS) (Background Intelligent Transfer Service)	Обеспечивает фоновую интеллектуальную передачу. После установки этого компонента сервер может действовать как BITS-сервер, который способен принимать загрузки файлов от клиентов. Этот компонент не является необходимым для клиентов, использующих BITS. Дополнительные подкомпоненты: **Расширение сервера IIS** (BITS IIS Server Extension) и **Облегченный сервер загрузки** (BITS Compact Server)
Шифрование диска BitLocker (BitLocker Drive Encryption)	Обеспечивает основанную на аппаратных средствах защиту данных с помощью шифрования всего тома. Компьютеры, оснащенные модулем Trusted Platform Module (TPM), могут использовать **Шифрование диска BitLocker** в режиме **Startup Key** или **TPM-Only**
Сетевая разблокировка BitLocker (BitLocker Network Unlock)	Обеспечивает поддержку для основанных на сети ключевых средств защиты, которые автоматически разблокируют BitLocker-защищенные диски операционной системы, когда присоединенный к домену компьютер будет перезапущен
BranchCache	Предоставляет функциональность, необходимую для клиентов и серверов BranchCache. Содержит службы HTTP protocol, Hosted Cache и др.
Клиент для NFS (Client for NFS)	Обеспечивает функциональность для доступа к файлам, находящимся на NFS-серверах под управлением UNIX
Мост для центра обработки данных (Data Center Bridging)	Поддерживает набор IEEE-стандартов для улучшения локальных Ethernet-сетей путем обеспечения гарантированной аппаратной пропускной способности
Enhanced Storage	Обеспечивает поддержку устройств Enhanced Storage
Отказоустойчивая кластеризация (Failover Clustering)	Позволяет нескольким серверам работать вместе для обеспечения высокого уровня доступности ролей серверов. Можно кластеризировать многие типы серверов, в том числе файловый сервер и сервер печати. Серверы баз данных и сообщений — отличные кандидаты для кластеризации
Управление групповой политикой (Group Policy Management)	Устанавливает консоль управления групповой политикой (Group Policy Management Console (GPMC)) для централизованного администрирования групповой политики
Служба рукописного ввода (Ink and Handwriting Services)	Обеспечивает использование ручки или стилуса, а также распознавания рукописного ввода
Сервер управления IP-адресами (IP Address Management Server)	Централизованно управляет пространством IP-адресов и соответствующими серверами инфраструктуры

Таблица 2.2 *(продолжение)*

Компонент	Описание
Клиент печати через Интернет (Internet Printing Client)	Позволяет клиентам использовать протокол HTTP для печати на принтерах, подключенных к веб-серверам печати
Служба iSNS-сервера (Internet Storage Naming Server (iSNS) Server Service)	Предоставляет управление и функции сервера для iSCSI-устройств. Позволяет серверу обрабатывать запросы регистрации и дерегистрации, также запросы от iSCSI-устройств
Монитор LPR-порта (LPR Port Monitor)	Позволяет выполнять печать на принтерах, подключенных к UNIX-компьютерам
Media Foundation	Обеспечивает необходимую функциональность для Windows Media Foundation
Очередь сообщений (Message Queuing)	Функции управления и сервер-функции для распределенной очереди сообщений. Как правило, доступна группа дополнительных подкомпонентов
Multipath I/O (MPIO)	Обеспечивает функциональность, необходимую для использования путей данных к устройствам хранения данных
.NET Framework 4.5	Предоставляет API для разработки приложений. Дополнительные подкомпоненты: .NET Framework 4.5, ASP.NET 4.5 и Windows Communication Foundation (WCF) Activation Components
Балансировка сетевой нагрузки (NLB) (Network Load Balancing)	Распределяет трафик между несколькими серверами по протоколу TCP/IP. Идеальными кандидатами для балансировки нагрузки являются веб-серверы
Протокол одноранговой разрешения имен (PNRP) (Peer Name Resolution Protocol)	Предоставляет функциональность Link-Local Multicast Name Resolution (LLMNR), обеспечивая тем самым одноранговое разрешение имен. После добавления этого компонента приложения, установленные на сервере, смогут регистрировать и разрешать имена с помощью LLMNR
QWave (Quality Windows Audio Video Experience)	Сетевая платформа для передачи аудио/видео по домашним сетям
Пакет администрирования диспетчера RAS-подключений (RAS Connection Manager Administration Kit)	Фреймворк для создания профилей соединений к удаленным серверам и сетям
Удаленный помощник (Remote Assistance)	Разрешает удаленному пользователю подключаться к серверу для обеспечения или получения удаленной помощи
Удаленное разностное сжатие (Remote Differential Compression)	Вычисляет и передает различия между двумя объектами данных и минимизирует объем передаваемых данных
Средства удаленного администрирования сервера (RSAT) (Remote Server Administration Tools)	Устанавливает средства управления ролями и компонентами, которые могут использоваться для удаленного администрирования других Windows-серверов. Администратор может выбрать, какие именно средства необходимо установить

Таблица 2.2 *(продолжение)*

Компонент	Описание
RPC через HTTP-прокси (Remote Procedure Call (RPC) over HTTP Proxy)	Устанавливает прокси для передачи RPC-сообщений от клиентских приложений к серверам через HTTP-прокси. RPC по HTTP — это альтернатива доступа клиента к серверу через частную сеть
Простые службы TCP/IP (Simple TCP/IP Services)	Устанавливает дополнительные TCP/IP-сервисы, в том числе Character Generator, Daytime, Discard, Echo и Quote of the Day
SMTP-сервер (Simple Mail Transfer Protocol (SMTP) Server)	SMTP — сетевой протокол для контроля передачи и маршрутизации сообщений e-mail. После установки этого компонента сервер может работать как базовый SMTP-сервер. Для полноценного решения нужно установить сервер сообщений вроде Microsoft Exchange Server
Служба SNMP (Simple Network Management Protocol (SNMP) Services)	SNMP — протокол, используемый для упрощения управления TCP/IP-сетями. Протокол SNMP используется для централизованного управления сетью, если в сети есть SNMP-совместимые устройства. Также протокол SNMP применяется для мониторинга сети с помощью программного обеспечения мониторинга сетью
Подсистема для UNIX-приложений (Subsystem for UNIX-Based Applications (SUA))	Предоставляет возможность запуска UNIX-приложений. Дополнительные инструменты управления доступны для загрузки с сайта Microsoft (не рекомендуется использовать)
Клиент Telnet (Telnet Client)	Используется для подключения к удаленному Telnet-серверу и запуска приложений на этом сервере
Сервер Telnet (Telnet Server)	Размещает удаленные сессии Telnet-клиентов. При запущенном сервере Telnet пользователи могут использовать клиенты Telnet для удаленного подключения к этому компьютеру
Пользовательские интерфейсы и инфраструктура (User Interfaces And Infrastructure)	Позволяет контролировать параметры пользовательского интерфейса (**Графические средства управления и инфраструктура**, **Возможности рабочего стола**, **Графическая оболочка сервера**)
Биометрическая платформа Windows (Windows Biometric Framework)	Поддерживает устройства сканирования отпечатков пальцев
Внутренняя база данных Windows (Windows Internal Database)	Реляционное хранилище данных, которое может быть использовано только функциями и ролями Windows Server, например, AD RMS, UDDI Services, WSUS, Windows SharePoint Services и WSRM
Windows PowerShell	Разрешает управлять функциями Windows PowerShell-сервера. Windows PowerShell 3.0 и PowerShell ISE устанавливаются по умолчанию
Windows PowerShell Web Access	Превращает сервер в веб-шлюз для удаленного управления серверами с помощью веб-браузера
Служба активации процессов Windows (Windows Process Activation Service)	Обеспечивает поддержку распределенных веб-приложений, которые используют HTTP- и не-HTTP-протоколы

Таблица 2.2 *(окончание)*

Компонент	Описание
Стандартизированное управление хранилищами Windows (Windows Standards-Based Storage Management)	Позволяет обнаруживать запоминающие устройства, управлять ними и контролировать их работу. Предоставляет классы для WMI и Windows PowerShell
Система архивации данных Windows Server (Windows Server Backup)	Позволяет выполнять резервное копирование и восстановление операционной системы, состояния системы и любых данных, хранящихся на сервере
Диспетчер системных ресурсов Windows (WSRM) (Windows System Resource Manager (WSRM))	Позволяет управлять использованием ресурсов (не рекомендуется)
Фильтр Windows TIFF IFilter (Windows TIFF IFilter)	Выполняет распознавания текста в файлах, соответствующих стандарту TIFF 6.0
Расширение IIS WinRM (WinRM IIS Extension)	Позволяет серверу принимать запросы от клиента, используя протокол WS-Management
WINS-сервер (WINS Server)	Сервис разрешения имен, который сопоставляет имена компьютеров их IP-адресам. Установка этого компонента превращает компьютер в WINS-сервер
Служба беспроводной локальной сети (Wireless LAN Service)	Позволяет серверу использовать беспроводную сеть
Поддержка WoW64 (WoW64 Support)	Поддержка WoW64, необходимая для полной установки сервера. Удаление этого компонента превращает полную установку сервера в установку основных компонентов
Средство просмотра XPS (XPS Viewer)	Программа для просмотра XPS-документов

Примечание

Компонент Возможности рабочего стола — теперь подкомпонент **Пользовательские интерфейсы и инфраструктура**. Компонент **Возможности рабочего стола** предоставляет функциональность рабочего стола Windows на сервере. Добавляет следующие компоненты: Проигрыватель Windows Media, темы оформления рабочего стола, Видео для Windows (поддержка AVI), Защитник Windows (Windows Defender), Очистка диска (Disk Cleanup), Центр синхронизации (Sync Center), Звукозапись (Sound Recorder), Таблица символов (Character Map), Ножницы (Snipping Tool). Хотя все эти функции позволяют использовать сервер как настольный компьютер, они отрицательно сказываются на его общей производительности.

Администратора могут попросить установить или удалить динамически подключаемые библиотеки (DLL), особенно если он работает в команде ИТ-разработчиков. Для этого используется утилита Regsvr32, которая запускается из командной строки.

После открытия окна **Командная строка** (Command Prompt) для установки или регистрации DLL-библиотеки введите команду `regsvr32 имя.dll`, например:

```
regsvr32 mylibs.dll
```

Если необходимо, для отмены регистрации DLL-библиотеки введите команду `regsvr32 /u` *`имя`*`.dll`:

```
regsvr32 /u mylibs.dll
```

Защита файлов Windows предотвращает замену защищенных системных файлов. Замена DLL-библиотек, установленных на Windows Server, возможна только как часть исправления, обновления Service Pack или обновления Windows. Защита файлов Windows — важная часть архитектуры безопасности Windows Server.

Установки сервера: полная, с минимальным графическим интерфейсом и установка основных серверных компонентов

Операционная Windows Server 2012 поддерживает следующие типы установки: полная установка, установка с минимальным графическим интерфейсом и установка основных серверных компонентов (Server Core). Полная установка также называется **Сервер с графическим интерфейсом пользователя**. Она содержит компоненты **Графические средства управления и инфраструктура** (Graphical Management Tools And Infrastructure) и **Графическая оболочка сервера** (Server Graphical Shell), которые входят в состав компонента **Пользовательские интерфейсы и инфраструктура**, а также компонент **Поддержка WoW64** (WoW64 Support). Установка с минимальным интерфейсом пользователя подобна полной установке, но без компонента **Графическая оболочка сервера**. Установка основных серверных компонентов (Server Core) обладает ограниченным интерфейсом пользователя и не содержит компонентов **Поддержка WoW64** и **Пользовательские интерфейсы и инфраструктура** (User Interfaces And Infrastructure).

Как будет отмечено в *разд. "Изменение типа установки" далее в этой главе*, тип установки можно изменить в любой момент. При полной установке у вас будет полноценная версия Windows Server 2012, которую можно размещать с любой допустимой комбинацией ролей, ролевых служб и компонентов. То же самое можно сказать и об установке с минимальным графическим интерфейсом пользователя. Однако установка основных серверных компонентов — это минимальная установка Windows Server 2012, поддерживающая ограниченный набор ролей и их комбинаций. Поддерживаемые роли: AD CS, AD DS, AD LDS, DCHP-сервер, DNS-сервер, Файловые службы, Hyper-V, медиаслужбы, Службы печати и документов, Маршрутизация и удаленный доступ, Streaming Media Services, Веб-сервер (IIS), Службы Windows Server Update Services (WSUS). В текущей реализации установка основных компонентов не является платформой для запуска серверных приложений.

Хотя все три типа установки используют те же правила лицензирования и могут управляться удаленно с помощью любого доступного и разрешенного метода удаленного администрирования, все эти три типа совершенно разные, когда речь заходит о локальной консоли управления. В состав полной установки входит интерфейс пользователя, содержащий полное окружение рабочего стола для локальной консоли управления сервером. В состав минимальной установки входят только консоли управления, диспетчер серверов и набор утилит администрирования Панели управления. Отсутствуют (по сравнению с первыми двумя типами установки): Проводник Windows, панель задач, область уведомлений, Internet Explorer, встроенная система помощи, темы оформления, Metro-приложения и Проигрыватель Windows Media (Windows Media Player).

Обзор установки основных серверных компонентов

Если выбрана установка основных серверных компонентов, будет установлен пользовательский интерфейс с ограниченным окружением рабочего стола для локального управления сервером. Этот минимальный интерфейс содержит:

- экран входа в систему, который служит для входа в систему и выхода из нее;
- редактор Блокнот (notepad.exe) для редактирования файлов;
- редактор реестра (regedit.exe) для управления реестром;
- диспетчер задач (taskmgr.exe) для управления задачами и запуска новых задач;
- командную строку (cmd.exe) для администрирования;
- оболочку PowerShell для администрирования;
- утилиту **Проверка подписи файла** (sigverif.exe) для проверки цифровых подписей системных файлов;
- утилиту **Сведения о системе** (msinfo32.exe) для получения системной информации;
- Установщик Windows (msiexec.exe);
- панель **Дата и время** (timedata.cpl) для просмотра/установки даты, времени и часового пояса;
- панель **Язык и региональные стандарты** (intl.cpl) для просмотра/изменения региональных и языковых опций, в том числе форматов и раскладки клавиатуры;
- утилиту конфигурации сервера (sconfig), предоставляющую текстовое меню для управления настройкой сервера.

При запуске сервера с основными серверными компонентами для входа в систему можно использовать экран входа в систему, точно такой же есть на сервере с полной установкой системы. В домене действуют стандартные ограничения входа на серверы, и на сервер может войти только пользователь с надлежащими правами и полномочиями входа. На серверах, не являющихся контроллерами домена, и серверах в рабочих группах можно использовать команды `NET USER` (для добавления пользователей) и `NET LOCALGROUP` для добавления пользователей в локальную группу для локального входа в систему.

После входа в сервер на базе установки с основными серверными компонентами будет доступно ограниченное окружение (нет рабочего стола, есть только окно командной строки) с командной строкой администратора. Командная строка используется для администрирования сервера. Если окно командной строки было нечаянно закрыто, открыть новое окно командной строки можно с помощью следующих шагов:

1. Нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc> для запуска диспетчера задач.
2. В меню **Файл** выберите команду **Новая задача (Выполнить)**.
3. В окне **Создать новую задачу** введите `cmd` и нажмите кнопку **OK**.

Этот же способ можно использовать для запуска дополнительной командной строки. Хотя можно запустить Блокнот и редактор реестра с помощью команд `notepad.exe` и `regedit.exe` вместо `cmd`, есть возможность запустить Блокнот и редактор реестра прямо из командной строки командами `notepad.exe` и `regedit.exe`[1].

[1] Обычно расширение исполняемого файла можно не вводить, и вместо команд `notepad.exe` и `regedit.exe` вы можете ввести команды `notepad` и `regedit`. — *Прим. пер.*

Утилита конфигурации сервера (`sconfig`) предоставляет текстовое меню, позволяющее легко выполнить следующие операции:

- настроить членство в домене или рабочей группе;
- добавить локальную учетную запись **Администратор**;
- настроить функции удаленного управления;
- настроить параметры Windows Update;
- загрузить и установить обновления Windows;
- включить или отключить удаленный рабочий стол;
- настроить сетевые параметры TCP/IP;
- настроить дату и время;
- выйти из системы, перезагрузить компьютер и завершить работу компьютера.

После входа в систему отобразить экран входа в любой момент можно с помощью нажатия комбинации клавиш <Ctrl>+<Alt>+<Delete>. В установке сервера с основными серверными компонентами экран входа такой же, как и в полной установке: пользователь может заблокировать компьютер, переключить пользователей, выйти из системы, сменить пароль или запустить диспетчер задач. В командной строке разрешается использовать все стандартные команды и утилиты командной строки, предназначенные для управления сервером. Однако команды, утилиты и программы будут доступны, только если они есть в установке сервера с основными серверными компонентами.

Хотя инсталляция Server Core поддерживает ограниченный набор ролей и ролевых служб, есть возможность установить большинство компонентов. Также ОС Windows Server 2012 поддерживает .NET Framework, Windows PowerShell 3.0, Удаленное управление Windows (WinRM) 2.0. Эта поддержка позволяет осуществлять локальное и удаленное администрирование с помощью PowerShell. Также доступны для использования службы удаленного рабочего стола для управления установкой Server Core удаленно. Некоторые общие задачи, которые можно выполнить, зарегистрировавшись локально, приведены в табл. 2.3.

Таблица 2.3. *Полезные команды и инструменты для управления установкой с основными серверными компонентами*

Команда	Задача
`Cscript Scregedit.wsf`	Настраивает операционную систему. Используйте параметр `/cli` для вывода доступных областей настройки
`Diskraid.exe`	Настраивает программный RAID-массив
`ipconfig /all`	Выводит информацию о настройке IP-адреса компьютера
`Netdom RenameComputer`	Устанавливает имя сервера
`Netdom Join`	Подключает сервер к домену
`Netsh`	Предоставляет контекст для управления конфигурацией сетевых компонентов. Введите `netsh interface ipv4` для настройки параметров IPv4 или `netsh interface ipv6` для настройки IPv6

Таблица 2.3 *(окончание)*

Команда	Задача
`Ocsetup.exe`	Добавляет или удаляет роли, ролевые сервисы и компоненты
`Pnputil.exe`	Устанавливает или обновляет драйверы устройств
`Sc query type=driver`	Выводит установленные драйверы устройств
`Serverweroptin.exe`	Настраивает Windows Error Reporting
`Slmgr –ato`	Средство Windows Software Licensing Management, используется для активации операционной системы. Запускает `Cscript slmgr.vbs –ato`
`Slmgr –ipk`	Устанавливает или заменяет ключ продукта. Запускает `Cscript slmgr.vbs –ipk`
`SystemInfo`	Выводит подробности конфигурации системы
`Wecutil.exe`	Создает и управляет подписками на перенаправляемые события
`Wevtutil.exe`	Позволяет просматривать системные события
`Winrm quickconfig`	Настраивает сервер на прием запросов WS-Management от других компьютеров. Запускает `Cscript winrm.vbs quickconfig`
`Wmic datafile where name="FullFilePath" get version`	Выводит версию файла
`Wmic nicconfig index=9 call enabledhcp`	Настраивает компьютер на использование динамического IP-адреса (вместо статического IP)
`Wmic nicconfig index=9 call enablestatic("IPAddress"), ("SubnetMask")`	Изменяет IP-адрес компьютера и сетевую маску
`Wmic nicconfig index=9 call setgateways("GatewayIPAddress")`	Устанавливает или изменяет шлюз по умолчанию
`Wmic product get name /value`	Выводит список установленных MSI-приложений
`Wmic product where name="Name" call uninstall`	Удаляет MSI-приложение
`Wmic qfe list`	Выводит список обновлений и исправлений
`Wusa.exe PatchName.msu /quiet`	Применяет обновление/исправление к операционной системе

Установка Windows Server 2012

Операционную систему Windows Sever 2012 можно установить либо на новое оборудование, либо в качестве обновления на уже работающее. При установке ОС Windows Server 2012 на компьютер с уже установленной операционной системой имеется возможность произвести либо установку, либо обновление. При обычной установке инсталлятор Windows Server 2012 заменяет имеющуюся операционную систему компьютера, и все на-

стройки пользователя и приложений будут потеряны. При обновлении инсталлятор сначала устанавливает операционную систему, а затем вызывает процесс переноса пользовательских настроек, документов и приложений из предыдущей версии Windows.

Операционная система Windows Server 2012 поддерживает только 64-разрядную архитектуру, т. е. Windows Server 2012 можно установить лишь на компьютер с 64-битным процессором. Перед установкой Windows Server 2012 убедитесь, что компьютер соответствует минимальным системным требованиям того выпуска, который планируется использовать. Microsoft предоставляет минимальные и рекомендуемые системные требования. Если компьютер не соответствует минимальным системным требованиям, установить операционную систему Windows Server 2012 невозможно. Если компьютер не соответствует рекомендуемым требованиям, пострадает производительность сервера.

ОС Windows Server 2012 требует как минимум 10 Гбайт дискового пространства для инсталляции базовой операционной системы. Microsoft рекомендует устанавливать Windows Server 2012 на жесткий диск объемом как минимум 32 Гбайт. Дополнительное дисковое пространство понадобится для процесса подкачки, а также для дополнительных компонентов, ролей и ролевых служб, которые будут установлены. Для оптимальной производительности должно быть как минимум 10% свободного места на всех дисках сервера в течение всей его работы.

При установке Windows Server 2012 программа установки автоматически делает доступными опции восстановления, доступные на вашем сервере в качестве расширенных опций загрузки. В дополнение к командной строке для решения проблем и изменения параметров можно использовать средство **Восстановление образа системы** (System Image Recovery) для полного восстановления с помощью предварительно созданного образа системы. Если другие механизмы решения проблем не помогли восстановить компьютер и у вас есть диск восстановления, можно использовать эту возможность для восстановления компьютера из резервного образа.

Чистая установка

Перед началом установки необходимо решить, нужно ли проверить и дефрагментировать диски и разделы компьютера. При желании использовать средства программы установки для создания и форматирования разделов необходимо загрузить компьютер с дистрибутивного диска. Если загрузка произведена иным способом, эти средства не будут доступны и управлять разделами можно будет только из командной строки, используя утилиту DiskPart.

Для осуществления чистой установки Windows Server 2012 выполните следующие действия:

1. Запустите программу установки, используя один из методов.
   - Для *новой установки* нужно загрузить компьютер с дистрибутивного диска Windows Server 2012 и нажать любую клавишу, когда это будет предложено. Если подобный запрос не появился, значит, нужно изменить опции загрузки так, чтобы компьютер сначала загружался с оптического диска, а только потом уже с жесткого диска. Для этого нужно изменить параметры BIOS SETUP.
   - Для *чистой установки поверх уже существующей системы* необходимо загрузить с дистрибутивного диска или запустить компьютер и войти, используя учетную запись с правами администратора, а затем запустить программу установки с дистрибутивного носителя. При установке дистрибутивного носителя Windows Server 2012 в дисковод программа установки операционной системы запустится автоматически. Если это не произошло, используя Проводник Windows, запустите программу Setup.exe с дистрибутивного диска.

2. При запуске компьютера с использованием дистрибутивного носителя выберите язык, форматы времени и валюты, а также раскладку клавиатуры. Во время установки доступна только одна раскладка. Если раскладка клавиатуры и язык выпуска Windows Server 2012 отличаются, при вводе можно увидеть неожиданные символы. Чтобы избежать этого, убедитесь, что выбрана правильная раскладка. Когда будете готовы начать установку, нажмите кнопку **Далее** (Next).
3. Нажмите кнопку **Установить** (Install Now) для начала установки. После того как инсталлятор скопирует временные файлы на ваш компьютер, укажите, нужно ли получить обновления во время установки. Если установка запущена поверх работающей Windows, отметьте один из переключателей — **Установить обновления из Интернета сейчас** (Go online to install updates now) или **Нет, спасибо** (No, thanks).
4. В корпоративных выпусках ОС Windows Server 2012 не нужно вводить ключ продукта. Однако в OEM-версиях следует ввести ключ продукта, как только инсталлятор попросит это сделать. Нажмите кнопку **Далее** для продолжения. Флажок **Автоматически активировать Windows при подключении к Интернету** (Activate Windows when I'm online) установлен по умолчанию, чтобы гарантировать активацию операционной системы, как только компьютер подключится к Интернету.

   Примечание

   Операционную систему Windows Server 2012 необходимо активировать после установки. Если не активировать систему в положенный срок, при запуске появится сообщение "Период активации истек" (Your activation period has expired), а также напоминание, что у вас установлена не подлинная версия Windows Server 2012. Это означает, что ОС Windows Server 2012 будет запущена с ограниченной функциональностью. Чтобы восстановить полную функциональность, необходимо активировать Windows Server 2012.

5. На странице **Выберите операционную систему, которую вы хотите установить** (Select The Operating System You Want To Install) доступны опции **Установка основных серверных компонентов** (Server Core Installation) и **Сервер с графическим интерфейсом пользователя** (Server With A GUI). Сделайте соответствующий выбор и нажмите кнопку **Далее**.
6. Лицензионное соглашение Windows Server 2012 отличается от предыдущих версий Windows. Прочитайте его, отметьте флажок **Я принимаю условия лицензии** и нажмите кнопку **Далее**.
7. На странице **Выберите тип установки** (Which Type Of Installation Do You Want) выберите тип установки, которую необходимо осуществить. Поскольку выполнится чистая установка, для замены существующей инсталляции или для настройки нового компьютера нажмите кнопку **Выборочная: только установка Windows (для опытных пользователей)** (Custom Install Windows Only (Advanced)). Если компьютер загружен с дистрибутивного диска, кнопка **Обновление** (Upgrade) будет недоступна. Для обновления системы нужно перезагрузить компьютер, загрузить установленную ОС, войти в систему и запустить установку.
8. На странице **Где вы хотите установить Windows**? (Where Do You Want To Install Windows?) выберите диск или раздел диска, на который необходимо установить операционную систему. Существуют две версии этой страницы, поэтому нужно иметь в виду следующее.
   - Когда у компьютера есть один жесткий диск с одним разделом на весь диск или одной областью нераспределенного пространства, указывают весь диск, и можно на-

жать кнопку **Далее** для выбора этого диска в качестве назначения установки. Если диск не размечен, можно создать необходимые разделы перед установкой операционной системы, как будет показано в *разд. "Создание, форматирование, удаление и расширение разделов диска во время установки" далее в этой главе*.

- Когда у компьютера имеется несколько дисков или один диск с несколькими разделами, нужно либо выбрать существующий раздел для установки операционной системы, либо создать новый раздел. Как можно создать новый раздел, будет показано в *разд. "Создание, форматирование, удаление и расширение разделов диска во время установки" далее в этой главе*.
- Если диск не инициализирован или BIOS компьютера не поддерживает запуск операционной системы с выбранного диска, нужно инициализировать диск, создав один или более разделов на этом диске. Нельзя выбрать диск, использующий файловую систему FAT/FAT32. Также нельзя отформатировать диск в этой файловой системе. Если раздел, на который планируется установить Windows Server, отформатирован как FAT32, нужно конвертировать его в NTFS. При работе с этой страницей программы установки можно получить доступ к командной строке для осуществления необходимых предустановочных задач *(см. разд. "Создание, форматирование, удаление и расширение разделов диска во время установки" далее в этой главе)*.

9. Если выбранный раздел содержит установку предыдущей версии Windows, инсталлятор сообщит вам, что существующие настройки пользователя и приложений будут перемещены в папку Windows.old и нужно будет скопировать эти параметры в новую установку Windows. Нажмите кнопку **OK**.
10. Нажмите кнопку **Далее**. Инсталлятор начнет установку операционной системы. Во время этого процесса инсталлятор скопирует полный образ диска Windows Server 2012 на выбранный вами диск/раздел, а затем развернет его. После этого инсталлятор установит дополнительные компоненты на основании конфигурации вашего компьютера и обнаруженных аппаратных средств. Этот процесс требует нескольких автоматических перезагрузок. После завершения установки будет загружена операционная система и можно осуществить начальную настройку, например, установить пароль администратора и имя сервера.

Практический совет

Серверы, созданные на базе установки с основными серверными компонентами, по умолчанию настроены на использование DHCP. При наличии сетевой карты и сетевого кабеля во время данной установки будет выполнено подключение к DHCP-серверу вашей организации и будут получены корректные сетевые параметры. Можно настроить сервер с помощью утилиты Sconfig, предоставляющей меню для настройки членства домена/рабочей группы, имени компьютера, удаленного управления, удаленного рабочего стола, обновления Windows, сетевых параметров, даты и времени, а также для выхода из системы, перезапуска и завершения работы.

Также можно настроить сервер и с помощью отдельных команд. Если необходимо использовать статический IP-адрес, запустите команду `Netsh` для применения необходимых параметров. Как только сеть будет настроена, используйте команды `Slmgr –ipk` для установки ключа продукта и `Slmgr –ato` для активации Windows. Для установки даты и времени введите команду `timedate.cpl`. Если нужно включить удаленное управление посредством протокола WS-Management, введите `winrm quickconfig`.

Далее, возможно, понадобится задать имя компьютера. Для просмотра имени введите команду `echo %computername%`. Для переименования компьютера используйте команду `Netdom RenameComputer` следующим образом: `netdom renamecomputer` *`старое_имя`* `/newname:`*`новое_имя`*. Где *`старое_имя`* — текущее имя компьютера, а *`новое_имя`* — имя, ко-

торое необходимо установить. Например: `netdom renamecomputer win-k4m6bnovlhe /newname:server18`. После изменения имени нужно перезагрузить компьютер с помощью команды `shutdown /r`.

После перезагрузки можно присоединиться к домену с помощью команды `Netdom Join`. Синтаксис команды можно узнать, введя `netdom join /?`.

Обновление существующей системы

Хотя Windows Server 2012 предоставляет опцию **Обновление** (Upgrade) во время установки, обновление — это немного не то, что кажется на первый взгляд. При выборе этой опции инсталлятор осуществляет чистую установку операционной системы и затем переносит в нее пользовательские настройки, документы и приложения из предыдущей версии Windows.

Во время этого процесса инсталлятор перемещает папки и файлы из предыдущей инсталляции в папку Windows.old. В результате предыдущая инсталляция перестает запускаться.

> ***Примечание***
>
> Невозможно осуществить обновление до Windows Server 2012 на компьютере с 32-битной операционной системой, даже если у компьютера 64-битный процессор. Нужно перенести службы, предоставляемые этим компьютером, на другие серверы, а затем осуществить чистую установку. В этом помогут средства переноса данных (Windows Server Migration tools). Эти утилиты доступны на компьютерах с запущенной ОС Windows Server 2012.

Осуществить обновление до Windows Server 2012 можно с помощью следующих действий:

1. Включите компьютер, войдите в систему, используя учетную запись администратора. После помещения установочного диска Windows Server 2012 в DVD-ROM автоматически запустится инсталлятор. Если это не произошло, используйте Проводник для доступа к файлу установочного диска и двойным щелчком запустите программу Setup.exe.
2. Поскольку программа установки запускается из текущей операционной системы, инсталлятор не будет просить выбрать пользователя язык, форматы валюты и времени и раскладку клавиатуры. При установке будет доступна только одна раскладка клавиатуры — та, которая используется в установленной операционной системе. Если язык раскладки и язык выпуска Windows Server 2012 не совпадают, при вводе можно увидеть неожиданные символы.
3. Нажмите кнопку **Установить** для запуска инсталляции. После этого инсталлятор скопирует временные файлы на компьютер и спросит, нужно ли получить обновления во время установки. Выберите переключатель **Установить обновления из Интернета сейчас** или **Нет, спасибо**.
4. В случае с корпоративными выпусками Windows Server 2012 не нужно вводить ключ продукта во время установки операционной системы. Если используется OEM-версия, скорее всего, вас попросят ввести ключ продукта. Нажмите кнопку **Далее** для продолжения. Флажок **Автоматически активировать Windows при подключении к Интернету** отмечен по умолчанию, чтобы гарантировать активацию операционной системы, как только компьютер подключится к Интернету.
5. На странице **Выберите операционную систему, которую вы хотите установить** доступны опции **Установка основных серверных компонентов** и **Сервер с графическим интерфейсом пользователя**. Сделайте соответствующий выбор и нажмите кнопку **Далее**.

6. Лицензионное соглашение Windows Server 2012 отличается от предыдущих версий Windows. Прочитайте его, отметьте флажок **Я принимаю условия лицензии** и нажмите кнопку **Далее**.
7. На странице **Выберите тип установки** (Which Type Of Installation Do You Want) выберите тип установки, которую необходимо осуществить. Поскольку осуществляется обновление, нажмите кнопку **Обновление** (Upgrade). Если установка запущена с загрузочного диска, а не из Windows, кнопка **Обновление** будет недоступной. Для обновления нужно перезагрузить компьютер, загрузить установленную версию Windows, войти в систему и запустить программу установки.
8. Затем инсталлятор начнет установку. Поскольку происходит обновление системы, не нужно выбирать место для установки. Во время этого процесса инсталлятор скопирует полный образ диска Windows Server 2012 на системный диск, а затем установит дополнительные компоненты в зависимости от конфигурации компьютера и обнаруженного оборудования. По окончанию установки будет загружена операционная система, и можно осуществить начальную настройку, например, установить пароль администратора и имя сервера.

Дополнительные административные задачи во время установки

Иногда требуется выполнить какую-то предустановочную задачу перед началом установки. Получить доступ к командной строке можно прямо из программы установки или же использовать расширенные опции диска для осуществления необходимых задач.

Использование командной строки во время установки

При получении доступа к командной строке из программы установки администратор будет работать с окружением MINWINPC (mini Windows PC), которое используется инсталлятором операционной системы. Получить доступ к командной строке можно с помощью комбинации клавиш <Shift>+<F10>, нажатой на странице **Где вы хотите установить Windows?** Окружение mini Windows PC предоставляет большинство утилит, доступных в командной строке Windows Server 2012 (табл. 2.4).

Таблица 2.4. *Утилиты командной строки в оболочке mini Windows PC*

Команда	Описание
ARP	Отображает и модифицирует таблицы преобразования IP-адресов в физические адреса с использованием протокола ARP (Address Resolution Protocol)
ASSOC	Отображает и модифицирует привязку расширений файлов
ATTRIB	Показывает и изменяет атрибуты файлов
CALL	Вызывает один сценарий из другого
CD/CHDIR	Используется для отображения имени текущего каталога и изменения текущего каталога
CHKDSK	Проверяет диск на наличие ошибок и отображает отчет
CHKNTFS	Показывает статус томов. Позволяет добавить/удалить том из списка автоматической проверки, которая осуществляется при запуске операционной системы

Таблица 2.4 *(продолжение)*

Команда	Описание
CHOICE	Создает список, из которого пользователи могут выбрать один из нескольких вариантов (используется в пакетном сценарии)
CLS	Очищает окно консоли
CMD	Запускает новый экземпляр окна командной строки Windows
COLOR	Устанавливает цвет окна командной оболочки Windows
CONVERT	Конвертирует FAT-тома в NTFS
COPY	Копирует или комбинирует файлы
DATE	Отображает/устанавливает системную дату
DEL	Удаляет один или больше файлов
DIR	Отображает список файлов и подкаталогов заданного каталога
DISKPART	Вызывает командный интерпретатор, позволяющий управлять дисками, разделами и томами, используя отдельную командную строку и внутренние команды DISKPART
DISM	Управляет образами Windows
DOSKEY	Используется для создания макросов, состоящих из команд Windows
ECHO	Отображает сообщения, а также переключает режим отображения команд на экране
ENDLOCAL	Завершение локализации окружения в пакетном файле
ERASE	Стирает один или более файлов
EXIT	Выход из командного интерпретатора
EXPAND	Разархивирует файлы
FIND	Производит поиск текстовой строки в файлах
FOR	Запускает указанную команду для каждого файла из набора файлов
FORMAT	Форматирует дискету или жесткий диск
FTP	Передает файлы
FTYPE	Отображает/изменяет типы файлов, используемые в ассоциации расширений
GOTO	Передает управление содержащей метку строке командного файла
HOSTNAME	Выводит имя компьютера
IF	Осуществляет проверку условия в пакетных программах
IPCONFIG	Отображает конфигурацию TCP/IP
LABEL	Создает, изменяет или удаляет информацию о томе диска
MD/MKDIR	Создает каталог или подкаталог
MORE	Поэкранно выводит данные
MOUNTVOL	Управляет точкой монтирования тома

Таблица 2.4 *(продолжение)*

Команда	Описание
MOVE	Перемещает файлы из одного каталога в другой на одном и том же диске
NBTSTAT	Отображает статус NetBIOS
NET ACCOUNTS	Управляет учетной записью пользователя и политиками паролей
NET COMPUTER	Добавляет/удаляет компьютер в домен или из домена
NET CONFIG SERVER	Отображает/модифицирует конфигурацию службы **Сервер**
NET CONFIG WORKSTATION	Отображает/модифицирует конфигурацию службы **Рабочая станция**
NET CONTINUE	Возобновляет работу приостановленной службы
NET FILE	Отображает открытые файлы на сервере или управляет ими
NET GROUP	Показывает глобальные группы или управляет ими
NET LOCALGROUP	Показывает локальные группы или управляет ими
NET NAME	Отображает/модифицирует получателей для службы сообщений
NET PAUSE	Приостанавливает службу
NET PRINT	Отображает/модифицирует задания печати и управляет очередью печати
NET SEND	Отправляет сообщение с использованием службы сообщений
NET SESSION	Показывает или завершает установленные сеансы
NET SHARE	Показывает общие принтеры и каталоги или управляет ими
NET START	Запускает сетевые сервисы или отображает запущенные сервисы
NET STATISTICS	Отображает статистику рабочей станции и сервера
NET STOP	Останавливает сервисы
NET TIME	Отображает/синхронизирует сетевое время
NET USE	Отображает удаленные соединения или управляет ими
NET USER	Управляет локальными учетными записями пользователей
NET VIEW	Отображает сетевые ресурсы или компьютеры
NETSH	Открывает отдельную командную оболочку, позволяющую управлять конфигурацией разных сетевых сервисов на локальном и удаленном компьютерах
NETSTAT	Отображает статус сетевых соединений
PATH	Отображает или устанавливает путь поиска исполняемых файлов в текущем командном окне
PATHPING	Трассирует маршрут и предоставляет информацию о потере пакетов
PAUSE	Приостанавливает обработку сценария и ждет ввод с клавиатуры
PING	Определяет, установлено ли сетевое соединение
POPD	Переходит в каталог, сохраненный командой PUSHD

Таблица 2.4 *(окончание)*

Команда	Описание
PRINT	Выводит текстовый файл
PROMPT	Изменяет приглашение командной строки Windows
PUSHD	Сохраняет текущий каталог, а затем переходит в указанный каталог
RD/RMDIR	Удаляет каталог
RECOVER	Восстанавливает информацию на поврежденном диске
REG ADD	Добавляет новый подключ или запись в реестр
REG COMPARE	Сравнивает подключи или записи реестра
REG COPY	Копирует запись реестра на локальной или удаленной машине
REG DELETE	Удаляет подключ или записи из реестра
REG QUERY	Отображает элементы ключа реестра и имена подключей (если они есть)
REG RESTORE	Записывает сохраненные подключи и записи обратно в реестр
REG SAVE	Сохраняет копию указанных подключей, элементов и их значений в файл
REGSVR32	Регистрирует и отменяет регистрацию DLL-библиотеки
REM	Добавляет комментарии в сценарии
REN	Переименовывает файл
ROUTE	Управляет таблицами сетевой маршрутизации
SET	Отображает или модифицирует переменные окружения Windows. Также используется для вычисления числовых выражений в командной строке
SETLOCAL	Начинает локализацию окружения в пакетном файле
SFC	Сканирует и проверяет защищенные системой файлы
SHIFT	Смещает подставляемые параметры для пакетного файла
START	Запускает новое окно командной строки и запускает в нем указанную программу или команду
SUBST	Сопоставляет букву диска указанному пути
TIME	Отображает или устанавливает системное время
TITLE	Устанавливает заголовок окна командной строки
TRACERT	Отображает путь между компьютерами
TYPE	Показывает содержимое текстового файла
VER	Отображает версию Windows
VERIFY	Включение или отключение режима проверки правильности записи файлов на диск
VOL	Отображает метку тома диска и серийный номер

Принудительное удаление раздела диска во время установки

Во время установки, возможно, не получится использовать желаемый раздел диска. Причиной может быть неверное значение байта смещения раздела жесткого диска. Чтобы исправить проблему, необходимо удалить разделы (что повлечет полную потерю данных) и создать необходимые разделы с использованием расширенных параметров программы установки на странице **Где вы хотите установить Windows?** Удалить нераспознанные разделы диска можно с помощью следующих действий:

1. Нажмите комбинацию клавиш <Shift>+<F10>, чтобы открыть окно командной строки.
2. В окне командной строки введите `diskpart` для запуска одноименной утилиты.
3. Для просмотра перечня дисков компьютера введите `list disk`.
4. Выберите диск командой `select disk` *`номер_диска`*, где *`номер_диска`* — это номер диска, с которым планируется работать.
5. Для удаления всех разделов на выбранном диске введите `clean`.
6. Введите команду `exit` для выхода из DiskPart.
7. Введите команду `exit` для завершения работы в окне командной строки.
8. В окне установщика Windows нажмите кнопку со стрелкой назад для возврата к предыдущему экрану.
9. На странице **Выберите тип установки** нажмите кнопку **Выборочная** (Custom) для запуска выборочной установки.
10. На странице **Где вы хотите установить Windows?** выберите только что очищенный диск в качестве раздела для установки. В случае необходимости воспользуйтесь ссылкой **Настройка диска** (Disk Options) для получения доступа к командам действий над разделами (**Удалить** (Delete), **Форматировать** (Format), **Создать** (New), **Расширить** (Extend)).
11. Нажмите кнопку **Создать** (New) и в появившемся окне введите размер раздела в мегабайтах, а затем нажмите кнопку **Применить** (Apply).

Загрузка драйверов устройств во время установки

В процедуре установки существует страница **Где вы хотите установить Windows?**, на которой присутствует кнопка **Загрузка** (Load Driver). Ее можно нажать для загрузки драйвера жесткого диска или контроллера жесткого диска. Обычно эту возможность нужно использовать, когда диск, на который планируется установка операционной системы, не отображается в списке, поскольку недоступен его драйвер.

Для загрузки драйвера диска выполните следующие действия:

1. Во время установки на странице **Где вы хотите установить Windows?** (Where Do You Want To Install Windows) нажмите кнопку **Загрузка**.
2. Когда вас попросят вставить инсталляционный носитель в DVD-дисковод или подключить флешку (USB-диск), сделайте это и нажмите кнопку **OK**. Инсталлятор произведет поиск драйверов устройств на всех сменных носителях.
   - Если инсталлятор найдет несколько драйверов, выберите драйвер, который нужно установить, и нажмите кнопку **Далее**.
   - Если инсталлятор не найдет драйвер устройства, нажмите кнопку **Обзор** (Browse) для появления окна выбора папки, выберите папку с драйвером и нажмите кнопку **OK**, а затем кнопку **Далее**.

Для повторного сканирования сменных носителей на предмет наличия драйверов нажмите кнопку **Пересканировать** (Rescan). Если драйвер найти не удалось, нажмите кнопку со стрелкой назад для возврата на предыдущую страницу инсталлятора.

Создание, форматирование, удаление и расширение разделов диска во время установки

При осуществлении чистой установки (при условии, что компьютер загружен с дистрибутивного носителя) на странице **Где вы хотите установить Windows?** появится кнопка **Настройка диска** (Drive Options (Advanced)), нажав которую можно получить набор дополнительных возможностей:

- **Создать** (New) — создает раздел; после этого нужно отформатировать раздел;
- **Форматировать** (Format) — форматирует новый раздел так, чтобы он был доступен для установки операционной системы;
- **Удалить** (Delete) — удаляет раздел, который больше не нужен;
- **Расширить** (Extend) — расширяет раздел, увеличивая его размер.

Далее объясняется, как правильно использовать каждую из этих возможностей. Если они недоступны, все еще можно работать с дисками компьютера. На странице **Где вы хотите установить Windows?** нажмите комбинацию клавиш <Shift>+<F10>, чтобы открыть окно командной строки. В этом окне введите команду `diskpart` для запуска одноименной утилиты.

Создание раздела диска во время установки

При создании раздела можно установить его размер. Поскольку допускается создание новых разделов только в неразмеченной области, для создания раздела необходимого размера придется удалить существующие разделы. Как только раздел создан, его нужно отформатировать для установки файловой системы. Но даже если раздел не отформатирован, его все равно можно использовать для установки операционной системы. В этом случае инсталлятор отформатирует раздел при установке операционной системы.

Для создания нового раздела выполните следующие действия:

1. Во время установки на странице **Где вы хотите установить Windows?** нажмите кнопку **Настройка диска** для отображения расширенных опций работы с дисками.
2. Выберите диск, на котором нужно создать раздел, а затем нажмите кнопку **Создать** (New).
3. В поле **Размер** (Size) введите размер раздела в мегабайтах, нажмите кнопку **Применить** (Apply) для создания раздела на выбранном диске.

После создания раздела его нужно отформатировать для продолжения установки.

Форматирование раздела диска во время установки

Форматирование создает файловую систему на выбранном разделе. После форматирования раздел будет доступен для установки операционной системы. Помните, что форматирование уничтожает все данные раздела. Форматировать раздел нужно только в том случае, если необходимо удалить все существующие данные и установить систему на только что отформатированный раздел (за исключением нового раздела — его нужно форматировать сразу после создания).

Для форматирования раздела выполните следующие действия:

1. Во время установки на странице **Где вы хотите установить Windows?** нажмите кнопку **Настройка диска** для отображения расширенных опций работы с дисками.
2. Выберите раздел, который нужно отформатировать.
3. Нажмите кнопку **Форматировать** (Format). Когда появится запрос подтвердить свое намерение, нажмите кнопку **OK**. Программа установки отформатирует раздел.

Удаление раздела диска во время установки

Удаление позволяет избавиться от раздела, который больше не нужен. После удаления раздела дисковое пространство, выделенное для него, превратится в нераспределенное пространство. Удаление уничтожает все данные раздела. Обычно нужно удалить раздел, только когда он в неправильном формате или когда нужно скомбинировать области свободного дискового пространства.

Для удаления раздела выполните следующие действия:

1. Во время установки на странице **Где вы хотите установить Windows?** нажмите кнопку **Настройка диска** для отображения расширенных опций работы с дисками.
2. Выберите раздел, который нужно удалить.
3. Нажмите кнопку **Удалить** (Delete). Когда появится запрос подтвердить свое намерение, нажмите кнопку **OK**. После этого инсталлятор удалит раздел.

Расширение раздела диска во время установки

Операционная система Windows Server 2012 требует как минимум 10 Гбайт дискового пространства для установки (рекомендуется 32 Гбайт). Если существующий раздел слишком мал, его нельзя использовать для установки ОС. Чтобы установить ОС, нужно расширить раздел для увеличения его размера за счет использования нераспределенного пространства текущего диска. Расширить раздел можно, только если он отформатирован под файловую систему NTFS 5.2 (или более позднюю версию NTFS). Новые разделы, созданные в инсталляторе, также могут быть расширены, если на диске есть нераспределенное дисковое пространство.

Для расширения раздела выполните следующие действия:

1. Во время установки на странице **Где вы хотите установить Windows?** нажмите кнопку **Настройка диска** для отображения расширенных опций работы с дисками.
2. Выберите раздел, который нужно расширить.
3. Нажмите кнопку **Расширить** (Extend). В поле **Размер** введите размер раздела в мегабайтах и нажмите кнопку **Применить**.
4. Подтвердите свое намерение, нажмите кнопку **OK**. После этого инсталлятор расширит раздел.

Изменение типа установки

В отличие от ранних выпусков Windows Server, можно изменить тип установки любого сервера на базе Windows Server 2012. Это возможно, поскольку основная разница между этими типами установки заключается в том, есть ли в установке следующие компоненты:

- графические средства управления и инфраструктура;
- возможности рабочего стола;
- графическая оболочка сервера.

В полной установке присутствуют оба компонента — **Графические средства управления и инфраструктура** (Graphical Management Tools And Infrastructure) и **Графическая оболочка сервера** (Server Graphical Shell). Также в ней может быть установлен компонент **Возможности рабочего стола** (Desktop Experience). С другой стороны, в установке с минимальным графическим интерфейсом есть только компонент **Графические средства управления и инфраструктура**. В установке Server Core нет ни одного из этих компонентов.

Зная, что Windows также автоматически устанавливает и удаляет зависимые компоненты, роли сервера и утилиты управления для соответствия типу установки, есть возможность перехода от одного типа установки к другому путем простого добавления или удаления соответствующих подкомпонентов компонента **Пользовательские интерфейсы и инфраструктура** (User Interfaces and Infrastructure).

Конвертирование полной установки и установки с минимальным графическим интерфейсом

Чтобы конвертировать полную установку в установку с минимальным графическим интерфейсом, нужно удалить компонент **Графическая оболочка сервера**. Хотя можно использовать мастер удаления ролей и компонентов (Remove Roles And Features Wizard), данную операцию можно выполнить с помощью команды PowerShell:

```
uninstall-windowsfeature server-gui-shell -restart
```

Эта команда предписывает Windows Server удалить компонент **Графическая оболочка сервера**, а затем перезапустить сервер. Если компонент **Возможности рабочего стола** установлен, его нужно также удалить.

> ***Совет***
>
> Перед вводом команды, у которой могут быть далеко идущие последствия, лучше всего выполнить ее с параметром `-Whatif`. Этот параметр заставляет PowerShell сообщать, что произойдет при запуске команды.

Чтобы конвертировать установку с минимальным интерфейсом в полную установку, нужно добавить компонент **Графическая оболочка сервера**. Можно использовать мастер добавления ролей и компонентов (Add Roles And Features Wizard) или выполнить следующую PowerShell-команду:

```
install-windowsfeature server-gui-shell -restart
```

Эта команда устанавливает компонент **Графическая оболочка сервера** и перезапускает сервер для завершения установки. Если также нужно добавить компонент **Возможности рабочего стола**, используйте эту команду вместо предыдущей:

```
install-windowsfeature server-gui-shell, desktop-experience -restart
```

Конвертирование установки с основными серверными компонентами

Для преобразования полной установки или установки с минимальным графическим интерфейсом в установку с основными серверными компонентами (Server Core) необходимо удалить компоненты **Графические средства управления и инфраструктура** и **Поддержка WoW64**. Сервер будет сконфигурирован под установку Server Core. Хотя для удаления пользовательского интерфейса обычно используется мастер удаления ролей и компонентов, можно обойтись командой, введенной в приглашении PowerShell:

```
uninstall-windowsfeature server-gui-mgmt-infra -restart
```

Эта команда указывает Windows Server удалить пользовательский интерфейс для компонента **Графические средства управления и инфраструктура** и перезагрузить сервер для завершения удаления. Поскольку многие зависимые роли, ролевые службы и компоненты могут быть удалены, введите команду с параметром `-Whatif`, чтобы увидеть, что было удалено.

Если сервер установлен с пользовательским интерфейсом, а потом установка конвертирована в Server Core, вернуться к полной установке можно командой:

```
install-windowsfeature server-gui-mgmt-infra -restart
```

Поскольку бинарные файлы для этого компонента и зависимых компонентов не были удалены, команда должна выполниться успешно. Если бинарные файлы были удалены или установлена оригинальная инсталляция Server Core, тогда нужно указать источник для требуемых бинарных файлов.

Чтобы восстановить бинарные файлы из точки монтирования Windows Imaging (WIM), нужно указать параметр `-Source`. Например, если в вашей компании есть смонтированный образ Windows Server 2012, доступный в сети по адресу \\ImServer18\WinS12EE, команда будет такой:

```
install-windowsfeature server-gui-mgmt-infra -source \\imserver18\wins12ee
```

Многие компании обычно размещают на своих серверах образ Windows Server 2012, поэтому можно смонтировать дистрибутивный диск, а затем использовать папку Windows\WinSXS в качестве источника. Для этого выполните следующие действия:

1. Вставьте инсталляционный диск в дисковод сервера и создайте папку, к которой будет подмонтирован инсталляционный образ: `mkdir c:\mountdir`.
2. Определите индекс образа с помощью команды: `dism /get-wiminfo /wimfile:e:\sources\install.wim`. Здесь `e:` — идентификатор дисковода сервера.
3. Подмонтируйте инсталляционный образ командой: `dism /mount-wim /wimfile:e:\sources\install.wim /index:2 /mountdir:c:\mountdir /readonly`. Где `e:` — буква дисковода сервера; `2` — индекс используемого образа; `c:\mountdir` — каталог монтирования. Монтирование занимает несколько минут.
4. Используйте командлет Install-WindowsFeature в приглашении PowerShell, указав источник c:\mountdir\windows\winsxs, как показано в примере:

   ```
   install-windowsfeature server-gui-mgmt-infra -source c:\mountdir\windows\winsxs
   ```

Управление ролями, службами ролей и компонентами

Для управления ролями, ролевыми службами и компонентами используется консоль **Диспетчер серверов**. Диспетчер серверов применяется не только для установки/удаления ролей, ролевых служб и компонентов, но и для просмотра конфигурации сервера и статуса этих программных компонентов.

Начальная настройка

Диспетчер серверов — центральная консоль для осуществления начальной настройки и настройки ролей и компонентов. Данная консоль позволяет быстро настроить не только новый сервер, но и окружение управления.

Обычно Windows Server 2012 автоматически запускает диспетчер серверов при входе в систему, и получить доступ к диспетчеру серверов можно через рабочий стол. Если не нужно запускать консоль при каждом входе в систему, выберите меню **Управление** (Manage), далее — **Свойства диспетчера серверов** (Server Manager Properties). В окне **Свойства диспетчера серверов** (Server Manager Properties) установите флажок **Не запускать диспетчер серверов автоматически при входе в систему** (Do Not Start Server Manager Automatically At Logon) и нажмите кнопку **OK**.

> ***Примечание***
>
> Для автоматического запуска диспетчера серверов используется групповая политика. Включать/выключать параметр **Не запускать диспетчер серверов автоматически при входе в систему** (Do Not Display Server Manager Automatically At Logon) можно с помощью групповой политики в узле **Конфигурация компьютера\Административные шаблоны\Система\Диспетчер серверов** (Computer Configuration\Administrative Templates\System\Server Manager).

Как показано на рис. 2.1, вид по умолчанию для диспетчера серверов — **Панель мониторинга** (Dashboard). Здесь находятся ссылки для быстрого добавления ролей и функций на локальные и удаленные серверы, добавления серверов для управления ими, а также создания групп серверов. В меню **Управление** (Manage) находятся следующие команды.

- **Добавить роли и компоненты** (Add Roles And Features) — запускает мастер добавления ролей и компонентов (Add Roles And Features Wizard), позволяющий установить роли, ролевые службы и компоненты на сервер.
- **Добавление серверов** (Add Other Servers To Manage) — открывает диалоговое окно **Добавить серверы** (Add Servers), используемое для добавления серверов, которые будут

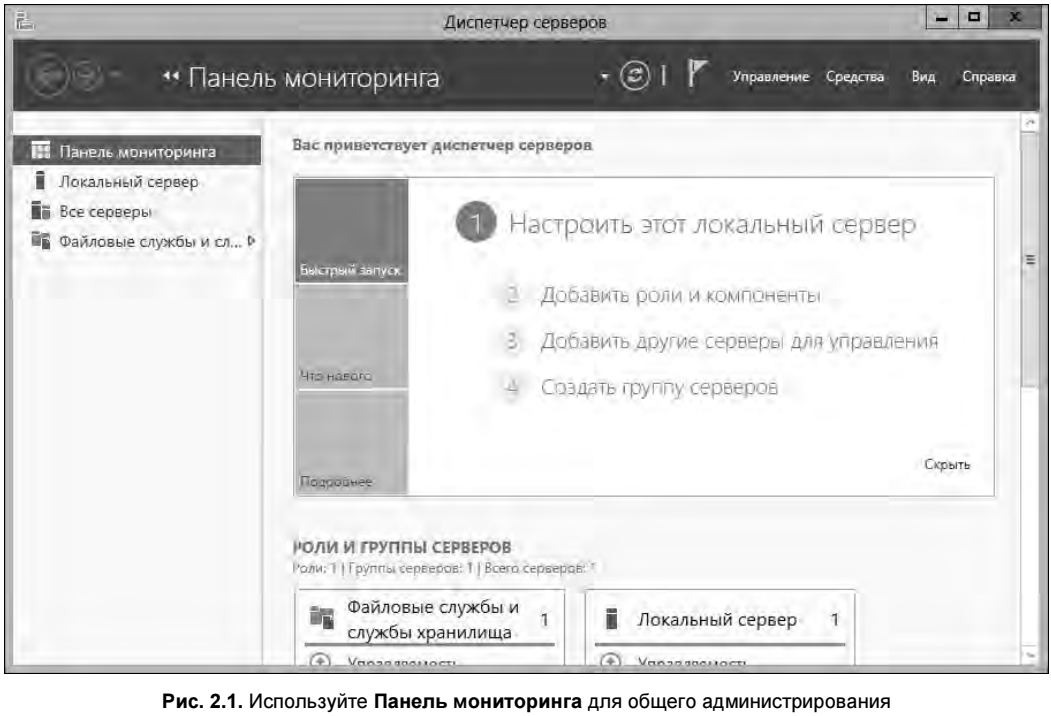


Рис. 2.1. Используйте **Панель мониторинга** для общего администрирования

доступны для управления. Список всех добавленных серверов отображается на панели **Все серверы** (All Servers). Нажмите и удерживайте пальцем или щелкните правой кнопкой мыши на имени сервера на панели **Серверы** (Servers) раздела **Все серверы** (All Servers) для отображения списка команд управления, в том числе команды перезагрузки/завершения работы, управления компьютером и т. д.

- **Создание группы серверов** (Create Server Group) — открывает одноименное диалоговое окно, которое используется для добавления серверов в группы, что упрощает управление ими. Диспетчер серверов автоматически создает группы серверов на основании ролей. Например, контроллеры домена перечислены в группе AD DS. Быстро найти информацию о любом контроллере домена можно с помощью выбора соответствующего узла.

> ***Совет***
>
> Когда нужно подключиться к серверу, используя альтернативные учетные данные (другие имя пользователя и пароль), щелкните правой кнопкой мыши (или нажмите и удерживайте сенсорный экран) на имени сервера (на панели **Все серверы**) и выберите команду **Управлять как** (Manage As). В окне **Безопасность Windows** (Windows Security) введите альтернативные имя пользователя и пароль и нажмите кнопку **OK**. Введенные учетные данные будут очищены после выхода из диспетчера серверов. Чтобы сохранить учетные записи и впоследствии использовать их, установите переключатель **Запомнить учетные данные** (Remember My Credentials) в окне **Безопасность Windows**. Эту процедуру нужно повторять при каждой смене пароля, связанного с учетной записью.

> ***Практический совет***
>
> При работе с установкой основных серверных компонентов утилита Sconfig может использоваться для настройки членства в домене и рабочей группе, имени компьютера, удаленного управления, Windows Update, сетевых настроек, а также даты и времени. Также можно применять Sconfig для выхода из системы, перезапуска и завершения работы сервера. Для запуска Sconfig просто введите `sconfig` в командной строке. Выберите опции из меню и настройте сервер.

На левой панели диспетчера серверов находятся команды для доступа к **Панели мониторинга**, локального сервера, всех серверов, доступных для управления, и групп серверов. Выбрав пункт **Локальный сервер** (Local Server) (рис. 2.2), можно управлять базовой конфигурацией локального сервера.

Информация о локальном сервере распределена по нескольким панелям.

- **АНАЛИЗАТОР СООТВЕТСТВИЯ РЕКОМЕНДАЦИЯМ** (BEST PRACTICES ANALYZER) — позволяет запустить анализатор соответствия рекомендациям на сервере и просмотреть результат. Для начала сканирования нажмите список-меню **Задачи** (Tasks), а потом выберите команду **Начать проверку BPA** (Start BPA Scan).
- **СОБЫТИЯ** (EVENTS) — общая информация об ошибках и предупреждениях, взятая из журналов сервера. Нажмите или щелкните по событию, чтобы получить больше информации о нем.
- **ПРОИЗВОДИТЕЛЬНОСТЬ** (PERFORMANCE) — позволяет настроить и просмотреть статус предупреждений производительности относительно использования центрального процессора и памяти.
- **СВОЙСТВА** (PROPERTIES) — показывает свойства компьютера, домена, конфигурации сети, часового пояса и т. д. Каждое свойство активно — по нему можно щелкнуть, чтобы вызвать соответствующий интерфейс управления.

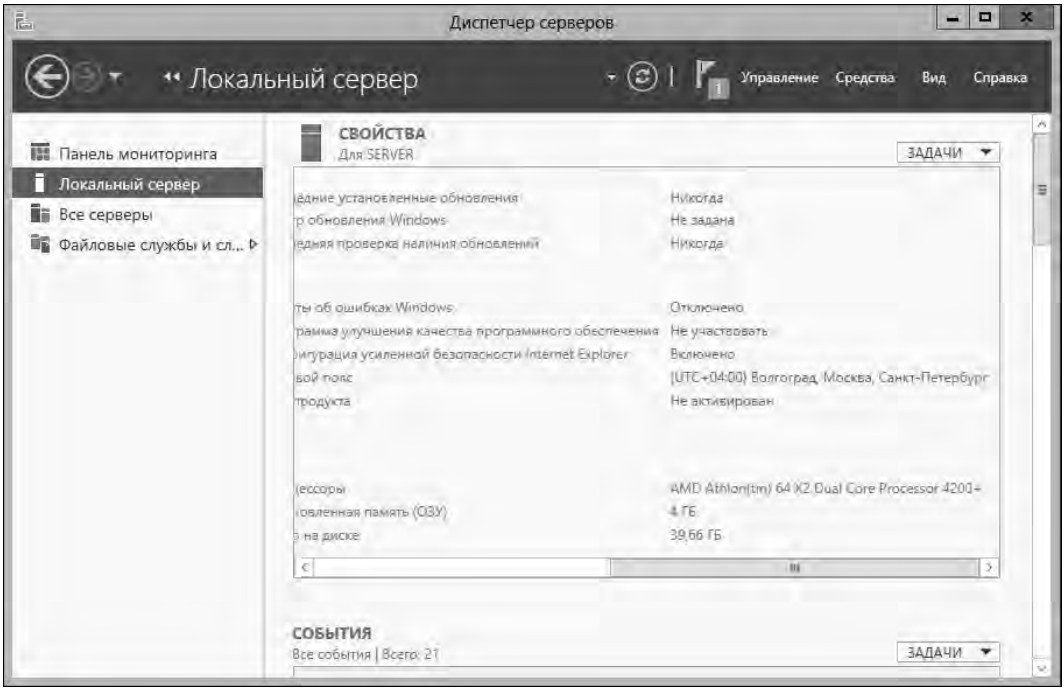


Рис. 2.2. Управление свойствами локального сервера

- **РОЛИ И КОМПОНЕНТЫ** (ROLES AND FEATURES) — выводит список ролей и компонентов в порядке их установки на сервер. Для удаления роли или компонента щелкните правой кнопкой мыши (или нажмите и удерживайте палец) и выберите команду **Удалить роль или компонент** (Remove role or feature).
- **СЛУЖБЫ** (SERVICES) — выводит список служб, запущенных на сервере (по имени, статусу и типу запуска). Для изменения статуса службы используйте контекстное меню.

Панель **СВОЙСТВА** (PROPERTIES) позволяет произвести начальную настройку сервера. Для быстрой настройки доступны следующие свойства.

- **Имя компьютера/Рабочая группа** (Computer Name/Domain) — отображает имя компьютера и домена. Щелкните по соответствующей ссылке, чтобы отобразить окно **Свойства системы** (System Properties) с активной вкладкой **Имя компьютера** (Computer Name). Затем можно изменить имя компьютера и имя домена, нажав кнопку **Изменить** (Change). После чего введите имя компьютера и домена и нажмите кнопку **OK**. По умолчанию серверам назначаются случайным образом сгенерированные имена, и они настраиваются как часть рабочей группы WORKGROUP. Вызвать окно **Свойства системы** можно с помощью Панели управления. Для этого запустите утилиту **Система** (System), когда выбрано представление **Крупные значки** (Large Icons) или **Мелкие значки** (Small Icons). Затем щелкните по ссылке **Изменить параметры** (Change Settings) напротив параметра **Компьютер** (Computer Name). Откроется окно **Свойства системы** с активной вкладкой **Имя компьютера**.
- **Программа улучшения качества программного обеспечения** (Customer Experience Improvement Program) — определяет, будет ли сервер принимать участие в Программе улучшения качества программного обеспечения (Customer Experience Improvement

Program, CEIP). Щелкните по соответствующей ссылке для изменения этой настройки. Участие в CEIP позволяет Microsoft собирать информацию об использовании вашего сервера. Microsoft собирает эти данные для улучшения будущих выпусков Windows. При участии в CEIP не собираются данные, позволяющие идентифицировать вас или вашу компанию. Если планируется участие в этой программе, можно также указать число серверов и рабочих станций в организации.

- **Ethernet** — показывает конфигурацию TCP/IP для проводных Ethernet-соединений. Щелкните по соответствующей ссылке, чтобы открыть консоль **Сетевые подключения** (Network Connections). Для настройки соединения дважды щелкните на нем, а затем нажмите **Свойства** (Properties) для открытия одноименного окна. По умолчанию серверы настраиваются для использования динамической адресации для IPv4 и IPv6. Консоль **Сетевые подключения** можно также вызвать из Центра управления сетями и общим доступом, выбрав задачу **Изменение параметров адаптера** (Change Adapter Settings).
- **Конфигурация усиленной безопасности Internet Explorer** (IE Enhanced Security Configuration) — показывает статус расширенной безопасности Internet Explorer (IE ESC). Щелкните по соответствующей ссылке для включения или отключения IE ESC. Данная функция может быть включена/выключена для пользователей, администраторов либо для тех и других одновременно. IE ESC — средство защиты, которое уменьшает восприимчивость сервера к потенциальным атакам, повышая стандартные уровни безопасности в зонах безопасности Internet Explorer и изменяя настройки этого браузера по умолчанию. По умолчанию функциональность IE ESC включена для администраторов и для пользователей.

  Практический совет

  В большинстве случаев у вас должна быть включена функциональность IE ESC и для администраторов, и для пользователей. Однако включение IE ESC ограничивает функциональность Internet Explorer. Когда расширенная безопасность Internet Explorer включена, зоны безопасности настраиваются так: для зоны **Интернет** (Internet) устанавливается высокий уровень безопасности, для зоны **Надежные сайты** (Trusted Sites) — средний, для зоны **Местная интрасеть** (Local Intranet) — ниже среднего, для зоны **Опасные сайты** (Restricted) — высокий. Также устанавливаются следующие параметры: включается параметр **Включить защищенный режим** (Enhanced Security Configuration), сторонние расширения и звуки страниц отключаются, анимация на веб-страницах отключается, включается проверка подписи для загружаемых программ, зашифрованные страницы не сохраняются, временные файлы Интернета удаляются при закрытии окна браузера, включаются предупреждения для защищенных и незащищенных режимов, включается защита памяти.

- **Объединение сетевых карт** (NIC Teaming) — показывает статус и конфигурацию объединения сетевых карт. Щелчок по соответствующей ссылке позволит добавить/удалить объединенные сетевые интерфейсы и изменить их настройки.
- **Код продукта** (Product ID) — показывает идентификатор продукта Windows Server. Щелкните по соответствующей ссылке для ввода кода продукта и активации операционной системы через Интернет.
- **Удаленный рабочий стол** (Remote Desktop) — щелкните по соответствующей ссылке, чтобы отобразить окно **Свойства системы** с активной вкладкой **Удаленный доступ** (Remote). Для настройки удаленного рабочего стола установите необходимые параметры и нажмите кнопку **OK**. По умолчанию удаленные соединения к серверу запрещены. Вызвать диалоговое окно **Свойства системы** можно с помощью утилиты **Система** (System) Панели управления, на левой панели которой нужно выбрать **Настройка удаленного доступа** (Remote Settings).

- **Удаленное администрирование** (Remote Management) — показывает, включено ли для этого сервера удаленное администрирование. Щелкните по соответствующей ссылке для включения или выключения удаленного администрирования.
- **Часовой пояс** (Time Zone) — показывает текущий часовой пояс для сервера. Щелкните по соответствующей ссылке для отображения окна **Дата и время** (Date And Time). Далее нажмите кнопку **Изменить часовой пояс** (Change Time Zone), выберите нужный часовой пояс и дважды нажмите кнопку **OK**. Также можно вызвать окно **Дата и время**, щелкнув правой кнопкой мыши на панели задач и выбрав команду **Настройка даты и времени** (Adjust Date/Time). Хотя все серверы настроены для автоматической синхронизации времени с интернет-сервером времени, процесс синхронизации времени не изменяет часовой пояс компьютера.
- **Отчеты об ошибках Windows** (Windows Error Reporting) — показывает статус средства Отчеты об ошибках Windows (Windows Error Reporting, WER). Щелкните по соответствующей ссылке для изменения настроек данного средства. В большинстве случаев нужно оставить средство включенным как минимум на протяжении 60 дней с момента установки операционной системы. С включенным средством WER ваш сервер будет отправлять описания проблем в Microsoft, а Windows — уведомлять вас о возможных решениях этих проблем. Просмотреть отчеты о проблеме и возможные решения можно с помощью Центра поддержки (Action Center). Чтобы открыть Центр поддержки, щелкните правой кнопкой мыши на значке Центра поддержки в области уведомлений панели задач и выберите команду **Открыть Центр поддержки** (Open Action Center).
- **Брандмауэр Windows** (Windows Firewall) — показывает статус брандмауэра Windows. Если брандмауэр активен, это свойство отображает имя активного профиля и статус брандмауэра. Щелкните по соответствующей ссылке для отображения окна утилиты **Брандмауэр Windows** (Windows Firewall). По умолчанию брандмауэр Windows включен. Эту же утилиту можно вызвать через Панель управления, переключив ее в режим **Крупные значки** (или **Мелкие значки**) и дважды щелкнув на ссылке **Брандмауэр Windows**.
- **Центр обновления Windows** (Windows Update) — показывает текущий статус Центра обновления Windows. Щелчок (или нажатие) по соответствующей ссылке позволяет вызвать утилиту Центр обновления Windows, которую можно использовать для автоматического обновления (если обновление отключено) или проверить наличие обновлений (если обновление включено). Аналогично, данную утилиту можно вызвать через Панель управления.

> ***Примечание***
>
> Данная сводка опций приведена в качестве введения и справочника. В дальнейшем упомянутые ранее технологии и задачи конфигурации будут подробно рассмотрены.

Основные компоненты диспетчера серверов и двоичные файлы

Консоль **Диспетчер серверов** разработана для того, чтобы управлять основными адмистративными задачами. С этим инструментом администратор проводит много времени, поэтому ему нужно знать каждую деталь. По умолчанию диспетчер серверов запускается автоматически. Если консоль закрыта или отключен автоматический запуск, открыть консоль можно путем нажатия соответствующей кнопки на панели задач. Аналогично, нажмите клавишу

<Windows>, введите `ServerManager.exe` в поле **Поиск** (Apps Search) и нажмите клавишу <Enter>.

Командная строка диспетчера серверов — это модуль диспетчера серверов для Windows PowerShell. При входе в Windows Server 2012 этот модуль импортируется в Windows PowerShell по умолчанию. В противном случае перед использованием командлетов, которые предоставляются этим модулем, нужно импортировать модуль командной строки. Импортировать модуль диспетчера серверов можно с помощью команды `Import-Module ServerManager` в приглашении Windows PowerShell.

Как только модуль будет импортирован, его можно использовать в текущем экземпляре Windows PowerShell. При следующем запуске Windows PowerShell этот модуль нужно будет импортировать снова (при необходимости).

В приглашении Windows PowerShell для получения полного списка текущих ролей, ролевых служб и компонентов используется команда `get-windowsfeature`. Каждая установленная роль, ролевая служба и компонент выделяется крестиком в квадратных скобках — `[x]`, если в скобках ничего нет, значит, роль или компонент не установлены. Используя командлеты Install-WindowsFeature или Uninstall-WindowsFeature, можно установить или удалить роль, ролевую службу или компонент. Например, для установки компонента **Балансировка сетевой нагрузки** (Network Load Balancing, NLB) используется команда `install-windowsfeature nlb`. Параметр `-includesubfeature` применяется для установки всех подчиненных ролевых служб и компонентов. Инструменты управления по умолчанию не устанавливаются, для этого нужно указать параметр `-includemanagementtools` при установке компонентов.

Двоичные файлы, необходимые для работы различных ролей и компонентов, называются *полезными данными* (payloads). Они хранятся в подпапках каталога *%SystemDrive%*\Windows\WinSXS. При удалении компонента можно удалить не только сам компонент или роль, но и связанные с ними полезные данные. Для этого укажите параметр `-Remove` командлета Uninstall-WindowsFeature. Подкомпоненты роли/компонента тоже будут удалены. Для удаления инструментов управления нужно использовать параметр `-includeallmanagementtools`.

При установке роли или компонента можно установить и соответствующие компоненты, а также восстановить любой удаленный дополнительный двоичный файл для этих компонентов, используя командлет Install-WindowsFeature. По умолчанию при использовании командлета Install-WindowsFeature полезные данные восстанавливаются через Центр обновления Windows.

В следующем примере восстанавливаются полезные данные AD DS и все соответствующие подкомпоненты с помощью Центра обновления Windows:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature
```

Параметр `-Source` используется для восстановления полезных данных из точки монтирования WIM (Windows Imaging). Например, если в вашей организации есть смонтированный образ Windows Server 2012, доступный в сети по адресу \\ImServer18\WinS12EE, можно установить его в качестве источника:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature -source
\\imserver18\wins12ee
```

Помните, что указанный вами путь используется только для полезных данных, не найденных в папке Windows Side-By-Side (WinSXS) сервера. На многих крупных предприятиях в сети доступен образ Windows Server 2012, но можно смонтировать дистрибутивный диск

и использовать папку Windows\WinSXS этого диска в качестве источника. Чтобы сделать это, выполните следующие действия:

1. Вставьте инсталляционный диск в привод сервера и создайте папку, к которой будет подмонтирован образ: `mkdir c:\mountdir`.
2. Определите номер образа командой `dism /get-wiminfo /wimfile:e:\ sources\ install.wim`, где `e:` — имя диска сервера.
3. Подмонтируйте инсталляционный образ с помощью команды: `dism /mount-wim /wimfile:e:\sources\install.wim /index:2 /mountdir:c:\mountdir /readonly`, где `e:` — буква диска сервера; `2` — индекс используемого образа; `c:\mountdir` — каталог монтирования. Монтирование образа занимает несколько минут.
4. Используйте командлет Install-WindowsFeature в приглашении PowerShell, укажите каталог `c:\mountdir\windows\winsxs` в качестве источника:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature -source
c:\mountdir\windows\winsxs
```

В качестве альтернативного источника для восстановления полезных данных Центром обновления Windows может использоваться групповая политика. Нужная политика называет-

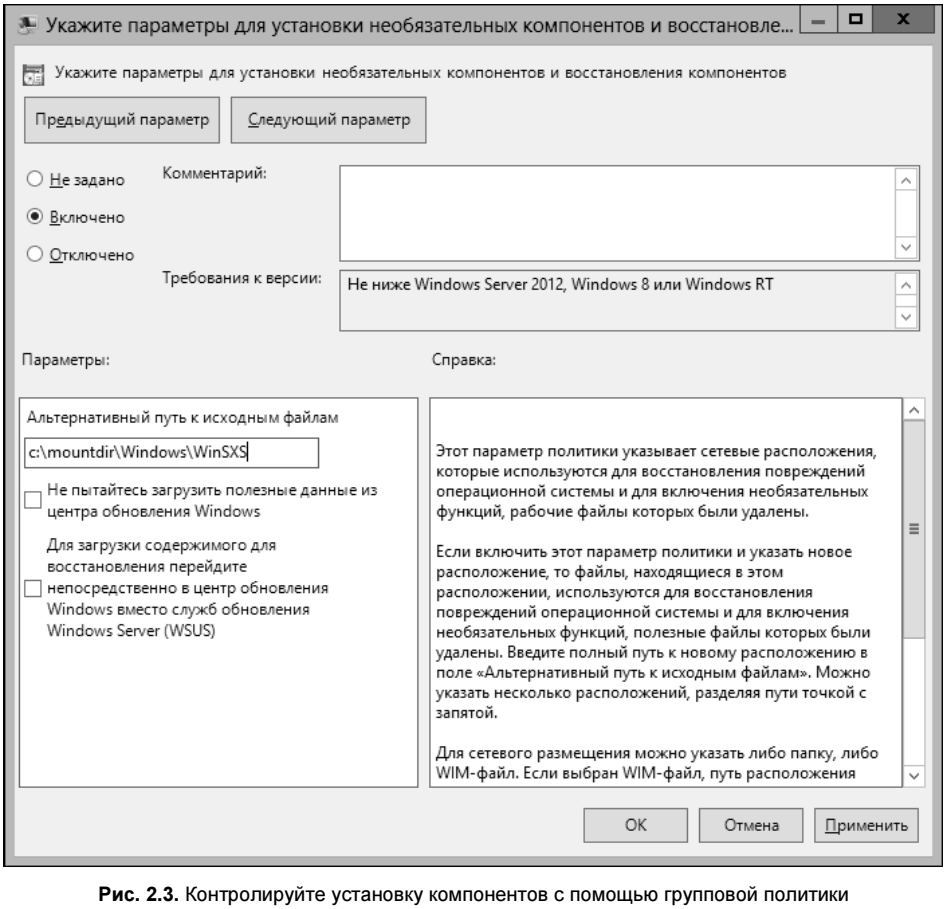


Рис. 2.3. Контролируйте установку компонентов с помощью групповой политики

ся **Укажите параметры для установки необязательных компонентов и восстановления компонентов** (Specify Settings For Optional Component Installation And Component Repair), она находится в узле **Конфигурация компьютера\Административные шаблоны\Система** (Computer Configuration\Administrative Templates\System). Эта политика также используется для получения полезных данных, необходимых для восстановления компонентов.

При включении этой политики (рис. 2.3) можно сделать следующее.

- Указать альтернативный источник для двоичных файлов ролей и компонентов. Для сетевых ресурсов укажите UNC, например, **\\CorpServer82\WinServer2012**, для смонтированных образов укажите префикс WIM и номер используемого образа, например, **WIM:\\CorpServer82\WinServer2012\install.wim:4**.
- Указать, что Центр обновления Windows не должен использоваться для загрузки полезных данных. Если включаете политику и используете эту опцию, не нужно указывать альтернативный источник. В этом случае полезные данные не будут получены автоматически, а администраторы должны явно указать альтернативный источник.
- Указать, что для восстановления компонентов вместо служб обновления Windows Server (WSUS) должен использоваться Центр обновления Windows.

Удаленное управление серверами

Диспетчер серверов и другие консоли управления Microsoft (Microsoft Management Consoles, MMC) могут использоваться для администрирования удаленных компьютеров, входящих как в состав домена, так и в состав рабочей группы. Возможно подключение к серверам, работающим под управлением полной установки, установки с минимальным графическим интерфейсом пользователя и установки Server Core. На компьютере, который будет использоваться для удаленного управления другими компьютерами, должна быть установлена ОС Windows 8 или ОС Windows Server 2012, а также **Средства удаленного администрирования сервера** (Remote Server Administration Tools).

В Windows Server 2012 **Средства удаленного администрирования сервера** могут быть установлены в виде компонента с помощью мастера добавления ролей и компонентов. Если двоичные файлы были удалены, необходимо указать источник двоичных файлов, как было показано ранее в этой главе.

Средства удаленного администрирования сервера для Windows 8 можно получить через центр загрузок Microsoft — Download Center (**download.microsoft.com**). Обратите внимание, что есть разные версии для систем *x*86 и *x*64.

По умолчанию удаленное управление включено для серверов под управлением Windows Server 2012 для двух типов приложений и команд:

- приложения и команды, которые используют для управления удаленный доступ WinRM и Windows PowerShell;
- приложения и команды, которые для удаленного управления используют WMI (Windows Management Instrumentation) и DCOM (Distributed Component Object Model).

Данные типы приложений и команд разрешены для удаленного управления, поскольку для них настроены исключения в правилах брандмауэра Windows, который включен по умолчанию в Windows Server 2012. В брандмауэре Windows есть исключения для разрешенных приложений, использующих удаленное управление, включая следующие средства:

- Windows Management Instrumentation;
- Windows Remote Management;
- Windows Remote Management (в режиме совместимости).

В дополнительных параметрах брандмауэра Windows имеются правила для входящих соединений, которые соответствуют стандартным разрешенным приложениям.

- Для WMI входящие правила называются: **Инструментарий управления Windows (WMI — входящий трафик)** (Windows Management Instrumentation (WMI-In)), **Инструментарий управления Windows (DCOM — входящий трафик)** (Windows Management Instrumentation (DCOM-In)), **Инструментарий управления Windows (асинхронный — входящий трафик)** (Windows Management Instrumentation (ASync-In)).
- Для WinRM входящее правило — **Удаленное управление Windows (HTTP — входящий трафик)** (Windows Remote Management (HTTP-In)).
- Для WinRM в режиме совместимости входящее правило — **Удаленное управление Windows — режим совместимости (HTTP — входящий трафик)** (Windows Remote Management — Compatibility Mode (HTTP-In)).

Управлять этими исключениями (или правилами) можно или в стандартном Брандмауэре Windows, или в Брандмауэре Windows в режиме повышенной безопасности. Если необходимо разрешить удаленное управление, а также работу диспетчера серверов, MMC и Windows PowerShell, обычно нужно разрешить исключения WMI, WinRM и WinRM (в режиме совместимости) в Брандмауэре Windows.

При работе с диспетчером серверов для просмотра статуса удаленного управления выберите кнопку **Локальный сервер** (Local Server) в его консоли. Для запрещения удаленного администрирования щелкните по соответствующей ссылке. В диалоговом окне **Настройка удаленного управления** (Configure Remote Management) сбросьте флажок **Разрешить удаленное управление этим сервером с других компьютеров** (Enable Remote Management Of This Server From Other Computers) и нажмите кнопку **OK**.

После этого диспетчер серверов выполнит несколько фоновых задач для отключения службы **Удаленное управление Windows (WinRM)** и удаленного доступа Windows PowerShell для управления локальным сервером. Одна из этих задач — выключение соответствующего исключения, которое позволяет приложениям взаимодействовать через Брандмауэр Windows, используя удаленное управление Windows. Исключения для компонентов **Инструментарий управления Windows** (Windows Management Instrumentation) и **Удаленное управление Windows в режиме совместимости** (Windows Remote Management (Compatibility)) не будут затронуты.

Для управления компьютером с помощью диспетчера серверов пользователь должен быть членом группы **Администраторы** (Administrators). Для удаленных соединений в конфигурациях "рабочая группа — рабочая группа" или "рабочая группа — домен" вам нужно войти в систему с использованием встроенной учетной записи **Администратор** (Administrator) или настроить ключ реестра `LocalAccountTokenFilterPolicy` для разрешения удаленного доступа с вашего компьютера. Для установки этого ключа используется следующая команда, которую нужно ввести в командной строке с привилегиями администратора:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

> ***Примечание***
>
> Для включения удаленного управления воспользуйтесь следующей командой, которую нужно ввести в командной строке с правами администратора:
>
> ```
> configure-SMRemoting.exe –enable
> ```

Примечание

Если нужно удаленно управлять компьютером, работающим на базе Windows 8, введите команду `winrm quickconfig` (управление производится с использованием протокола WS-Management). На все задаваемые вопросы нужно ответить `Y`. В результате будет запущена служба **Удаленное управление Windows (WinRM)** и настроена на прием запросов WS-Management с любого IP-адреса, созданы исключения брандмауэра для удаленного управления Windows, а также настроен ключ `LocalAccountTokenFilterPolicy` для предоставления соответствующих административных прав для удаленного управления.

Множество иных типов удаленного управления зависит от других исключений брандмауэра Windows.

- **Удаленный рабочий стол (Remote Desktop)** — может быть включен/отключен отдельно от удаленного администрирования. Чтобы разрешить другим пользователям подключаться к локальному серверу с использованием удаленного рабочего стола, нужно разрешить соответствующие соединения к компьютеру и настроить доступ к нему *(см. главу 4)*.
- **Удаленное управление службами (Remote Service Management)** — используется для удаленного управления службами компьютера, должно быть создано соответствующее правило Брандмауэра Windows. В дополнительных параметрах брандмауэра есть несколько правил, разрешающих управление, например, **Удаленное управление службой (RPC)** и **Удаленное управление службой (именованные каналы, NP)**.
- **Удаленное управление журналом событий** — должно быть настроено как разрешенное приложение Брандмауэра Windows для удаленного управления журналом событий компьютера. В дополнительных параметрах брандмауэра есть несколько соответствующих правил, разрешающих управление с помощью технологий NP (Named Pipes) и RPC (Remote Procedure Call).
- **Удаленное управление томами** — должно быть настроено как разрешенное управление Брандмауэром Windows для удаленного управления томами. В дополнительных параметрах брандмауэра есть несколько соответствующих правил: **Управление удаленными томами — служба виртуальных дисков**, **Управление удаленными томами — загрузчик службы виртуальных дисков**.
- **Удаленное управление назначенными задачами** — должно быть настроено как разрешенное приложение Брандмауэра Windows, чтобы удаленно управлять назначенными задачами компьютера. В дополнительных настройках брандмауэра есть несколько соответствующих правил, которые разрешают управление назначенными задачами через RPC.

По умолчанию включено лишь исключение **Удаленное управление службами**.

В установке основных серверных компонентов удаленное управление настраивается с помощью утилиты Sconfig. Запустите конфигурационную утилиту с помощью команды `sconfig`.

Подключение и работа с удаленными серверами

Используя диспетчер серверов, можно подключиться к удаленным серверам и управлять ими при условии, что сервер добавлен в список для управления. Для добавления сервера в диспетчер серверов выполните следующие действия:

1. Откройте диспетчер серверов. В левой панели выберите пункт **Все серверы** для просмотра всех добавленных для управления серверов. Если необходимого сервера нет

в списке, в меню **Управление** (Manage) выберите команду **Добавление серверов** (Add Servers). Откроется одноименное диалоговое окно.

2. В окне **Добавление серверов** есть две панели:
   - **Active Directory** (выбрана по умолчанию) — позволяет ввести короткое или полное имя удаленного сервера, работающего под управлением Windows Server. Введите имя сервера и нажмите кнопку **Найти** (Find Now);
   - **DNS** — позволяет добавить серверы по имени или IP-адресу. Введите имя или IP-адрес и нажмите кнопку **Поиск** (Search).
3. Дважды щелкните на найденном сервере для помещения его в список **Выбрано** (Selected).
4. Повторите действия 2—3 для добавления других серверов. Нажмите кнопку **OK**.

Для добавления сразу нескольких серверов в диспетчер серверов применяется процесс импорта:

1. Создайте текстовый файл, который содержит имена добавляемых серверов — по одному в каждой строке (можно указывать имя, полное имя или IP-адрес).
2. В диспетчере серверов в меню **Управление** выберите команду **Добавление серверов**. В окне **Добавление серверов** перейдите на панель **Импорт** (Import).
3. Нажмите кнопку выбора файла справа от поля **Файл** (File). Используя окно открытия файла, откройте список серверов.
4. В списке компьютеров дважды щелкните на каждом сервере, который нужно добавить. Он будет перемещен в список **Выбрано**. Нажмите кнопку **OK**.

После добавления удаленного компьютера консоль диспетчера серверов покажет имя удаленного компьютера в представлении **Все серверы**. Диспетчер серверов всегда разрешает IP-адреса в имена узлов. Панель **Все серверы** также отображает статус управляемости каждого сервера (рис. 2.4). Если сервер имеет статус **Недоступен** (Not accessible), нужно зарегистрироваться на нем локально для решения проблемы.

В представлении **Все серверы** все добавленные вами серверы перечислены на панели **СЕРВЕРЫ**, поэтому можно управлять каждым из них всякий раз при работе с диспетчером серверов. Консоль **Диспетчер серверов** отслеживает службы, события и многое другое для каждого добавленного сервера. Каждый сервер автоматически добавляется в соответствующую группу в зависимости от его роли и установленных компонентов.

Автоматические создаваемые группы делают проще управление различными ролями и компонентами, установленными на серверах. Например, если выбрать группу AD DS, будет отображен список контроллеров доменов, добавленных для управления, также будет можно просмотреть любое критическое событие или предупреждение на этих серверах и просмотреть статус служб, от которых зависит роль сервера.

Если необходимо группировать серверы по департаменту, географическому расположению, можно создать собственные группы серверов. При создании группы серверы, с которыми планируется работа, не следует добавлять в диспетчер серверов. Серверы можно добавить с помощью поиска по Active Directory или DNS либо посредством импорта списка имен/IP-адресов. Любой сервер, добавленный в группу, также будет доступен для управления.

Чтобы создать группу серверов, выполните следующие действия:

1. Откройте диспетчер серверов. В меню **Управление** выберите команду **Создание группы серверов** (Create Server Group) для отображения одноименного окна.

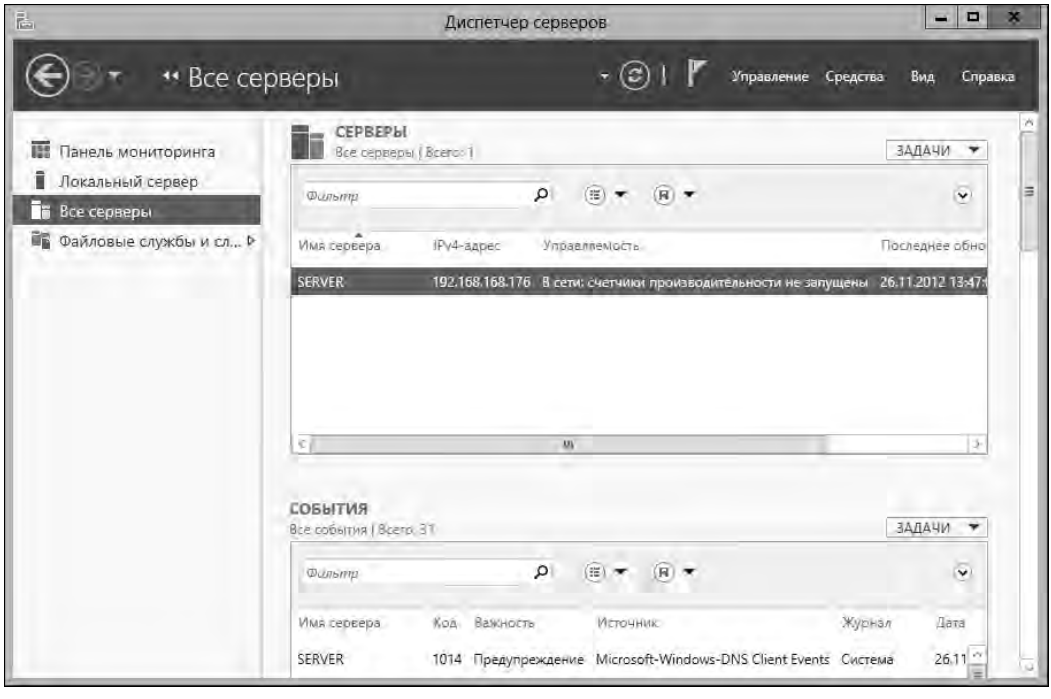


Рис. 2.4. Обратите внимание на статус **Управляемость** каждого сервера и внесите коррективы при необходимости

2. Введите имя группы. Используйте панели и параметры, предназначенные для добавления серверов в группы. Помните о следующем.
   - Панель **Пул серверов** (Server Pool) выбирается по умолчанию, выводит серверы, уже добавленные для управления. Если сервер, который нужно добавить в группу, есть в этом списке, добавьте его в группу с помощью двойного нажатия или двойного щелчка.
   - Панель **Active Directory** позволяет ввести полное или сокращенное имя удаленного сервера, работающего под управлением Windows Server. После того как введете имя, нажмите кнопку **Найти** (Find Now). В списке имен выберите сервер и с помощью двойного нажатия или двойного щелчка добавьте его в список **Выбрано** (Selected).
   - Панель **DNS** позволяет добавить серверы по имени компьютера или IP-адресу. Введите IP-адрес или имя и нажмите кнопку **Поиск** (Search). В списке серверов дважды щелкните по серверу для его добавления в список **Выбрано**.
   - Панель **Импорт** (Import) позволяет импортировать список серверов. Нажмите кнопку выбора файла справа от поля **Файл** (File), затем используйте окно открытия, чтобы открыть список серверов. В списке **Компьютер** (Computer) дважды щелкните по серверу, чтобы добавить его в список **Выбрано**.
3. Нажмите кнопку **OK** для создания группы сервера.

При щелчке правой кнопкой мыши по имени сервера на панели **Серверы** (в группе серверов или в представлении **Все серверы**) будет отображен расширенный список команд управления. Все эти команды позволяют выполнить соответствующее действие или открыть соответствующую утилиту управления для выбранного сервера. Например, если

щелкнуть правой кнопкой мыши по серверу CorpServer172, а затем выбрать команду **Управление компьютером** (Computer Management), оснастка **Управление компьютером** подключится к CorpServer172 и откроет его.

Работать с удаленным компьютером можно и с использованием интерактивной удаленной сессии Windows PowerShell. Для этого откройте командную строку Windows PowerShell с правами администратора и введите команду `enter-pssession` *ИмяКомпьютера* `-credential` *ИмяПользователя*, где *ИмяКомпьютера* — имя удаленного компьютера, а *ИмяПользователя* — имя пользователя, являющегося членом группы **Администраторы** на удаленном компьютере или домене, к которому принадлежит этот компьютер. Когда вас попросят, введите пароль пользователя и нажмите клавишу <Enter>. Теперь можно вводить команды, как будто бы Windows PowerShell используется локально. Для выхода из удаленной сессии введите команду `exit-pssession`.

В следующем примере мы устанавливаем интерактивную удаленную сессию с сервером Server85, используя учетные данные пользователя Williams:

```
enter-pssession server85 -credential williams
```

Добавление и удаление ролей, ролевых служб и компонентов

Диспетчер серверов автоматически создает группы серверов, добавленных для управления, на основании их ролей. Например, при создании первого контроллера домена диспетчер серверов создаст группы **AD DS**, **DNS** и **Файловые службы и службы хранилища** (File And Storage Services), чтобы администратор мог легко отслеживать роли контроллеров домена.

При выборе на панели слева группы, основанной на роли, панель **СЕРВЕРЫ** отображает перечень всех серверов, добавленных для управления и обладающих этой ролью. Предоставлена следующая информация:

- общая информация о событиях. Диспетчер серверов выводит последние предупреждения и ошибки. Если щелкнуть по событию, то можно получить подробную информацию;
- общая информация о статусе соответствующих системных сервисов. Можно щелкнуть правой кнопкой мыши (или нажать и удерживать палец) для управления статусом службы.

> ***Совет***
>
> По умолчанию диспетчер серверов обновляет подробности каждые 10 минут. Для самостоятельного обновления консоли **Диспетчер серверов** нажмите кнопку **Обновить "Все серверы"** (Refresh Servers) на панели инструментов. Если нужно установить другой интервал обновления, в меню **Управление** выберите команду **Свойства диспетчера серверов** (Server Manager Properties). Далее установите новый интервал обновления в минутах и нажмите кнопку **OK**.

Для управления службой щелкните правой кнопкой мыши по службе и выберите одну из команд: **Остановить службы** (Stop Service), **Запустить службы** (Start Service), **Приостановить службы** (Pause Service), **Перезапустить службы** (Restart Service), **Возобновить работу служб** (Resume Service). Во многих случаях, если служба не работает, можно использовать команду **Перезапустить службы** (Restart Service): служба будет сначала остановлена, а потом запущена. Для получения дальнейшей информации о работе с событиями и системными службами *см. главу 3*.

В меню **Управление** есть две ключевые команды для работы с ролями и компонентами:

- **Добавить роли и компоненты** (Add Roles And Features) — запускает мастер добавления ролей и компонентов, который используется для установки ролей и компонентов на сервере, добавленном для управления;
- **Удалить роли и компоненты** (Remove Roles And Features) — запускает мастер удаления ролей и компонентов, используемый для деинсталляции ролей и компонентов на серверах, доступных для администрирования.

В ОС Windows Server 2012 можно установить роли, компоненты и виртуальные жесткие диски на запущенных серверах (без разницы — виртуальных или физических). Серверы должны быть добавлены в диспетчер серверов и находиться в онлайн-режиме. Виртуальные жесткие диски, с которыми необходимо работать, не должны быть в онлайн-режиме, они должны быть доступны для выбора. Учитывая все это, добавить роль сервера или компонент можно с помощью следующих действий:

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**. Можно отказаться от просмотра этой страницы при каждом запуске мастера, установив флажок **Пропускать эту страницу по умолчанию** (Skip This Page By Default) перед нажатием кнопки **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**.

   Примечание

   В списке серверов (шаг 3) будут только серверы под управлением Windows Server 2012 и те, которые администратор добавил в диспетчере серверов.

4. На странице **Выбор ролей сервера** (Server Roles) выберите одну или несколько ролей для установки. Если для установки роли требуются дополнительные компоненты, будет отображено дополнительное 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) выберите один или несколько компонентов для установки. Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, 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**.
6. В случае с некоторыми ролями будут показаны дополнительные страницы мастера, на которых нужно будет предоставить дополнительную информацию относительно использования и настройки роли. Также можно установить дополнительные ролевые службы

как часть роли. Например, при установке следующих ролей будут отображены дополнительные страницы мастера: **Службы печати и документов**, **Веб-сервер (IIS)**, **Службы Windows Server Update Services (WSUS)**.

7. 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.
8. Если сервер, на котором необходимо установить роли или компоненты 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**. Например, образ Windows смонтирован и сделан доступным на локальном сервере, как было показано в *разд. "Основные компоненты диспетчера серверов и двоичные файлы" ранее в этой главе*, можно ввести альтернативный путь в виде c:\mountdir\windows\winsxs. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer20120\. Для смонтированных образов введите WIM-путь с префиксом `WIM` и индексом используемого образа, например, `WIM:\\CorpServer82\WinServer2-12\install.wim:4`.
9. 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.
10. О завершении установки выбранных ролей и компонентов сообщит страница **Ход установки**. 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 диспетчера сервера, чтобы понять суть проблемы, и примите соответствующие корректирующие действия.

> ***Примечание***
>
> Некоторые роли не могут быть добавлены одновременно с другими ролями. Тогда нужно установить каждую роль отдельно. Другие роли не могут быть установлены совместно с уже установленными ролями, и об этом будут отображены соответствующие сообщения. Сервер с установкой основных серверных компонентов может работать как контроллер домена и выполнять любые FSMO-роли (операции с одним исполнителем) для Active Directory.

Для удаления роли сервера или компонента выполните следующие действия:

1. В консоли **Диспетчер серверов** в меню **Управление** выберите команду **Удалить роли и компоненты** (Remove Roles And Features). Будет запущен мастер удаления ролей и компонентов. Если мастер отобразит страницу **Перед началом работы**, прочитайте вступительный текст и затем нажмите кнопку **Далее**. Можно отказаться от просмотра этой страницы при каждом запуске мастера, установив флажок **Пропускать эту страницу по умолчанию** перед нажатием кнопки **Далее**.
2. На странице **Выбор целевого сервера** укажите, где находятся удаляемые роли и компоненты — на сервере или на виртуальном жестком диске (VHD). Выберите сервер из пула

серверов либо сервер, на котором можно смонтировать виртуальный жесткий диск. При удалении ролей и компонентов из VHD нажмите кнопку **Обзор**, а затем используйте окно **Обзор виртуальных жестких дисков** для выбора вашего VHD. Когда будете готовы продолжить, нажмите кнопку **Далее**.

3. На странице **Удаление ролей сервера** (Server Roles) снимите флажок напротив названия роли, которую нужно удалить. При попытке удалить роль, от которой зависит другая роль или компонент, появится соответствующее предупреждение о невозможности сделать это без удаления других ролей или компонентов. Если нажать кнопку **Удалить компоненты** (Remove Features), мастер удалит зависимые роли и компоненты. Заметьте, что если необходимы соответствующие инструменты управления, следует сбросить флажок **Удалить средства управления** (Remove Management Tools) перед нажатием кнопки **Удалить компоненты**, затем нажать кнопку **Далее**.
4. На странице **Удаление компонентов** (Features) снимите флажок напротив названия компонента, который необходимо удалить. При попытке удалить компонент, от которого зависит другая роль или компонент, появится соответствующее предупреждение о невозможности сделать это без удаления других ролей или компонентов. Если нажать кнопку **Удалить компоненты** (Remove Features), мастер удалит зависимые роли и компоненты. Если нужно сохранить соответствующие инструменты управления, снимите флажок **Удалить средства управления** перед нажатием кнопки **Удалить компоненты**, затем нажмите кнопку **Далее**.
5. На странице **Подтверждение удаления компонентов** (Confirmation) просмотрите соответствующие компоненты, которые мастер будет удалять, и нажмите кнопку **Удалить** (Remove). Страница **Ход удаления** (Removal Progress) отобразит процесс удаления компонентов. Если окно мастера закрыто, заново открыть его можно с помощью значка **Уведомления** (Notifications) на панели инструментов диспетчера серверов: щелкните по нему и щелкните по ссылке, предназначенной для повторного открытия мастера.
6. О завершении конфигурации сервера сообщит страница **Ход удаления**. Просмотрите детали установки и убедитесь, что все фазы процесса удаления завершены успешно. Заметьте, что для полного удаления могут понадобиться дополнительные действия, например, перезагрузка или дополнительные задачи удаления. Если какая-нибудь часть удаления провалена, запомните причину сбоя. Просмотрите записи диспетчера серверов для решения проблем и внесите соответствующие коррективы.

Управление свойствами системы

Консоль **Система** (System) используется для просмотра системной информации и осуществления базовых задач конфигурации. Чтобы открыть эту консоль, дважды щелкните по значку **Система** в Панели управления. Консоль **Система** делится на четыре основных области (рис. 2.5), предоставляющие обзор системы и ссылки для осуществления общих задач:

- **Выпуск Windows** (Windows Edition) — показывает выпуск и версию операционной системы, а также список примененных сервис-паков;
- **Система** (System) — выводит информацию о процессоре, оперативной памяти и типе установленной операционной системы — 32- или 64-разрядная;
- **Имя компьютера, имя домена и параметры рабочей группы** (Computer Name, Domain, And Workgroup Settings) — выводит имя компьютера, описание, домен и пара-

метры рабочей группы. Для изменения этой информации щелкните по ссылке **Изменить параметры** (Change Settings), затем нажмите кнопку **Изменить** (Change) в окне **Свойства системы** (System Properties);

- **Активация Windows** (Windows Activation) — показывает, активирована ли операционная система, а также выводит ключ продукта. Если система Windows Server 2012 еще не активирована, щелкните по соответствующей ссылке для начала процесса активации, а затем следуйте инструкциям.

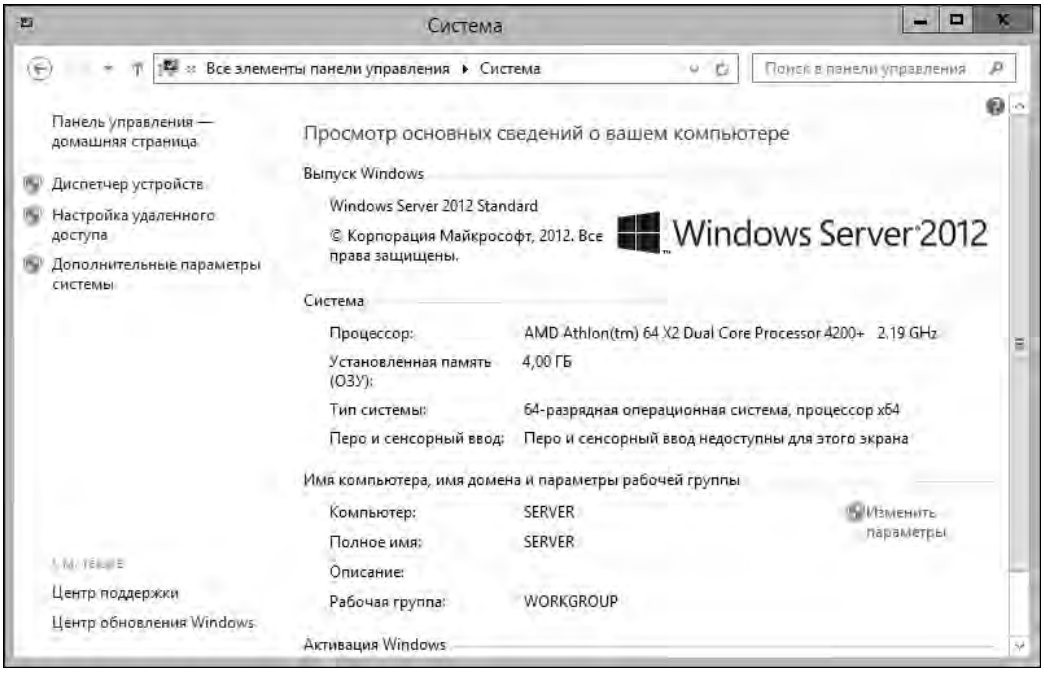


Рис. 2.5. Используйте консоль **Система** для просмотра и управления свойствами системы

В консоли **Система** слева находятся ссылки для быстрого доступа к ключевым инструментам:

- **Диспетчер устройств** (Device Manager);
- **Настройка удаленного доступа** (Remote Settings);
- **Дополнительные параметры системы** (Advanced System Settings).

Хотя корпоративные версии ОС Windows Server 2012 могут не требовать активации и ввода ключа продукта, коробочные (retail) версии запрашивают и активацию, и ключ продукта. Если Windows Server 2012 еще не активирована, щелкните по ссылке **Активировать Windows сейчас** (Activate Windows Now) в разделе **Активация Windows**. Также можно активировать Windows путем ввода команды `slmgr -ato` в командной строке.

Для изменения кода продукта, введенного во время установки Windows Server 2012, введите команду `slmgr -ipk`, сопровождаемую ключом продукта, который нужно установить, а затем нажмите клавишу <Enter>. После проверки подлинности ключа нужно будет заново активировать операционную систему.

Примечание

У утилиты slmgr (Windows Software Management Licensing tool) много разных параметров, в том числе опции для оффлайн-активации. Чтобы просмотреть эти опции, введите `slmgr` в командной строке.

Из консоли **Система** можно открыть окно **Свойства системы**, которое используется для управления различными свойствами системы. Для этого щелкните по ссылке **Изменить параметры** в области **Имя компьютера, имя домена и параметры рабочей группы**. В следующих разделах мы рассмотрим ключевые области операционной системы, которые можно настроить с помощью окна **Свойства системы**.

Вкладка *Имя компьютера*

Просмотреть и изменить сетевой идентификатор компьютера можно на вкладке **Имя компьютера** окна **Свойства системы**. Эта вкладка отображает полное имя системы, а также членство в домене. Полное имя компьютера — это, по сути, DNS-имя, которое также определяет место компьютера в иерархии Active Directory. Если компьютер — контроллер домена или центр сертификации, изменить имя можно только после удаления соответствующей роли компьютера.

Для присоединения компьютера к домену или рабочей группе выполните следующие действия:

1. На вкладке **Имя компьютера** окна **Свойства системы** нажмите кнопку **Изменить** (Change). Откроется окно **Изменение имени компьютера или домена** (Computer Name/Domain Changes).
2. Для добавления компьютера в рабочую группу выберите переключатель **Является членом рабочей группы** (Workgroup), а затем введите имя самой рабочей группы и нажмите кнопку **OK**.
3. Для добавления компьютера в домен выберите переключатель **Является членом домена** (Domain), введите имя домена и нажмите кнопку **OK**.
4. При изменении членства компьютера в домене будет отображено окно **Безопасность Windows** (Windows Security). Введите имя и пароль учетной записи с правами, позволяющими добавить компьютер в специфический домен или удалить компьютер из ранее установленного домена, а затем нажмите кнопку **OK**.
5. Потом появится уведомление о том, что компьютер присоединен к указанному домену или рабочей группе, нажмите кнопку **OK**.
6. Далее появится сообщение о необходимости перезагрузки компьютера, нажмите кнопку **OK**.
7. Нажмите кнопку **Закрыть** (Close), а затем кнопку **Перезагрузить сейчас** (Restart Now) для перезапуска компьютера.

Для изменения имени компьютера выполните следующие действия:

1. На вкладке **Имя компьютера** окна **Свойства системы** нажмите кнопку **Изменить**. Откроется окно **Изменение имени компьютера или домена**.
2. В поле **Имя компьютера** (Computer Name) введите новое имя.
3. Появится сообщение о необходимости перезагрузки компьютера, нажмите кнопку **OK**.
4. Нажмите кнопку **Закрыть**, а затем кнопку **Перезагрузить сейчас** для перезапуска компьютера.

Вкладка *Оборудование*

Вкладка **Оборудование** (Hardware) окна **Свойства системы** предоставляет доступ к диспетчеру устройств и параметрам установки устройств.

Для установленных устройств можно настроить Windows Server для загрузки драйверов и отображения реалистичных значков устройств. По умолчанию Windows Server не делает этого.

Если нужно, чтобы компьютер загружал драйверы автоматически, нажмите кнопку **Параметры установки устройств** (Device Installation Settings), а затем выберите вариант **Да, делать это автоматически** (Yes, Do This Automatically) или **Нет, предоставить мне возможность выбора** (No, Let Me Choose What To Do). Если выбран второй вариант, то можно указать следующее:

- **Всегда устанавливать наиболее подходящие драйверы из Центра обновления Windows** (Always install the best driver software from Windows Update);
- **Никогда не устанавливать драйверы из Центра обновления Windows** (Never install driver software from Windows Update);
- **Получать приложения для устройств и информацию, предоставляемую изготовителем устройства** (Automatically get the device apps and info provided by your device manufacturer).

Первые две опции понятны без дополнительных пояснений. Третья опция просит Центр обновления Windows загружать метаданные и сопутствующие программы для устройств. Нажмите кнопку **Сохранить** (Save Changes), а затем кнопку **OK**.

Вкладка *Дополнительно*

Вкладка **Дополнительно** (Advanced) окна **Свойства системы** позволяет контролировать много ключевых моментов операционной системы Windows, в том числе производительность приложений, использование виртуальной памяти, профиль пользователя, переменные окружения, загрузку и восстановление.

Настройка быстродействия Windows

Множество графических расширений было добавлено в интерфейс Windows Server 2008, все эти изменения доступны и в следующих версиях. Все эти расширения представляют собой множество визуальных эффектов для меню, панелей инструментов, окон и панели задач. Настроить быстродействие Windows можно с помощью следующих действий:

1. Активизируйте вкладку **Дополнительно** (Advanced), а затем нажмите кнопку **Параметры** (Settings) в группе **Быстродействие** (Performance).
2. По умолчанию будет выбрана вкладка **Визуальные эффекты** (Visual Effects) окна **Параметры быстродействия**. Для контроля визуальных эффектов доступны следующие опции.
   - **Пусть Windows выберет, что лучше для моего компьютера** (Let Windows Choose What's Best For My Computer) — операционная система выберет оптимальные настройки быстродействия на основании вашей аппаратной конфигурации. Для новых компьютеров эта опция, возможно, будет идентична выбору **Обеспечить наилучший вид** (Adjust For Best Appearance). Разница заключается в том, что эта опция бу-

дет выбрана операционной системой на основании соответствующих требований к аппаратным возможностям компьютера.

- **Обеспечить наилучший внешний вид** (Adjust For Best Appearance) — включаются все визуальные эффекты для всех графических интерфейсов. Меню и панель задач используют прозрачность и тени. Экранные шрифты обладают гладкими краями, у списков более плавная прокрутка. Папки используют веб-вид и т. д.
- **Обеспечить наилучшее быстродействие** (Adjust For Best Performance) — выключаются все визуальные эффекты, потребляющие много ресурсов, например, прозрачность, тени у шрифтов и т. д.
- **Особые эффекты** (Custom) — можно самостоятельно выбрать необходимые визуальные эффекты. Если отключить все опции, Windows не будет использовать визуальные эффекты.

3. Нажмите кнопку **Применить** (Apply) для завершения изменений визуальных эффектов. Нажмите кнопку **OK** дважды, чтобы закрыть все открытые диалоговые окна.

Настройка быстродействия приложений

Производительность приложений связана с опциями кэширования/планирования процессора, которые устанавливаются администратором для Windows Server 2012. Планирование определяет скорость отклика приложений, которые запускаются интерактивно (в противовес фоновым приложениям, которые должны быть запущены в системе как службы). Контролировать быстродействие приложений можно так:

1. Активизируйте вкладку **Дополнительно** окна **Свойства системы**, затем откройте окно **Параметры быстродействия** (Performance Options), нажав кнопку **Параметры** в группе **Быстродействие**.
2. В окне **Параметры быстродействия** (Performance Options) переключитесь на вкладку **Дополнительно** (Advanced).
3. На панели **Распределение времени процессора** (Processor Scheduling) находятся две опции:
   - **программ** (Programs) — используется, чтобы предоставить активным приложениям наилучшее время отклика и большую часть доступных ресурсов. Этот вариант подойдет для серверов разработки или при использовании Windows Server 2012 как настольной операционной системы;
   - **служб, работающих в фоновом режиме** (Background Services) — используйте эту опцию, чтобы предоставить фоновым приложениям лучшее время отклика, чем у активных приложений. Это оптимальная опция для сервера.
4. Нажмите кнопку **OK**.

Настройка виртуальной памяти

С помощью виртуальной памяти дисковое пространство может использоваться для расширения объема памяти, доступной в системе путем использования жесткого диска как части системной памяти. Эта функция записывает содержимое ОЗУ на диски, используя процесс, называемый *подкачкой*. Подкачка записывает определенный объем ОЗУ, скажем 8192 Мбайт, на диск в файл подкачки. Файл подкачки используется, когда нужно место в физическом ОЗУ.

Начальный файл подкачки создается автоматически для диска, содержащего операционную систему. По умолчанию на других дисках нет файлов подкачки, но при необходимости их можно создать. При создании файла подкачки устанавливается его максимальный размер. Файлы подкачки хранятся в корневом каталоге тома и называются Pagefile.sys.

> ***Практический совет***
>
> Текущие выпуски Windows Server автоматически управляют виртуальной памятью лучше, чем их предшественники. Обычно Windows Server размещает виртуальную память в размере, как минимум, равном объему физической оперативной памяти. Это позволяет убедиться, что файлы подкачки не будут фрагментированы, что в результате отрицательно скажется на быстродействии системы. Если есть необходимость управлять виртуальной памятью вручную, можно использовать фиксированный размер виртуальной памяти. Для этого установите одинаковое значение для исходного и максимального размера оперативной памяти. В результате будет создан файл подкачки постоянного размера (если это возможно, учитывая объем свободного пространства на вашем томе). В большинстве случаев для компьютеров с 8 Гбайт ОЗУ или меньше рекомендуется установить размер файла подкачки, в два раза превышающий объем физического ОЗУ. Например, на компьютере с 8 Гбайт ОЗУ нужно убедиться, что параметр **Общий объем файла подкачки на всех дисках** (Total Paging File Size For All Drives) равен как минимум 16 384 Мбайт. На системах, где более 8 Гбайт оперативной памяти, нужно следовать рекомендациям производителя оборудования для настройки размера файла подкачки. Обычно в этом случае можно установить размер файла подкачки, равный размеру ОЗУ.

Настроить виртуальную память можно так:

1. Активизируйте вкладку **Дополнительно** окна **Свойства системы**, затем откройте окно **Параметры быстродействия**, нажав кнопку **Параметры** в группе **Быстродействие**.
2. В диалоговом окне **Параметры быстродействия** перейдите на вкладку **Дополнительно** и нажмите кнопку **Изменить** (Change) для отображения окна **Виртуальная память** (Virtual Memory) (рис. 2.6). Здесь предоставлена следующая информация.
   - **Размер файла подкачки для каждого диска** (Paging File Size For Each Drive) — предоставляет информацию по выбранному диску и позволяет установить файл подкачки этого диска. Поле **Свободно** (Space Available) показывает, сколько места доступно на диске.
   - **Диск [метка тома] и Размер файла подкачки** (Drive [Volume Label] and Paging File Size) — показывает, как виртуальная память настроена в этой системе. Выводится, существует ли на том или ином томе файл подкачки, и сообщается, каков исходный и максимальный размеры файла подкачки для конкретного тома.
   - **Общий объем файла подкачки на всех дисках** (Total Paging File Size For All Drives) — показывает минимальный, рекомендуемый и текущий размер виртуальной памяти. При первой настройке виртуальной памяти учтите, что рекомендуемый размер уже был назначен системному диску (в большинстве случаев).
3. По умолчанию Windows Server управляет размерами файла подкачки для всех дисков. Если нужно настроить виртуальную память вручную, установите флажок **Автоматически выбирать объем файла подкачки** (Automatically Manage Paging File Size For All Drives).
4. В списке дисков выберите том, с которым планируете работать.
5. Отметьте переключатель **Указать размер** (Custom Size), введите значения в поля **Исходный размер** (Initial Size) и **Максимальный размер** (Maximum Size).
6. Нажмите кнопку **Задать** (Set), чтобы сохранить изменения.
7. Повторите шаги 4—6 для каждого тома, который нужно настроить.

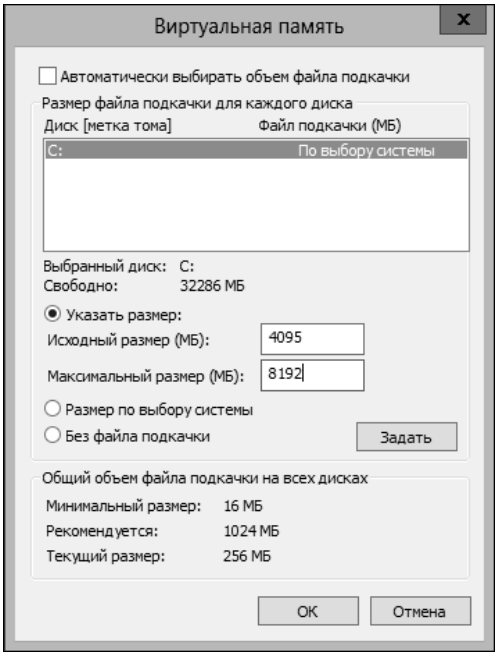


Рис. 2.6. Виртуальная память расширяет объем ОЗУ системы

Примечание

Файл подкачки также используется для отладки при ошибках синего экрана (в английской терминологии stop error). Если размер файла подкачки на системном диске меньше, чем минимальный размер памяти, необходимой для записи отладочной информации, эта функция будет отключена. Если нужно использовать отладку, установите размер файла подкачки равным объему оперативной памяти. Например, если в системе установлено 4 Гбайт ОЗУ, вам нужен файл подкачки размером 4 Гбайт на *системном диске*.

8. Нажмите кнопку **OK**. Если появится запрос, нужно ли перезаписать существующий файл Pagefile.sys, нажмите кнопку **Да** (Yes).
9. Если были обновлены параметры для файла подкачки, который в данный момент используется, будет показано сообщение о необходимости перезагрузки системы. Нажмите кнопку **OK**.
10. Нажмите кнопку **OK** дважды, чтобы закрыть диалоговые окна. После закрытия утилиты **Система** будет предложено перезагрузить систему. Нажмите кнопку **Перезагрузить** (Restart).

Сконфигурировать Windows Server 2012 на автоматическую настройку виртуальной памяти можно так:

1. Активизируйте вкладку **Дополнительно** окна **Свойства системы**, затем откройте окно **Параметры быстродействия**, нажав кнопку **Параметры** в группе **Быстродействие**.
2. Перейдите на вкладку **Дополнительно**, затем нажмите кнопку **Изменить** для отображения диалогового окна **Виртуальная память** (Virtual Memory).
3. Отметьте переключатель **Автоматически выбирать объем файла подкачки** (Automatically Manage Paging File Size For All Drives).
4. Нажмите кнопку **OK** трижды, чтобы закрыть все открытые окна.

Примечание

При обновлении параметров используемого в данный момент файла подкачки будет выведено сообщение о необходимости перезагрузки сервера (чтобы изменения вступили в силу). Нажмите кнопку **OK**. После закрытия окна **Свойства системы** будет предложено перезагрузить систему. На производственном сервере нужно запланировать эту перезагрузку вне рабочего времени.

Настройка предотвращения выполнения данных

Предотвращение выполнения данных (Data Execution Prevention, DEP) — это технология защиты памяти. DEP указывает процессору пометить все ячейки памяти в приложении как невыполнимые, кроме блоков явно содержащих исполняемый код. Если код, выполняемый со страницы памяти, отмечен как невыполняемый, процессор может породить исключительную ситуацию и предотвратить выполнение кода. Это предотвращает выполнение вредоносного кода, например кода вируса.

Примечание

32-битные версии Windows поддерживают DEP, как реализовано процессорами AMD, которые предоставляют защиту невыполняемых страниц (функция NX). Такие процессоры поддерживают связанные инструкции и должны работать в режиме PAE (Physical Address Extension).

Использование и настройка DEP

Определить, поддерживает ли компьютер DEP, можно с помощью утилиты **Система**. Если компьютер поддерживает DEP, ее можно настроить с помощью следующих действий:

1. Активизируйте вкладку **Дополнительно** окна **Свойства системы**, затем откройте окно **Параметры быстродействия**, нажав кнопку **Параметры** в группе **Быстродействие**.
2. В окне **Параметры быстродействия** перейдите на вкладку **Предотвращение выполнения данных** (Data Execution Prevention). Текст внизу этой вкладки указывает, поддерживает ли компьютер защиту выполнения данных.
3. Если компьютер поддерживает DEP, можно настроить DEP следующим образом.
   - **Включить DEP только для основных программ и служб Windows** (Turn On DEP For Essential Windows Programs And Services Only) — включает DEP только для служб, программ и компонентов операционной системы. Это значение является значением по умолчанию и рекомендуемым для компьютеров, которые поддерживают DEP и настроены соответствующим образом.
   - **Включить DEP для всех программ и служб, кроме выбранных ниже** (Turn On DEP For All Programs Except Those I Select) — настраивает DEP для всех программ, кроме указанных в списке. Выберите эту опцию и затем нажмите кнопку **Добавить** (Add), чтобы указать программы, которые должны запускаться без защиты выполнения.
4. Нажмите кнопку **OK**.

Если технология DEP включена и разрешены исключения, добавить программы в список или удалить их из списка исключений можно так:

1. Активизируйте вкладку **Дополнительно** окна **Свойства системы**, затем откройте окно **Параметры быстродействия**, нажав кнопку **Параметры** в группе **Быстродействие**.
2. В окне **Параметры быстродействия** перейдите на вкладку **Предотвращение выполнения данных**.

3. Чтобы добавить программу как исключение, нажмите кнопку **Добавить**. Появится окно **Открыть** (Open), выберите исполняемый файл программ и нажмите кнопку **Открыть**.
4. Для временного удаления программы из списка исключений (например, для решения проблем) отметьте флажок возле имени программы.
5. Для удаления программы из списка исключений щелкните на программе и нажмите кнопку **Удалить** (Remove).
6. Нажмите кнопку **OK** для сохранения изменений.

DEP-совместимость

Чтобы быть совместимыми с DEP, приложения должны уметь явно помечать блок памяти разрешением Execute. Приложения, которые не могут сделать это, несовместимы с функцией процессора NX. Если возникают проблемы, связанные с памятью при запуске приложений, необходимо определить "проблемные" приложения и настроить их как исключения, а не полностью отключать защиту выполнения. Таким образом, все еще можно извлечь пользу от защиты памяти, выборочно отключив защиту для программ, которые не работают должным образом с функцией процессора NX. В этом случае защита памяти будет выключена только для "проблемных" приложений, но будет включена для всех остальных.

Защита DEP применяется и к пользовательским программам, и программам режима ядра. Нарушение защиты выполнения непривилегированного режима (пользовательские программы) приводит к исключению STATUS_ACCESS_VIOLATION. В большинстве процессов это исключение будет необработанным исключением, приводящим к завершению процесса. Большинство программ, нарушающих защиту памяти, будут вредоносны по своей природе — вирус, червь и т. д.

Нельзя выборочно включить или выключить защиту выполнения для драйверов устройств режима ядра (привилегированного режима), как в случае с приложениями. Кроме того, в DEP-совместимых 32-разрядных системах защита выполнения применена по умолчанию к стеку памяти. В DEP-совместимых 64-разрядных системах защита выполнения применена по умолчанию к стеку памяти, пулу подкачиваемой памяти и пулу сеанса. Нарушение прав доступа защиты выполнения привилегированного режима для драйвера устройства приводит к исключению ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY.

Настройка системных и пользовательских переменных среды

Windows использует переменные среды для отслеживания важных строк, например, пути поиска файлов или имени узла контроллера домена. Переменные среды, предназначенные для использования самой системой Windows, называются *системными переменными среды*. Они одинаковы для всех, вне зависимости от того, кто вошел в систему на определенном компьютере. Переменные среды, определенные для применения пользователями или программами, называются *пользовательскими переменными среды*. Они различны для каждого пользователя конкретного компьютера. Настроить системные и пользовательские переменные среды можно с помощью окна **Переменные среды** (Environment Variables), показанного на рис. 2.7. Чтобы получить доступ к этому окну, откройте окно **Свойства системы**, перейдите на вкладку **Дополнительно** и нажмите кнопку **Переменные среды** (Environment Variables).

Создание переменной среды

Для создания переменной среды выполните следующие действия:

1. Нажмите кнопку **Создать** (New) в группе **Переменные среды пользователя** (User Variables) или группе **Системные переменные** (System Variables). Откроется окно **Но-**

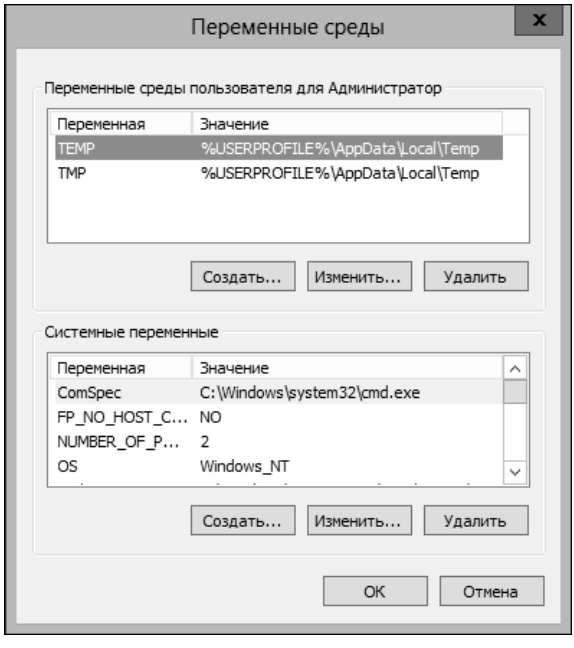


Рис. 2.7. Пользовательские и системные переменные среды в окне **Переменные среды**

вая пользовательская переменная (New User Variable) или **Новая системная переменная** (New System Variable) соответственно.

2. В поле **Имя переменной** (Variable Name) введите имя переменной, а в поле **Значение переменной** (Variable Value) — ее значение.
3. Нажмите кнопку **OK**.

Редактирование переменной среды

Для редактирования значения переменной среды выполните такие действия:

1. Выберите переменную в группе **Переменные среды пользователя** или группе **Системные переменные**.
2. Нажмите кнопку **Изменить** (Edit) в группе **Переменные среды пользователя** или группе **Системные переменные**. Откроется окно **Изменение пользовательской переменной** (Edit User Variable) или **Изменение системной переменной** (Edit System Variable) соответственно.
3. Введите новое значение в поле **Значение переменной** и нажмите кнопку **OK**.

Удаление переменной среды

Для удаления переменной среды выделите ее и нажмите кнопку **Удалить** (Delete).

> ***Примечание***
>
> При создании или изменении переменных среды большинство из них становятся доступными сразу после их создания или изменения. Для некоторых системных переменных изменения вступят в силу после перезапуска компьютера, а для некоторых пользовательских переменных — после следующего входа в систему.

Настройка загрузки и восстановления системы

Настроить параметры загрузки и восстановления системы можно в окне **Загрузка и восстановление** (Startup And Recovery) (рис. 2.8). Чтобы открыть это окно, откройте окно **Свойства системы** и перейдите на вкладку **Дополнительно**, а затем нажмите кнопку **Параметры** в группе **Загрузка и восстановление** (Startup And Recovery).

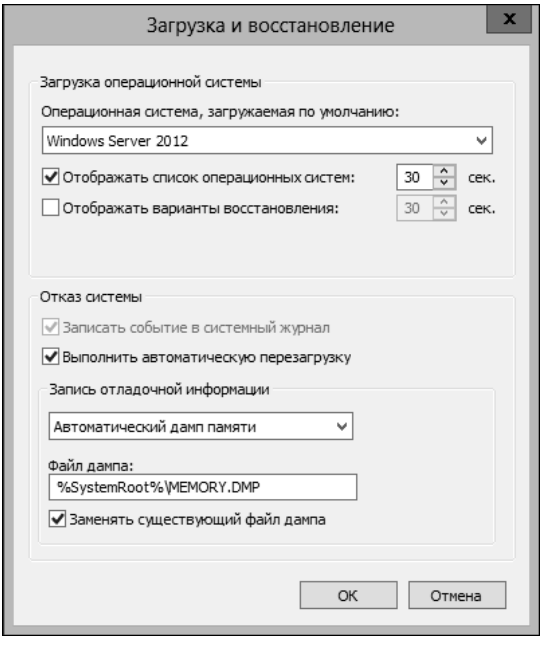


Рис. 2.8. Параметры загрузки и восстановления системы в окне **Загрузка и восстановление**

Установка параметров загрузки

Группа **Загрузка операционной системы** (System Startup) окна **Загрузка и восстановление** контролирует запуск системы. Чтобы выбрать операционную систему по умолчанию для компьютеров с несколькими операционными системами, выберите одну из операционных систем в списке **Операционная система, загружаемая по умолчанию** (Default Operating System). Эти параметры изменяют конфигурационные настройки, используемые менеджером загрузки Windows.

После запуска компьютера с несколькими операционными системами Windows Server отображает меню конфигурации на протяжении 30 секунд (по умолчанию). Изменить это поведение можно так:

- немедленно загрузить операционную систему по умолчанию можно, сбросив флажок **Отображать список операционных систем** (Time To Display List Of Operating Systems);
- отобразить список операционных систем на протяжении указанного времени. Установите флажок **Отображать список операционных систем** и установите время, на протяжении которого система будет отображать список операционных систем.

В большинстве случаев, возможно, устроит значение 3 или 5 секунд. Этого вполне достаточно для выбора операционной системы, и в то же время это значение существенно сокращает время загрузки системы по умолчанию.

Когда система находится в режиме восстановления, при загрузке отображается список вариантов восстановления. Как и в случае со стандартными параметрами загрузки, можно настроить восстановление системы двумя способами. Можно настроить компьютер на немедленную загрузку, используя вариант восстановления по умолчанию, отметив флажок **Отображать варианты восстановления**. Можно указать количество секунд, на протяжении которых будут отображены варианты восстановления.

Определение параметров восстановления

Контролировать восстановление системы можно с помощью областей **Отказ системы** (System Failure) и **Запись отладочной информации** (Write Debugging Information) окна **Загрузка и восстановление**. Администраторы используют опции восстановления для точного контроля, что случится, если система встретится с фатальной ошибкой ("синий экран смерти" или stop error). Доступные варианты:

- **Записать событие в системный журнал** (Write An Event To The System Log) — протоколирует ошибку в системный журнал, позволяя администраторам просмотреть последнюю ошибку с помощью утилиты Просмотр событий (Event Viewer);
- **Выполнить автоматическую перезагрузку** (Automatically Restart) — выберите эту опцию, чтобы перезагрузить систему в случае возникновения фатальной ошибки.

> ***Примечание***
>
> Автоматическая перезагрузка — не всегда удачный метод избавиться от ошибки. В некоторых случаях нужно, чтобы система была остановлена, а не перезагружена, и этим привлекла к себе надлежащее внимание.

Список **Запись отладочной информации** (Write Debugging Information) служит для определения типа отладочной информации, которую необходимо записать в файл дампа. Его можно использовать для диагностики системных сбоев. Доступные варианты:

- **(нет)** (None) — отладочная информация не записывается;
- **Малый дамп памяти** (Small Memory Dump) — малый дамп физической памяти, только того участка, где произошла ошибка. Размер файла — 256 Кбайт;
- **Дамп памяти ядра** (Kernel Memory Dump) — дамп памяти, используемой ядром Windows. Размер файла определяется размером ядра;
- **Полный дамп памяти** (Kernel Memory Dump) — используется для полного дампа всей физической памяти. Размер файла дампа зависит от размера используемой физической памяти и равен максимальному размеру всей физической памяти сервера;
- **Автоматический дамп памяти** (Complete Memory Dump) — разрешите Windows самой выбрать, какой тип дампа лучше, и создать соответствующий файл дампа.

Если определена запись отладочной информации в дамп-файл, также можно выбрать и его расположение. По умолчанию файлы дампа создаются в папке *%SystemRoot%*\Minidump для малых дампов и *%SystemRoot%*\Memory.dmp для всех остальных типов дампов. Обычно можно включить режим **Заменять существующий файл дампа** (Overwrite Any Existing File). В этом случае любой существующий файл дампа будет перезаписан при возникновении новой фатальной ошибки.

> ***Рекомендации***
>
> Можно создать файл дампа, только если система правильно настроена. Системный диск должен иметь большой файл подкачки (параметры виртуальной памяти были описаны ранее в этой главе), а диск, где нужно сохранить файл дампа, должен иметь достаточно сво-

бодного пространства для записи огромного файла дампа. Например, у сервера автора этой книги 8 Гбайт оперативной памяти, он требует такого же объема на диске для хранения файла подкачки — 8 Гбайт. Серверы, как правило, используют 892—1076 Мбайт для памяти ядра. Поскольку этот диск используется и для дампа-файла, на диске должно быть, по крайней мере, 9 Гбайт свободного пространства, чтобы создать дамп отладочной информации (8 Гбайт для файла подкачки и 1 Гбайт для файла дампа).

Вкладка *Удаленный доступ*

Вкладка **Удаленный доступ** (Remote) окна **Свойства системы** контролирует параметры удаленного помощника (Remote Assistance) и удаленного рабочего (Remote Desktop) стола. Эти параметры будут обсуждаться в *главе 4*.

ГЛАВА 3

Мониторинг процессов, служб и событий

Администратору нужно тщательно присматривать за сетевыми системами. Состояние использования системных ресурсов может измениться в любой момент и вовсе не в лучшую сторону. Службы могут перестать работать. В файловых системах может закончиться свободное пространство. Приложения могут порождать исключительные ситуации, что приведет к системным проблемам. Неавторизированные пользователи будут пытаться получить несанкционированный доступ. Методы, рассмотренные в этой главе, помогут идентифицировать и разрешить эти и другие системные проблемы.

Управление приложениями, процессами и производительностью

При запуске приложения или вводе команды в командной строке операционная система Microsoft Windows Server запускает один или более процессов для управления соответствующей программой. Вообще говоря, все процессы, запускаемые таким образом, называются *интерактивными процессами* — ведь пользователь взаимодействует с ними с помощью клавиатуры или мыши. Если приложение (или программа) активно и выбрано, интерактивный процесс контролирует клавиатуру и мышь, пока пользователь не завершит программу или не выберет другую. Если у процесса есть управление, говорят, что он работает в *интерактивном режиме* (foreground).

Процесс может также работать в *фоновом режиме* (background). Для процессов, запущенных пользователем, это означает, что программа в настоящее время не активна, но может продолжить работать, однако ей не предоставляется такой же приоритет, как у активного процесса. Фоновые процессы могут выполняться независимо от пользовательского сеанса; обычно такие процессы запускает сама операционная система. Пример такого фонового процесса — задание планировщика, которое запускает сама операционная система. В этом случае пользователь говорит системе, что ей нужно выполнить команду в указанное время.

Диспетчер задач

Диспетчер задач (Task Manager) — ключевая утилита для управления системными процессами и приложениями. Есть несколько способов открыть диспетчер задач:

- нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc>;
- нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, а затем выберите опцию **Диспетчер задач**;

- нажмите клавишу <Windows>, введите `taskmgr` и нажмите клавишу <Enter>;
- нажмите и удерживайте палец на панели задач (или щелкните правой кнопкой мыши) и выберите команду **Диспетчер задач** из появившегося контекстного меню.

> ***Примечание***
>
> Если нажмете клавишу <Windows> и введете `taskmgr`, то увидите два совпадения. Одно из них — полное название **Диспетчер задач**, а второе — введенная команда `taskmgr`.

В следующих разделах описано, как работать с диспетчером задач.

Просмотр и работа с процессами

У диспетчера задач есть два представления:

- **Сводка** (Summary) — перечисляются только приложения, запущенные в интерактивном режиме, что позволяет быстро выбирать такие приложения;
- **Подробный вид** (Expanded) — расширенное представление, где есть дополнительные вкладки, которые можно использовать для получения информации обо всех запущенных процессах, производительности системы, подключенных пользователях и настроенных службах.

Находясь в первом представлении, переключиться во второе представление можно нажатием кнопки **Подробнее** (More Details). Для переключения со второго представления в первое используется кнопка **Меньше** (Fewer Details). При повторном открытии диспетчера задач он будет находиться в последнем выбранном представлении.

Вообще говоря, администратору положено работать в расширенном представлении. В этом представлении есть несколько вкладок (рис. 3.1), позволяющих работать с запущенными процессами, производительностью системы, подключенными пользователями и настроенными службами. Вкладка **Процессы** (Processes), также показанная на рис. 3.1, показывает общий статус процессов. Процессы группируются по типу и выводятся в алфавитном порядке в пределах каждого типа. Есть три общих типа процессов:

- **Приложения** (Apps) — процессы, запущенные в интерактивном режиме;
- **Фоновые процессы** (Background processes) — процессы, работающие в фоновом режиме;
- **Процессы Windows** (Windows processes) — процессы, запускаемые операционной системой.

> ***Примечание***
>
> В меню **Вид** (View) есть команда **Группировать по типу** (Group By Type), определяющая, будут ли процессы группироваться по типу или выводиться просто в алфавитном порядке. Также заметьте, что можно запустить программу прямо из диспетчера задач. Для этого в меню **Файл** (File) выберите команду **Запустить новую задачу** (Run New Task). В появившемся окне у вас будет возможность выбрать исполняемый файл программы и запустить задачу с правами администратора.

> ***Практический совет***
>
> Многие Windows-процессы также группируются по узлу службы, под управлением которой они работают. Узлы службы могут быть такими: **Локальная служба** (Local Service), **Локальная система** (Local System), **Сетевая служба** (Network Service). В круглых скобках указывается число сгруппированных процессов. Чтобы просмотреть фактические процессы, можно развернуть узел. В меню **Вид** есть команда **Развернуть все** (Expand All) для разворачивания всех групп процессов для более простого просмотра.

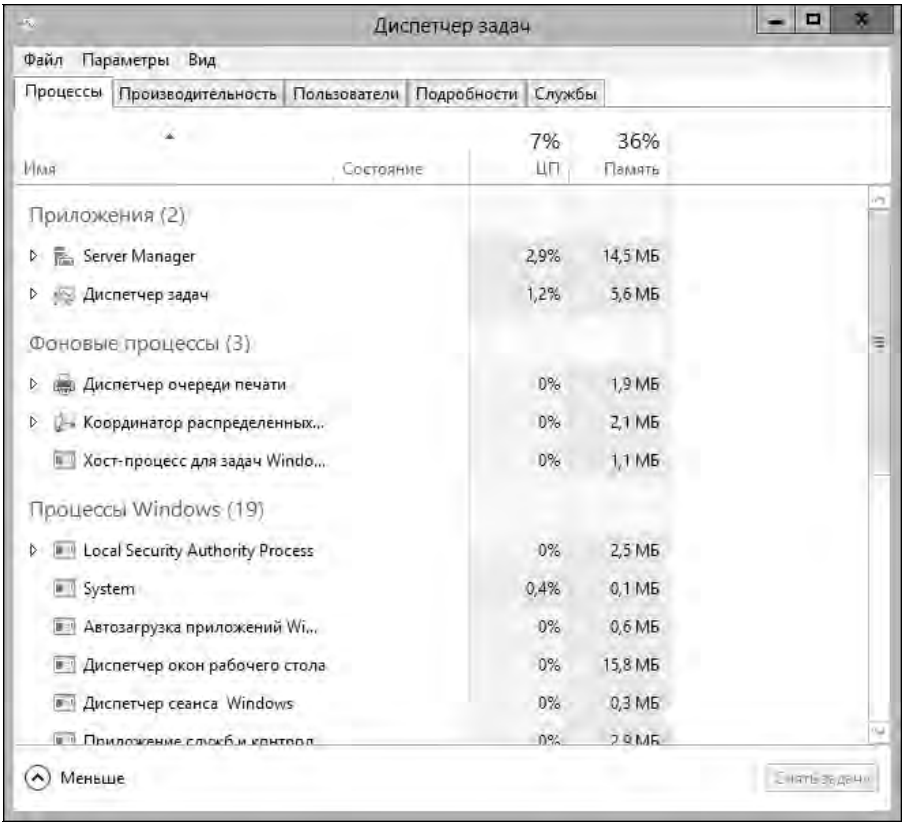


Рис. 3.1. Просмотрите статус процессов, запущенных на сервере

Колонка **Состояние** (Status) показывает, выполняется ли приложение или же остановлено. Если в этой колонке ничего нет, это означает нормальное выполнение процесса. Любое другое значение в этой колонке свидетельствует о наличии какой-то проблемы, например приложение может "зависнуть", и администратору придется завершить соответствующую ему задачу. Однако некоторые приложения могут не отвечать на запросы системы во время интенсивных вычислений. Поэтому перед завершением задачи убедитесь, что приложение действительно зависло.

Для завершения процесса нужно выбрать его и нажать кнопку **Снять задачу** (End Task). Однако не нужно пытаться завершить работу Windows-процессов с помощью этой кнопки. При попытке остановить Windows-процесс или группу Windows-процессов диспетчер задач отобразит окно, показанное на рис. 3.2. Это окно предупреждает, что завершение данного процесса может привести к нестабильной работе системы и даже завершению работы. Чтобы продолжить, нужно установить флажок **Не сохранять данные и завершить работу** (Abandon Unsaved Data And Shut down) и нажать кнопку **Завершить работу** (Shut down). Затем Windows отобразит голубой экран с кодом ошибки. После сбора информации об ошибке Windows будет перезагружена.

Другие колонки вкладки **Процессы** предоставляют дополнительную информацию о выполнении процессов. Эти сведения можно использовать, чтобы определить, какие процессы потребляют больше всех системных ресурсов. По умолчанию на вкладке отображаются только столбцы **ЦП** (CPU) и **Память** (Memory), но добавить дополнительные можно, щелк-

нув правой кнопкой мыши по любому заголовку и затем выбрав нужный столбец из появившегося меню. В дополнение к названию и состоянию, доступны следующие столбцы:

- **ЦП** (CPU) — процент использования процессора текущим процессом (по всем ядрам). Значение в заголовке — общее использование процессора (по всем ядрам) всеми запущенными процессами;
- **Память** (Memory) — общий объем памяти, зарезервированный для процесса. Значение в заголовке столбца — общее использование физической памяти сервером;
- **Командная строка** (Command Line) — полный путь к исполняемому файлу процесса, а также любые переданные при запуске аргументы;
- **ИД процесса** (PID) — числовой идентификатор процесса;
- **Имя процесса** (Process Name) — имя процесса или исполняемого файла процесса;
- **Издатель** (Publisher) — название издателя процесса, например Microsoft Corporation;
- **Тип** (Type) — тип процесса (приложение, фоновый процесс, Windows-процесс). Эта информация полезна, если опция **Группировать по типу** (Group By Type) в меню **Вид** (View) выключена.

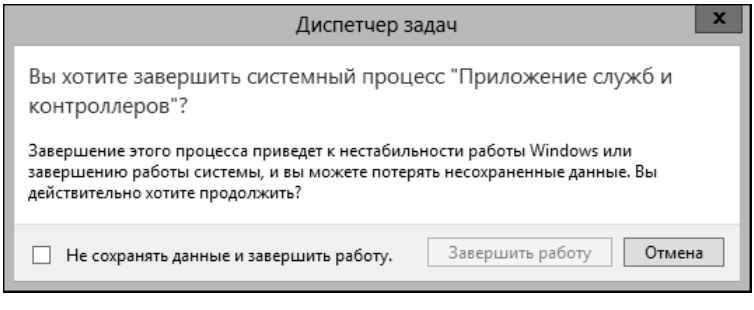


Рис. 3.2. Остановка Windows-процессов может сделать систему нестабильной или привести к завершению ее работы

Щелчок правой кнопкой мыши по процессу отображает контекстное меню действий над ним:

- **Снять задачу** (End Task) — завершает задачу приложения;
- **Создать файл дампа** (Create Dump File) — создает файл дампа для отладки;
- **Подробно** (Go to details) — открывает страницу **Подробности** (Details) и отображает на ней выбранный процесс;
- **Открыть расположение файла** (Open File Location) — открывает папку, в которой находится исполняемый файл процесса;
- **Свойства** (Properties) — открывает окно **Свойства** (Properties) для соответствующего исполняемого файла процесса.

Примечание

Опция **Подробно** очень полезна, когда нужно найти первичный процесс для определенного приложения. После выбора этой опции на вкладке **Подробности** (Details) будет подсвечен именно он.

Администрирование процессов

Вкладка **Подробности** (Details) диспетчера задач (рис. 3.3) предоставляет подробную информацию о запущенных процессах. Столбцы, по умолчанию отображаемые на этой вкладке, подобны тем, которые отображаются на вкладке **Процессы**:

- **Имя** (Name) — имя процесса или исполняемого файла;
- **Состояние** (Status) — состояние процесса;
- **Имя пользователя** (User Name) — имя пользователя;
- **ЦП** (CPU) — использование процессора текущим процессом;
- **Память** (Memory) — использование памяти процессом;
- **Описание** (Description) — описание процесса.

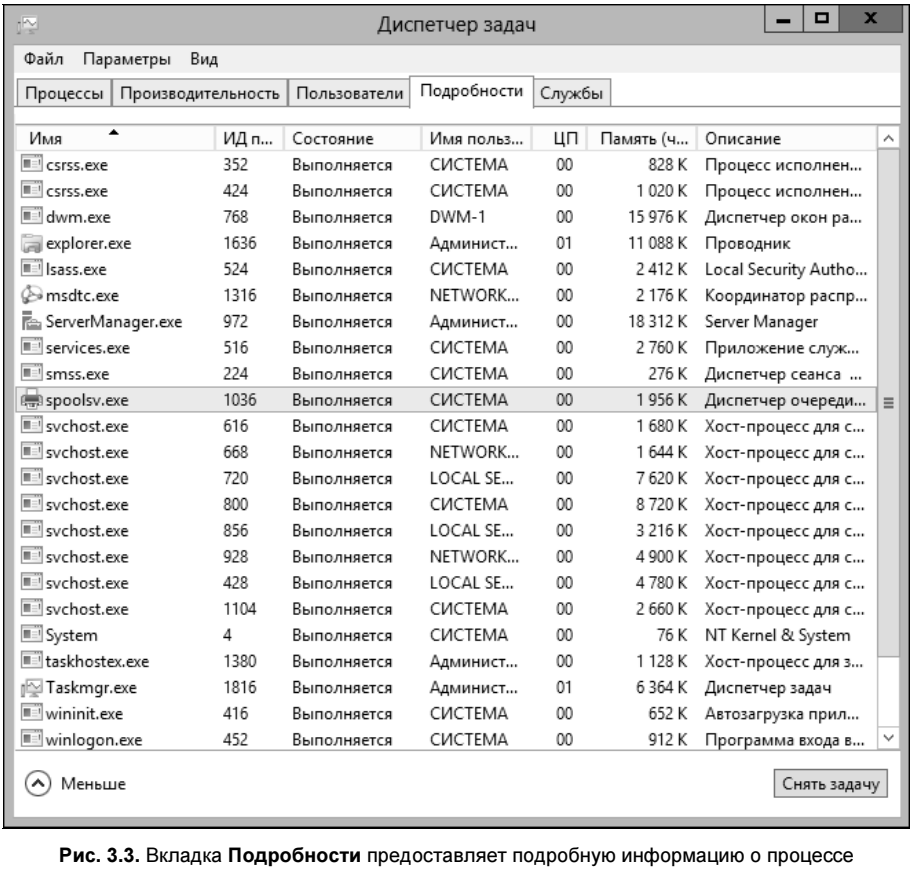


Рис. 3.3. Вкладка **Подробности** предоставляет подробную информацию о процессе

Если щелкнуть правой кнопкой мыши по заголовку любого столбца и выбрать команду **Выбрать столбцы** (Select Columns), можно добавить дополнительные колонки, которые пригодятся при решении системных проблем.

- **Базовый приоритет** (Base Priority) — определяет, сколько системных ресурсов будет выделено процессу. Для установки приоритета щелкните правой кнопкой мыши по процессу и выберите команду **Задать приоритет** (Set Priority). Затем выберите приоритет:

Низкий (Low), **Ниже среднего** (Below Normal), **Обычный** (Normal), **Выше среднего** (Above Normal), **Высокий** (High), **Реального времени** (Realtime). Большинство процессов выполняется с обычным приоритетом. Наивысший приоритет у процессов реального времени.

- **Время ЦП** (CPU Time) — общее процессорное время, использованное процессом с момента его запуска. Чтобы просмотреть процессы, использующие больше всего процессорного времени, отобразите эту колонку и щелкните на ее заголовке для сортировки записей по процессорному времени.
- **Предотвращение выполнения данных** (Data Execution Protection) — показывает, включена ли функциональность DEP для этого процесса.
- **С более высоким уровнем разрешений** (Elevated) — показывает, выполняется ли процесс с правами администратора.
- **Дескрипторы** (Handles) — общее число дескрипторов, связанных с процессом. Используйте число дескрипторов, чтобы определить, сколько файлов открыл процесс. У некоторых процессов, таких как Microsoft Internet Information Services (IIS), есть тысячи открытых дескрипторов файлов. Каждый дескриптор требует системную память.
- **Операций чтения** (I/O Reads), **Операций записи** (I/O Writes) — общее число операций дискового ввода/вывода (I/O) с момента запуска проекта. Общее число операций чтения и записи говорит о том, как активно процесс использует диск. Если число операций чтения/записи растет непропорционально фактической активности сервера, процесс может не использовать кэширование файлов или же кэширование не настроено должным образом. В идеале кэширование сокращает потребность в операциях ввода/вывода.
- **Ошибки страницы** (Page Faults) — ошибки страниц возникают, когда процесс запрашивает страницу в памяти, которую система не может найти в запрашиваемом месте. Если страница находится где-то в памяти, ошибка называется *мягкой*. Если же запрашиваемая страница находится на диске, ошибка называется *жесткой*. Большинство процессоров может обработать огромное число мягких ошибок. Жесткие ошибки вызывают существенные задержки.
- **Выгружаемый пул, невыгружаемый пул** (Paged Pool, NP Pool) — выгружаемый пул — область системной памяти для объектов, которые могут быть записаны на диск, если они не используются. Невыгружаемый пул — область системной памяти для объектов, которые не могут быть записаны на диск. Отметьте процессы, требующие большого объема невыгружаемой памяти. Если недостаточно свободной памяти на сервере, эти процессы могут стать причиной большого количества ошибок страниц.
- **Пиковый рабочий набор** (Peak Working Set) — наибольшее количество памяти, используемой процессом. Разница, или дельта, между текущим использованием памяти и пиковым значением также важна. Приложения с большой дельтой между использованием базовой памяти и пиковым рабочим набором, как например Microsoft SQL Server, нуждаются в выделении большего объема памяти при запуске — так они будут лучше работать.
- **Платформа** (Platform) — платформа, для которой предназначен процесс (32- или 64-битные). 64-разрядные версии Windows могут выполнять 64- и 32-разрядные приложения, используя уровень эмуляции WoW64 (Windows on Windows 64) *x*86. Подсистема WoW64 изолирует 32-разрядные приложения от 64-разрядных. Это позволяет избежать проблем с файловой системой и реестром. Операционная система обеспечивает функциональную совместимость по границе 32/64 для COM (Component Object Model) и для

базовых операций. Однако 32-битный процесс не может загрузить 64-битную DLL-библиотеку, а 64-битный процесс не может загрузить 32-битную DLL-библиотеку.

- **ИД процесса** (PID) — числовой идентификатор процесса.
- **ИД сеанса** (Session ID) — идентификатор сеанса, в котором запущен процесс.
- **Потоки** (Threads) — текущее число потоков, используемых процессом. Большинство серверных приложений являются многопотоковыми. Многопоточность допускает параллельное выполнение запросов процесса. Некоторые приложения могут динамически управлять числом параллельно выполняющихся потоков для улучшения производительности приложения. Однако слишком много потоков может фактически уменьшить производительность, поскольку операционная система должна слишком часто переключать контексты потока.
- **Виртуализация UAC** (UAC Virtualization) — показывает, включена ли виртуализация контроля учетных записей (User Account Control, UAC). Виртуализация может быть включена, выключена или не поддерживаться процессом. Виртуализация необходима для старых приложений, написанных для Windows XP, Windows Server 2003 и более ранних версий Windows. Когда виртуализация контроля учетных записей включена, уведомления об ошибках и протоколирование ошибок, связанных с виртуализированными файлами и значениями реестра, будут записаны в виртуализированное расположение, а не в фактическое, в которое процесс пытался записать. Если виртуализация выключена или не поддерживается, при попытке записать данные в защищенные папки или области реестра, процесс прекратит свою работу.

В списке диспетчера задач есть специальный процесс — **Бездействие системы** (System Idle Process). Нельзя установить приоритет для этого процесса. В отличие от других процессов, для этого процесса выводится количество свободных ресурсов (которые не используются). Так, 99% в колонке **ЦП** (CPU) для бездействия системы означает, что система практически не используется.

Процессы, ожидающие освобождения ресурса, заблокированного другим процессом, находятся в состоянии ожидания и смогут продолжить свою работу только после того, как требуемый ресурс освобожден. Как часть нормального функционирования, ресурсы блокируются, когда они используются одним процессом и могут быть использованы другим только после их освобождения. Однако с плохо спроектированными программами происходит неприятная ситуация, когда ресурс никогда не освобождается.

Просмотреть цепочку ожидания можно, щелкнув по процессу правой кнопкой мыши и выбрав команду **Анализировать цепочку ожидания** (Analyze Wait Chain). Если процесс ожидает освобождения ресурса, будет показана цепочка для этого процесса, в противном случае будет показано сообщение, что процесс работает нормально (рис. 3.4). Корневым узлом в дереве ожидания является процесс, использующий или ожидающий использования, требуемый ресурс. Процесс ожидания может объяснить, почему процесс не реагирует быстро, как от него этого ожидают.

При подозрении проблемы блокировки можно выбрать один или более процессов в цепочке блокировки и затем нажать кнопку **Завершить процесс** (End Process). Диспетчер задач остановит процессы, что должно освободить заблокированный ресурс. Имейте в виду, что блокирование и освобождение процессов — это нормальный рабочий метод: ресурсы блокируются на время использования и освобождаются, когда они не нужны. Проблемы случаются с плохо спроектированными программами, когда процесс "забывает" освободить ресурс.

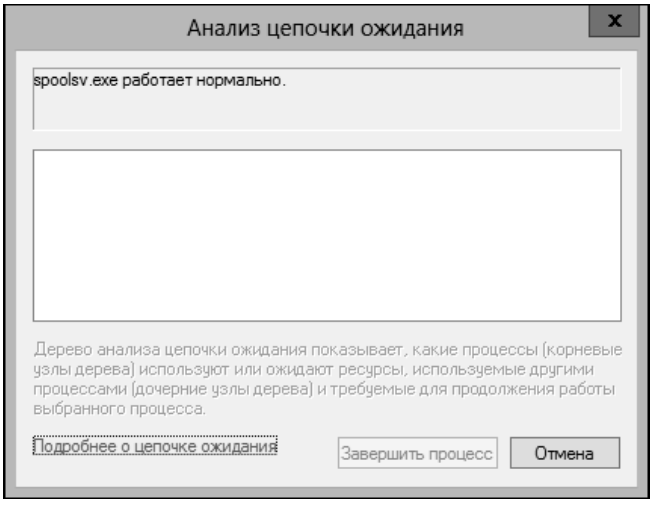


Рис. 3.4. Анализ цепочки ожидания

Помните, что одно приложение может запускать несколько процессов. Эти процессы зависимы от центрального процесса. Начиная с этого главного процесса, формируется дерево процесса, состоящее из зависимых процессов. Найти главный процесс приложения можно, щелкнув на нем правой кнопкой мыши на вкладке **Процессы** и выбрав команду **Подробно**. При завершении приложения нужно завершить основной процесс приложения, а не зависимые процессы. Это гарантирует, что приложение будет корректно остановлено.

Чтобы закрыть основной процесс приложения и все зависимые процессы, можно выполнить одно из следующих действий:

- находясь на вкладке **Процессы**, щелкните на приложении правой кнопкой мыши и выберите команду **Снять задачу** (End Task);
- находясь на вкладке **Подробности**, щелкните правой кнопкой мыши на главном процессе приложения и выберите команду **Снять задачу**;
- находясь на вкладке **Подробности**, щелкните правой кнопкой мыши на главном или зависимом процессе и выберите команду **Завершить дерево процессов** (End Process Tree).

Просмотр системных служб

Вкладка **Службы** (Services) диспетчера задач предоставляет обзор системных служб. Вкладка отображает имя службы, ИД процесса, описание, состояние и группу службы. У нескольких служб может быть один и тот же ИД процесса (рис. 3.5). Можно быстро отсортировать службы по их ИД процесса, щелкнув по соответствующему заголовку. Аналогично можно отсортировать службы по их состоянию — **Выполняется** (Running) или **Остановлено** (Stopped).

Колонка **Группа** (Group) предоставляет дополнительную информацию о контекстах узла службы, под которым выполняется служба.

- Для служб, работающих с ограничениями, эти ограничения указываются в колонке **Группа**. Например, если для локальной службы в колонке указано **LocalServiceNoNetwork**, это означает, что у службы нет доступа к сети; также может быть указано **LocalServiceNetworkRestricted**, т. е. у службы ограниченный доступ к сети.

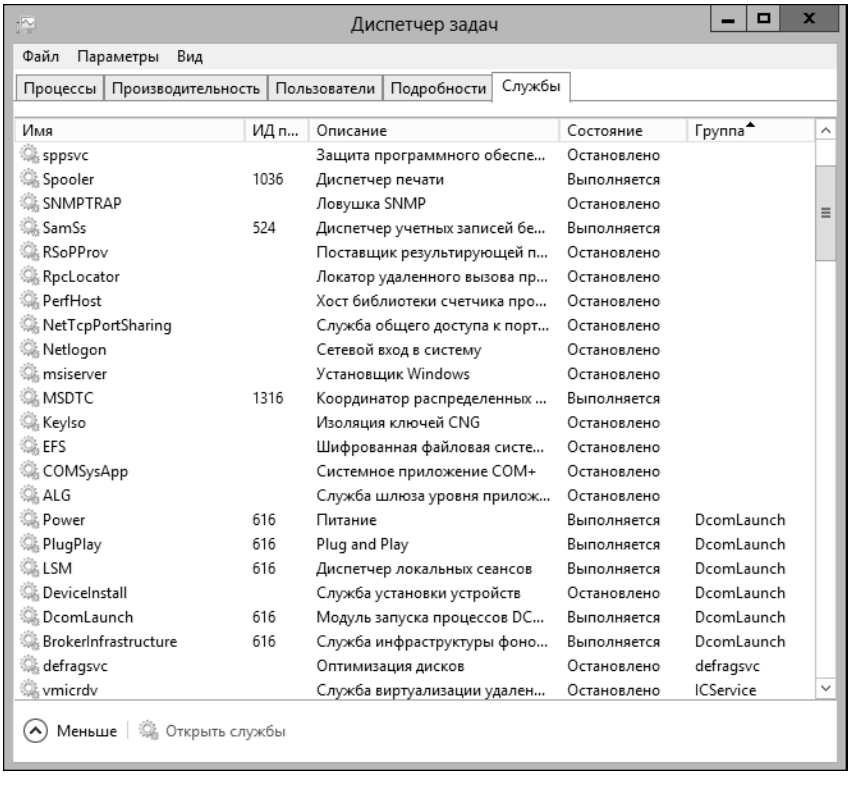


Рис. 3.5. Вкладка **Службы** предоставляет быстрый обзор состояния системных служб

- Некоторые службы выполняются через Svchost.exe (параметр `-k`). Например, служба **RemoteRegistry** запускается командой `svchost.exe -k regsvc`. В колонке **Группа** для нее будет значение **regsvc**.

Если щелкнуть правой кнопкой мыши (или нажать и удерживать палец) по службе, появится контекстное меню, позволяющее выполнить следующие операции над службой:

- запустить остановленную службу;
- остановить работающую службу;
- перейти к процессу службы на вкладку **Подробности**.

Просмотр и управление производительностью системы

Вкладка **Производительность** (Performance) предоставляет общую информацию об использовании ЦП и памяти и отображает графики и статистику (рис. 3.6). Эта вкладка позволяет быстро получить данные об использовании системных ресурсов. Для более подробной информации нужно использовать Монитор ресурсов (Performance Monitor), но о нем мы поговорим чуть позже в этой главе.

Графики на вкладке **Производительность** предоставляют следующую информацию:

- **ЦП** (CPU) — график использования ЦП в разрезе времени;
- **Память** (Memory) — график использования памяти в разрезе времени;
- **Ethernet** — график использования сети в разрезе времени.

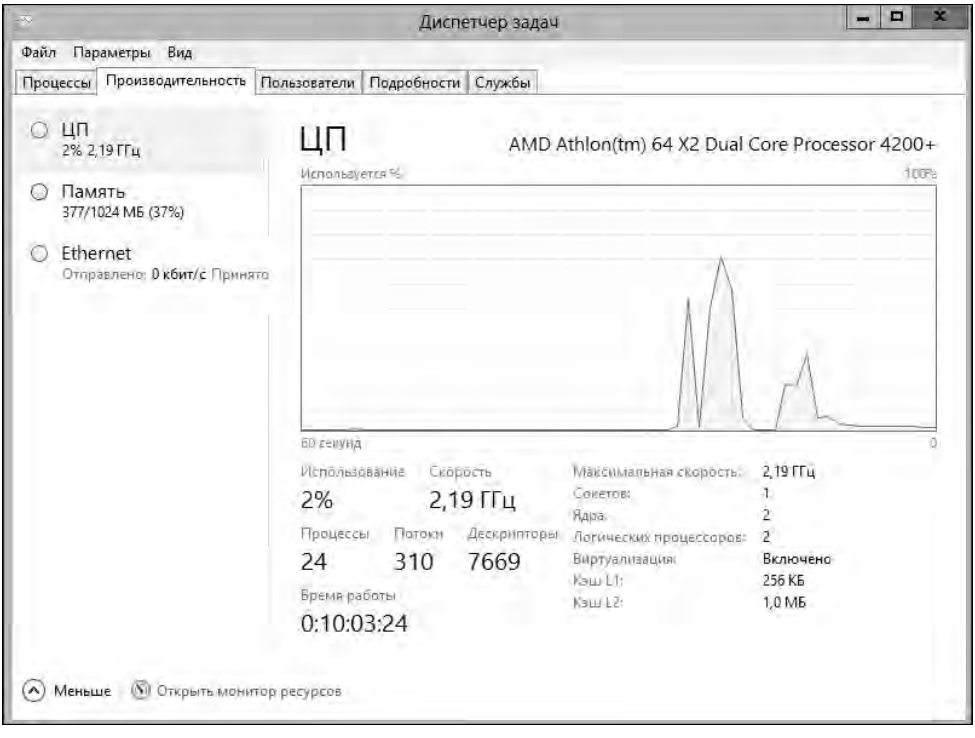


Рис. 3.6. Вкладка **Производительность** предоставляет информацию об использовании системных ресурсов

Для просмотра подробной информации в области справа щелкните по сводному графику на левой панели вкладки. Чтобы увидеть крупный план любого графика, дважды щелкните по нему. Повторный двойной щелчок возвращает прежний режим просмотра.

В меню **Вид** (View) есть команда **Скорость обновления** (Update Speed), позволяющая изменять скорость обновления графика. При низкой скорости график обновляется каждые 4 секунды, 2 секунды при обычной скорости и дважды в секунду при высокой скорости.

Использование центрального процессора

При выборе режима **ЦП** график **Используется %** (% Utilization) показывает общее использование процессора за последние 10 секунд. Если у системы есть несколько процессоров, то для каждого из них выводится отдельный график. Также можно просмотреть логические процессоры или NUMA-узлы, щелкнув правой кнопкой мыши и выбрав команду **Изменить график** (Change Graph To), а затем выбрав опцию **Логические процессоры** (Logical Processors) или **NUMA-узлы** (NUMA Nodes).

Чтобы просмотреть время ядра, щелкните правой кнопкой мыши на графике **ЦП** и выберите команду **Показать время ядра** (Show Kernel Times). Поскольку использование ядра графически изображено отдельно, можно легко отследить количество процессорного времени, которое используется ядром операционной системы.

Совет

Отслеживание времени ядра может быть полезно при решении проблем. Например, если используется IIS с кэшированием вывода в режиме ядра, просмотрев время ядра, можно

лучше понять, как кэширование ядра может повлиять на использование центрального процессора и общую производительность системы. Отслеживание времени ядра не включено по умолчанию, поскольку оно требует дополнительных системных ресурсов.

Информацию с графика **ЦП** можно использовать для быстрого определения времени работы сервера (с момента запуска), числа физических процессоров, числа логических процессоров, кэша процессора (L1, L2, L3), а также определения, включена ли аппаратная виртуализация.

- **Дескрипторы** (Handles) — показывает число используемых дескрипторов ввода-вывода, которые действуют как токены, позволяющие программам получать доступ к ресурсам. Пропускная способность ввода-вывода и производительность дисковой подсистемы влияют на систему больше, чем высокое число дескрипторов ввода-вывода.
- **Потоки** (Threads) — показывает число используемых потоков, поток — базовая единица выполнения в пределах процесса.
- **Процессы** (Processes) — показывает число используемых процессов. Процессы — это запущенные экземпляры исполнимых файлов программы.
- **Время работы** (Up Time) — показывает, как долго система работает с последнего запуска.

Если использование процессора постоянно высокое, необходимо произвести детальный мониторинг производительности для определения источника проблемы. Память — частый источник проблем производительности и нужно помнить об этом перед апгрейдом/добавлением ЦП. Подробно проблемы производительности рассмотрены в *разд. "Тюнинг быстродействия системы" далее в этой главе.*

Использование памяти

При выборе режима **Память** (Memory) график **Использование памяти** (Memory Usage) покажет общее использование частного рабочего набора за последние 60 секунд. Гистограмма **Структура памяти** (Memory Composition) показывает следующее:

- **Используется** (In-Use Memory) — объем памяти, используемый процессами;
- **Изменено** (Modified Memory) — память, содержимое которой необходимо записать на диск, прежде чем использовать ее в других целях;
- **Зарезервировано** (Standby Memory) — память, содержащая кэшированные данные и код, которые сейчас не используются;
- **Свободно** (Free Memory) — память, которая сейчас не используется ни для каких целей.

> ***Примечание***
>
> Учитывать информацию о памяти можно для быстрого определения скорости памяти, числа слотов памяти и используемого форм-фактора памяти.

Общий объем физической памяти сервера выводится в правом верхнем углу при работе с графиком памяти. Снизу под графиком выводится следующая информация:

- **Используется** (In Use) — показывает, сколько физической памяти используется;
- **Доступно** (Available) — показывает объем физического ОЗУ, доступный для использования (включает память, помеченную как "зарезервировано" и "свободно"). Если у сервера небольшой объем физической памяти, необходимо добавить память в систему. В общем, должно быть не менее 5% свободной физической памяти на сервере;

- **Выделено** (Committed) — показывает виртуальную память, используемую в данный момент, и общий объем виртуальной памяти. Если первое значение всего лишь на 10% меньше второго (общий объем), тогда нужно добавить физическую память и/или добавить виртуальную память (увеличить файл подкачки);
- **Кэшировано** (Cached) — показывает объем памяти, используемой для системного кэша;
- **Выгружаемый пул** (Paged Pool) — предоставляет информацию о некритической памяти ядра, которая используется ядром ОС;
- **Невыгружаемый пул** (Nonpaged Pool) — предоставляет информацию по критической памяти ядра, которая используется ядром ОС.

Критические части памяти ядра должны работать в ОЗУ и не могут быть помещены в виртуальную память. Из-за этого данный тип памяти относится к невыгружаемому пулу. Остальная часть памяти ядра может быть разбита на страницы виртуальной памяти и относится к выгружаемому пулу.

Использование сети

При выборе режима **Ethernet** диспетчер задач отобразит общую информацию об использовании сетевых адаптеров системы. Можно учитывать эти сведения для быстрого определения процента использования, скорости соединения и операционного статуса использования каждого сетевого адаптера, настроенного в системе.

Имя активного сетевого адаптера отображается в правом верхнем углу. Если в системе есть всего один сетевой адаптер, график показывает информацию об использовании только этого сетевого адаптера. Если у системы есть несколько сетевых адаптеров, график выводит общую информацию по всем сетевым соединениям, обо всем сетевом трафике.

Если щелкнуть правой кнопкой мыши по графику и выбрать команду **Просмотреть сведения о сети** (View Network Details), можно просмотреть информацию о скорости соединения, состоянии связи, количестве отправленной и полученной информации и другую полезную информацию:

- **Использование сети** (Network Utilization) — процент использования сети, основан на начальной скорости соединения для интерфейса или скорости объединенных интерфейсов. Например, если начальная скорость адаптера равна 10 Гбит/с, а трафик составляет 100 Мбит/с, то использован 1%;
- **Скорость линии** (Link Speed) — начальная скорость интерфейса, например, 1 Гбит/с или 10 Гбит/с;
- **Состояние** (State) — статус сетевых адаптеров, например, **Подключено** или **Отключено**;
- **Пропускная способность отправки** (Bytes Sent Throughput) — процент текущей пропускной способности, используемой для отправки трафика;
- **Пропускная способность получения** (Bytes Received Throughput) — процент текущей пропускной способности, используемой для получения трафика;
- **Общая пропускная способность** (Bytes Throughput) — процент текущей пропускной способности, используемой для всего трафика сетевого адаптера;
- **Отправлено байт** (Bytes Sent) — общее число отправленных байтов;
- **Получено байт** (Bytes Received) — общее число принятых байтов.

Практический совет

Если сетевая нагрузка равна 50% и при этом постоянна, необходимо начать мониторинг сервера, чтобы понять, что вызвало такую нагрузку. Вполне возможно, придется рассмотреть добавление сетевых адаптеров. Любую модернизацию нужно тщательно спланировать. Подумайте о последствиях не только для сервера, но и для сети в целом. Также можно ожидать проблем со связью, если сервер превысил выделенную провайдером пропускную способность. Часто могут потребоваться месяцы, чтобы получить дополнительную пропускную способность для внешних соединений.

Просмотр и управление удаленными сеансами пользователей

Удаленные пользователи могут использовать удаленный рабочий стол (Remote Desktop) для подключения к удаленным системам. Удаленный рабочий стол позволяет администрировать системы удаленно, как будто это локальные системы. Операционная система Windows Server 2012 поддерживает два активных одновременных сеанса.

Один из способов контролировать подключения удаленного рабочего стола заключается в использовании диспетчера задач. Откройте диспетчер задач и перейдите на вкладку **Пользователи** (Users) (рис. 3.7). Данная вкладка показывает интерактивные сеансы пользователей (как локальные, так и удаленные).

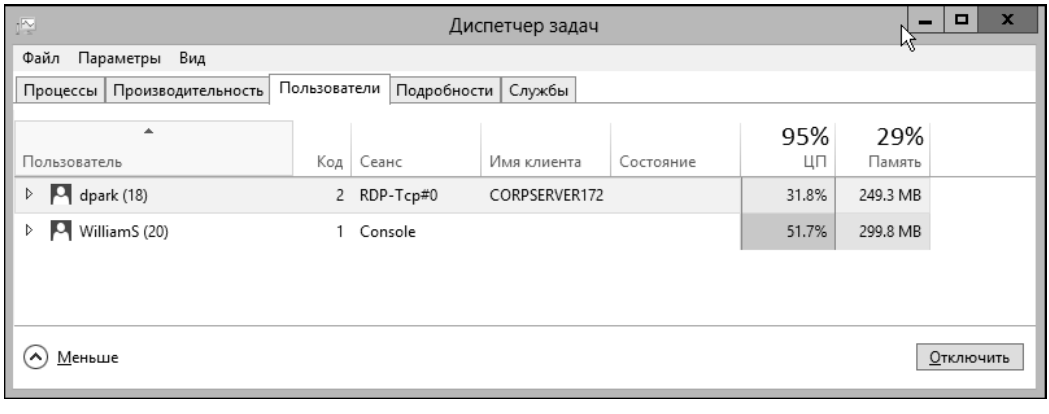


Рис. 3.7. Вкладка **Пользователи** позволяет просматривать и управлять сеансами пользователей

Для каждого сеанса пользователя по умолчанию выводится имя пользователя, статус, загрузка ЦП, использование памяти. Другие колонки можно добавить с помощью правого щелчка мышью по заголовку и выбора нужной колонки. Доступны следующие варианты:

- **Код** (ID) — идентификатор сессии. У первого входа в систему код 1, у второго — 2;
- **Сеанс** (Session) — тип сеанса. У пользователя, зарегистрировавшегося в системе локально, будет тип **Console**. В других случаях выводится тип соединения и используемый протокол, например, RDP-TCP для Remote Desktop Protocol (RDP) и TCP в качестве транспортного протокола;
- **Имя клиента** (Client name) — для удаленных соединений здесь выводится имя компьютера клиента;
- **ЦП** (CPU) и **Память** (Memory) — новые колонки для Windows Server 2012, и они действительно пригодятся при решении проблем производительности, связанных с зарегист-

рированными в системе пользователями. Общий процент использования по всем пользователям приводится в заголовке таблицы. Из рис. 3.7 видно, что загрузка ЦП составляет 95% по всем зарегистрированным пользователям. Высокий уровень загрузки сказывается на общей производительности сервера и на его времени отклика при обработке других задач.

Если щелкнуть правой кнопкой мыши на сеансе пользователя, появится контекстное меню со следующими командами:

- **Подключить** (Connect) — позволяет подключиться к сеансу удаленного пользователя, если он неактивен;
- **Отключить** (Disconnect) — позволяет отключить сеанс удаленного или локального пользователя и завершить все запущенные пользователем приложения без сохранения данных;
- **Выход из системы** (Sign Off) — позволяет осуществить нормальный процесс выхода из системы. Приложения будут закрыты с сохранением данных так, если бы пользователь выполнил нормальный выход из системы;
- **Отправить сообщение** (Send Message) — позволяет отправить консольное сообщение зарегистрированному пользователю.

Есть еще одно новшество для Windows Server 2012: в скобках возле имени пользователя выводится число процессов, запущенных этим пользователем. Дважды щелкните по имени пользователя, чтобы увидеть каждый запущенный процесс. Выводится имя процесса, использование центрального процессора и памяти.

Управление системными службами

Службы предоставляют ключевую функциональность рабочим станциям и серверам. Для управления системными службами можно использовать панель **Службы** (Services) в диспетчере серверов или узел **Службы** (Services) в оснастке **Управление компьютером** (Computer Management). Для работы со службами на удаленных серверах должны быть включены удаленное управление и входящие исключения для приложения **Удаленное управление Windows** (в настройках брандмауэра). Более детальная информация по этой теме представлена в *главе 2*.

Навигация по службам в диспетчере серверов

Если при работе с диспетчером серверов выбрать узел **Локальный сервер** (Local Server), **Все серверы** (All Servers) или узел группы серверов, в области справа будет панель **СЛУЖБЫ** (SERVICES), как показано на рис. 3.8. Если выбрать сервер, панель **СЛУЖБЫ** отобразит запущенные на этом сервере службы. Использовать эту панель можно так:

- для локальных серверов можно использовать панель **СЛУЖБЫ** в узле **Локальный сервер**;
- для удаленных серверов или локального сервера можно использовать панель **СЛУЖБЫ** в узле **Все серверы**, чтобы работать со службами;
- автоматически создаваемые группы серверов организованы по ролям серверов, например, **Доменные службы Active Directory (AD DS)** или **DNS-сервер** (Domain Name System). Управлять службами на сервере можно в зависимости от ролей;

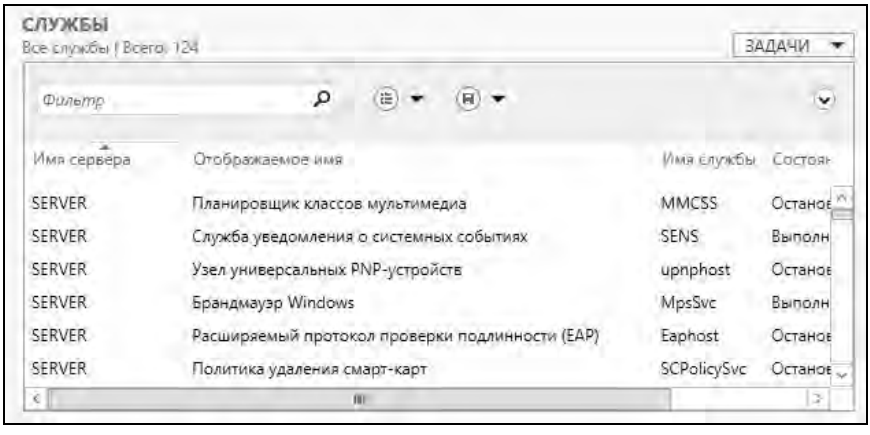


Рис. 3.8. Используйте панель **СЛУЖБЫ** в диспетчере серверов для управления службами на локальных и удаленных серверах

- для пользовательских групп, созданных администраторами, можно использовать панель **СЛУЖБЫ** в целях управления сервисами на любых удаленных серверах, добавленных в группу.

Добавить колонки панели **СЛУЖБЫ** можно с помощью щелчка правой кнопкой мыши (или жеста нажатия и удерживания на сенсорном экране), после этого можно добавить или удалить следующие колонки:

- **Имя сервера** (Server Name) — имя сервера, на котором запущена служба;
- **Полное имя сервера** (FQDN) — полное доменное имя сервера, на котором запущена служба;
- **Отображаемое имя** (Display Name) — отображаемое имя службы, используется для лучшего восприятия службы;
- **Имя службы** (Service Name) — внутреннее название службы;
- **Описание** (Description) — краткое описание назначения службы;
- **Состояние** (Status) — состояние службы (может быть **Выполняется** (Running), **Приостановлена** (Paused), **Остановлена** (Stopped));
- **Тип запуска** (Start Type) — тип запуска службы. Службы с автоматическим запуском загружаются при загрузке системы. Пользователи или другие службы могут запускать службы с типом запуска **Вручную** (Manual). Отключенные службы не могут быть запущены, пока их статус — **Отключена** (Disabled).

> ***Совет***
>
> При работе с множеством серверов используйте опции группировки служб для более простого управления службами. Можно сгруппировать службы по имени сервера, полному имени сервера, состоянию, типу запуска. Для этого щелкните правой кнопкой мыши по колонке заголовка и выберите команду **Группировать по** (Group By).

Навигация по службам в консоли *Управление компьютером*

Для быстрого и простого управления любой службой на удаленном сервере можно использовать узел **Службы** (Services) в оснастке **Управление компьютером** (Computer Manage-

ment). Открыть оснастку **Управление компьютером** и автоматически подключиться к удаленному серверу можно из диспетчера серверов. Для этого выполните следующие действия:

1. Выберите **Все серверы** или любую группу серверов на панели слева.
2. На панели **СЕРВЕРЫ** щелкните правой кнопкой мыши по серверу, к которому нужно подключиться.
3. Выберите команду **Управление компьютером** (Computer Management).

> ***Совет***
>
> При работе с удаленными серверами в оснастке **Управление компьютером** много функций относится к удаленному управлению, и для их работы должны быть включены соответствующие исключения брандмауэра, как было отмечено в *главе 2*. Если у используемой учетной записи пользователя не будет надлежащих прав, чтобы работать с удаленным сервером, подключиться к серверу в оснастке **Управление компьютером** не получится. Чтобы использовать альтернативные учетные данные, щелкните правой кнопкой мыши по серверу и выберите команду **Управлять как** (Manage As), введите альтернативные учетные данные и нажмите кнопку **OK**. Дополнительно можно выбрать флажок **Запомнить мои учетные данные** (Remember My Credentials) перед нажатием кнопки **OK**, чтобы сохранить учетные данные и не вводить их при каждом входе на удаленный сервер. После установки своих учетных данных щелкните правой кнопкой мыши по серверу и выберите команду **Управление компьютером**. Теперь оснастка **Управление компьютером** будет открыта с использованием предоставленных учетных данных.

При работе с оснасткой **Управление компьютером** можно управлять службами, развернув узел **Службы и приложения** (Services And Applications) и выбрав элемент **Службы** (Services), как показано на рис. 3.9. Колонки панели **СЛУЖБЫ** немного отличаются от имеющихся в элементе **Службы** оснастки **Управление компьютером**:

- **Имя** (Name) — имя службы. Здесь приводятся только службы, которые устанавливаются в системе. Двойной щелчок по имени службы позволит настроить параметры загрузки.

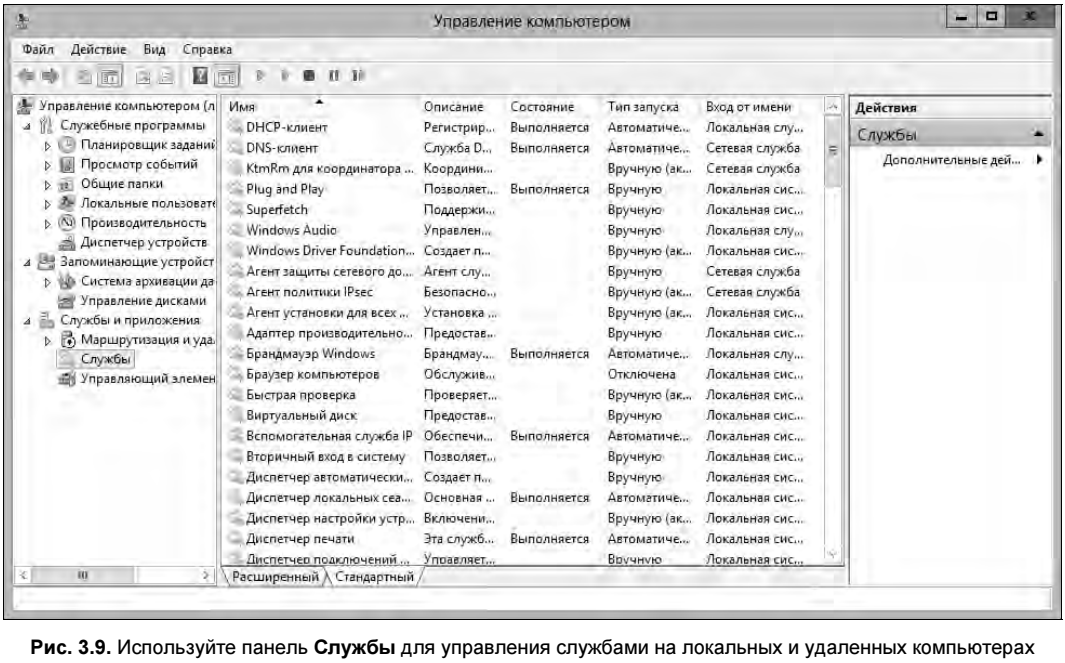


Рис. 3.9. Используйте панель **Службы** для управления службами на локальных и удаленных компьютерах

Если нужной службы здесь нет, ее можно установить путем инсталляции соответствующей роли или компонента *(см. главу 2)*;

- **Описание** (Description) — короткое описание сервиса и его назначения;
- **Состояние** (Status) — показывает статус службы (может быть **Выполняется** (Running), **Приостановлена** (Paused), **Остановлена** (Stopped));
- **Тип запуска** (Startup Type) — тип запуска службы. Службы с автоматическим запуском загружаются при загрузке системы. Пользователи или другие службы могут запускать службы с типом запуска **Вручную** (Manual). Отключенные службы не могут быть запущены, пока у них статус **Отключена** (Disabled);
- **Вход от имени** (Log On As) — учетная запись, от имени которой работает служба. В большинстве случаев служба запускается от имени **Локальная система** (Local System).

У панели **Службы** есть два представления — **Расширенный** (Extended) и **Стандартный** (Standard). Для изменения представления просто используйте вкладки внизу панели **Службы** (Services). В режиме **Расширенный** предоставляются быстрые ссылки на управление службами: ссылка **Запустить** (Start) служит для запуска остановленной службы. Ссылка **Перезапустить** (Restart) останавливает и запускает службу заново — осуществляет перезапуск службы. При выборе службы ее описание выводится на панели слева (при активном расширенном представлении).

> ***Примечание***
>
> Отключить службу могут и пользователь, и операционная система. Windows Server 2012 отключает службы, если возможен конфликт с другими службами.

Запуск, остановка и приостановка служб

Администратору приходится часто запускать, останавливать или приостанавливать службы. Для запуска, остановки или приостановки службы щелкните по ее имени правой кнопкой мыши и выберите команду **Запустить** (Start), **Остановить** (Stop), **Приостановить** (Pause) соответственно. Можно также выбрать **Перезапустить** (Restart) для остановки и повторного запуска сервиса после небольшой паузы. Дополнительно, если служба была приостановлена для восстановления ее нормальной работы, выберите команду **Продолжить** (Resume).

> ***Примечание***
>
> При невозможности запуска автоматически запускаемых служб в их состоянии не будет ничего указано, а пользователь получит уведомление в виде всплывающего сообщения. Сообщение о сбое службы будет также записано в системный журнал. В ОС Windows Server 2012 можно настроить действия, которые будут вызываться при обнаружении сбоя автоматического запуска службы. Например, Windows Server 2012 может попытаться перезапустить службу. Подробно об этом мы поговорим в *разд. "Настройка восстановления службы" далее в этой главе*.

Настройка запуска службы

Службы можно запускать вручную или автоматически. Также можно выключить службы, запретив их запуск. Для настройки автоматического запуска службы выполните следующие действия в оснастке **Управление компьютером**:

1. Щелкните на службе правой кнопкой мыши, в появившемся меню выберите команду **Свойства** (Properties).

2. На вкладке **Общие** (General) открывшегося диалогового окна используйте список **Тип запуска** (Startup Type) для выбора типа запуска (рис. 3.10):
   - **Автоматически** (Automatic) — установите этот тип запуска для автоматического запуска службы во время загрузки системы;
   - **Автоматически (отложенный запуск)** (Automatic (Delayed Start)) — выберите этот тип для отсрочки запуска службы, ее запуск будет отложен, пока не будут запущены все службы, запуск которых нельзя отложить;
   - **Вручную** (Manual) — выберите этот тип запуска, когда нужен ручной запуск службы;
   - **Отключена** (Disabled) — выберите этот тип для выключения службы.
3. Нажмите кнопку **OK**.

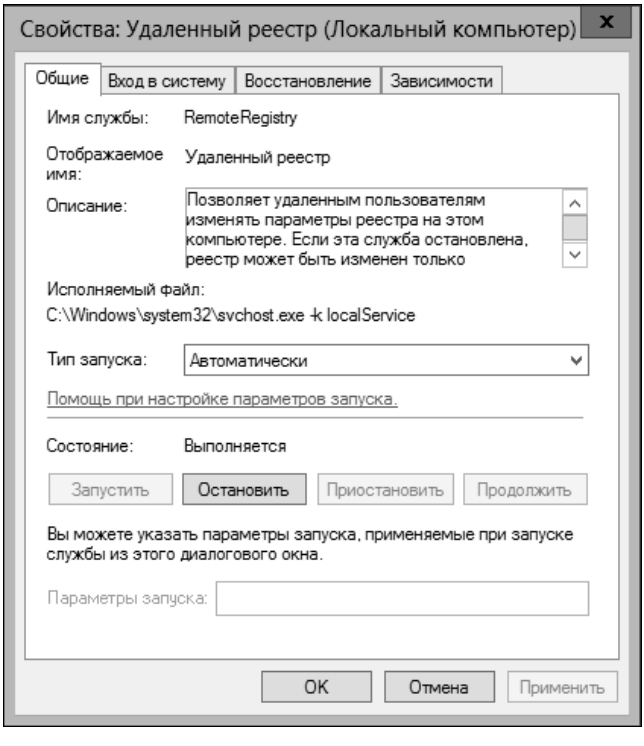


Рис. 3.10. Настройте параметры запуска службы на вкладке **Общие** с помощью списка **Тип запуска**

Настройка входа в систему службы

Вход в систему службы можно настроить как от имени системной учетной записи, так и от имени конкретного пользователя. Для этого выполните следующие действия:

1. В оснастке **Управление компьютером** щелкните правой кнопкой мыши на интересующей службе и выберите команду **Свойства**.
2. Перейдите на вкладку **Вход в систему** (Log On) (рис. 3.11).
3. Отметьте переключатель **С системной учетной записью** (Local System Account), если служба должна входить в систему с использованием системной учетной записи (по

умолчанию для большинства служб). Если служба предоставляет интерфейс пользователя, можно установить флажок **Разрешить взаимодействие с рабочим столом** (Allow Service To Interact With Desktop), чтобы разрешить пользователю контролировать интерфейс службы.

4. Выберите переключатель **С учетной записью** (This Account), если нужно, чтобы служба входила в систему с указанной учетной записью пользователя. Убедитесь, что в текстовых полях ниже указаны имя пользователя и пароль. Нажмите кнопку **Обзор** для поиска нужной учетной записи, если это необходимо.
5. Нажмите кнопку **OK**.

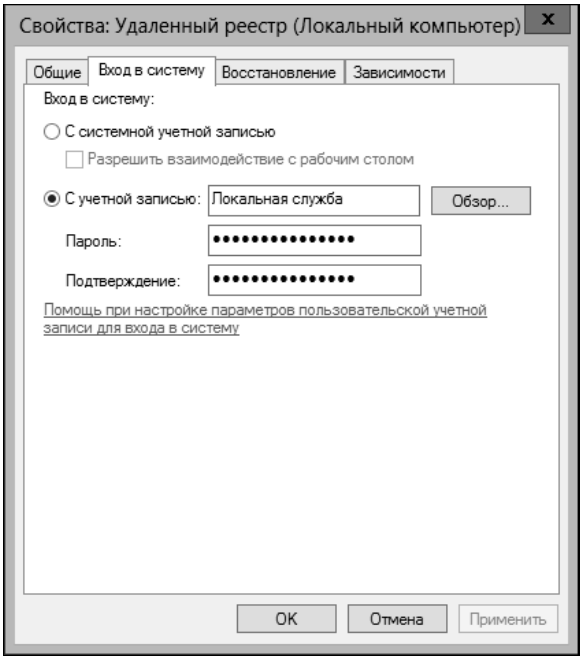


Рис. 3.11. Используйте вкладку **Вход в систему** для настройки параметров входа в систему службы

Внимание!

Необходимо отслеживать любые учетные записи, которые используются со службами. Эти учетные записи могут быть источником проблем безопасности, если не настроены должным образом. У таких учетных записей должны быть самые строгие настройки безопасности и как можно меньше полномочий, позволяющих службе выполнить только необходимые функции. Как правило, учетные записи, используемые со службами, не требуют многих полномочий, которые присвоены нормальной учетной записи пользователя. Например, большинство учетных записей службы не требует права локального входа в систему. Каждый администратор должен знать, какие учетные записи службы используются (так, чтобы лучше отследить использование этих учетных записей), и должен обрабатывать их, как будто они являются учетными записями администратора. Это означает использование безопасных паролей, тщательный контроль использования учетной записи, тщательное назначение полномочий учетной записи и т. д.

Настройка восстановления службы

Можно настроить реакцию на сбой службы. Например, попытаться перезапустить службу или запустить приложение. Для настройки опций восстановления службы выполните следующие действия:

1. В оснастке **Управление компьютером** щелкните правой кнопкой мыши на службе и выберите команду **Свойства**.
2. Перейдите на вкладку **Восстановление** (Recovery) (рис. 3.12).

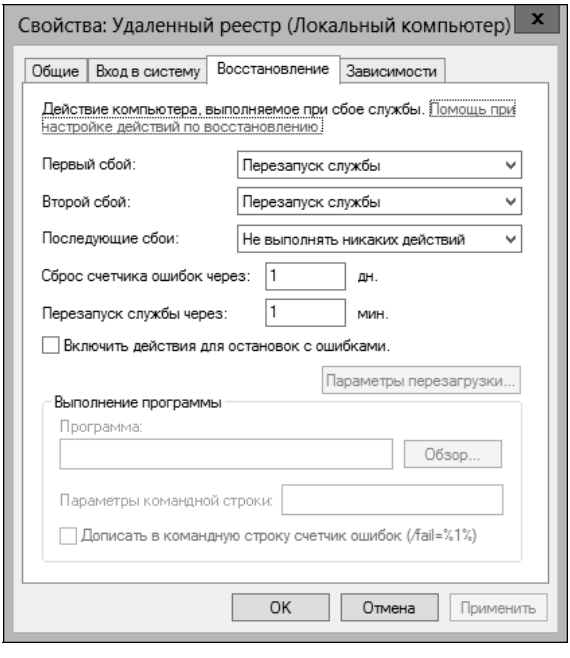


Рис. 3.12. Используйте вкладку **Восстановление** для определения действий, которые будут выполнены в случае сбоя запуска службы

Примечание

ОС Windows Server 2012 автоматически настраивает восстановление для критических системных служб: они будут автоматически перезапущены в случае сбоя. В случае сбоя некоторых экстремально важных служб, например Модуль запуска процессов DCOM-сервера и Клиент групповой политики, будет перезапущена операционная система.

3. Здесь можно указать действия для первого, второго и всех последующих сбоев.
   - **Не выполнять никаких действий** (Take No Action) — операционная система не будет восстанавливать службу для этого отказа, но она все еще может попытаться применить восстановление для предыдущего или последующего отказов.
   - **Перезапуск службы** (Restart The Service) — останавливает и затем запускает службу после непродолжительной паузы.
   - **Запуск программы** (Run A Program) — позволяет запустить программу или сценарий в случае сбоя. Сценарий может быть командным сценарием или Windows-сценарием. Установите полный путь к исполняемому файлу программы, которую

нужно запустить, а также в случае необходимости задайте параметры, которые будут переданы программе при ее запуске.

- **Перезапуск компьютера** (Restart The Computer) — завершает работу и перезагружает компьютер. Перед выбором этой опции дважды проверьте параметры запуска и восстановления. Нужно, чтобы система выбрала умолчания быстро и автоматически.

Рекомендации

При настройке параметров восстановления для критических служб нужно два раза попытаться перезагрузить службу, а потом уже перезагрузить сервер.

4. Настройте параметры на основании ранее выбранных параметров восстановления. Если в качестве опции восстановления выбран запуск программы, нужно установить параметры на панели **Запуск программы** (Run Program). Если выбран перезапуск службы, нужно указать задержку перезапуска. После остановки службы Windows Server будет ждать указанное время перед попыткой запустить службу. В большинстве случаев достаточно задержки от 1 до 2 минут.
5. Нажмите кнопку **OK**.

Отключение ненужных служб

Администратор должен убедиться, что серверы и сеть безопасны, а ненужные службы являются потенциальным источником проблем безопасности. Например, во многих организациях автор этой книги обнаруживал проблемы безопасности, находил запущенные и неиспользующиеся WWW-, FTP- и SMTP-серверы. Такие службы предоставляют анонимным пользователям доступ к серверам, а также открывают сервер для атаки, если он не был должным образом настроен.

При обнаружении ненужных служб можно действовать по-разному. Если эта служба была установлена вместе с ролью (служба роли) или компонентом, можно удалить связанную роль или компонент для удаления из системы всех ненужных компонентов и связанных с ними служб. Второй способ — отключить службу, обычно он и используется вместо деинсталляции компонентов. При этом всегда есть возможность быстро включить эту службу, если какой-то пользователь или другой администратор скажет, что она ему нужна.

Для отключения службы выполните следующие действия:

1. В оснастке **Управление компьютером** щелкните правой кнопкой мыши по службе, которую нужно настроить, и выберите команду **Свойства**. На вкладке **Общие** (General) из списка **Тип запуска** (Startup Type) выберите команду **Отключена** (Disabled).
2. Отключение службы не означает ее остановку. Отключение только предотвращает запуск службы при следующей загрузке компьютера, поэтому риск для безопасности все еще есть. Чтобы завершить службу, нажмите кнопку **Остановить** (Stop) на вкладке **Общие** (General) окна **Свойства**, а затем нажмите кнопку **OK**.

Просмотр и протоколирования событий

Журналы событий предоставляют историческую информацию, которая может помочь при отслеживании проблем с системой. Для работы со службами на удаленных серверах должны быть включены удаленное управление и входящие исключения для службы удаленного управления, как было показано в *главе 2*.

Служба **Журнал событий Windows** (Windows Event Log) контролирует события Windows. После запуска этой службы можно будет отследить действия пользователей и использование ресурсов в журналах событий. Доступны два вида журналов:

- **Журналы Windows** (Windows logs) — сюда записываются системные события, относящиеся к приложениям, безопасности, установке и системным компонентам;
- **Журналы приложений и служб** (Applications and services logs) — сюда записываются сведения, относящиеся к приложениям и службам.

К журналам Windows относятся следующие журналы.

- **Приложение** (Application) — здесь хранятся записи событий, относящиеся к приложениям, например, сбой SQL Server при доступе к базе данных. Размещение по умолчанию — *%SystemRoot%*\System32\Winevt\Logs\Application.evtx.
- **Перенаправленные события** (Forwarded Events) — когда настроено перенаправление событий, этот журнал содержит записи журналов, перенаправленные с других серверов. По умолчанию журнал находится в *%SystemRoot%*\ System32\Config\ForwardedEvents.evtx.
- **Безопасность** (Security) — содержит записи, которые можно использовать для аудита локальных и глобальных групповых политик. По умолчанию журнал называется *%SystemRoot%*\System32\Winevt\ Logs\Security.evtx.

> ***Примечание***
>
> Любой пользователь, которому нужен доступ к журналу безопасности, должен обладать соответствующими правами. По умолчанию такие права есть у членов группы **Администраторы**. О том, как назначить пользователям их права, будет рассказано в *главе 8*.

- **Установка** (Setup) — записи в этот журнал заносит сама операционная система или ее компоненты при инсталляции чего-либо. Название журнала по умолчанию — *%SystemRoot%*\System32\Winevt\Logs\Setup.evtx.
- **Система** (System) — в журнал записывают данные либо операционная система, либо ее компоненты, записи касаются системных событий вроде сбоя службы при ее запуске. Размещение по умолчанию — *%SystemRoot%*\System32\Winevt\Logs\System.evtx.

> ***Внимание!***
>
> Администратор должен просматривать журналы приложений и системы, но не нужно забывать и о журнале безопасности. Этот журнал — один из наиболее важных, его нужно мониторить очень тщательно. Если журнал безопасности не содержит событий, наиболее вероятная причина в том, что локальный аудит не был настроен должным образом либо настроен глобальный аудит домена — в этом случае необходимо мониторить журналы безопасности на контроллерах домена, а не на рядовых серверах.

К журналам приложений и служб относятся следующие журналы:

- **Репликация DFS** (DFS Replication) — регистрирует записи активности DFS-репликации (Distributed File System). Имя журнала по умолчанию — *%SystemRoot%*\System32\ Winevt\Logs\DfsReplication.evtx;
- **Служба каталогов** (Directory Service) — регистрирует записи AD DS (Active Directory Domain Services) и связанных служб. Журнал по умолчанию — *%SystemRoot%*\ System32\Winevt\Logs\Directory Service.evtx;
- **DNS-сервер** (DNS Server) — регистрирует события DNS-сервера — запросы, ответы и другую активность DNS. Файл журнала по умолчанию — *%SystemRoot%*\System32\ Winevt\Logs\DNS Server.evtx;

- **Служба репликации файлов** (File Replication Service) — регистрирует активность репликации файлов в системе. Журнал по умолчанию — *%SystemRoot%*\System32\ Winevt\Logs\File Replication Service.evtx;
- **События оборудования** (Hardware Events) — когда подсистема событий оборудования настроена, в этом журнале будут события, относящиеся к оборудованию. Журнал по умолчанию — *%SystemRoot%*\System32\Config\Hardware.evtx;
- **Microsoft\Windows** — предоставляет журналы событий, относящихся к Windows-службам и компонентам. Журналы организованы по типу компонента и категории события. Операционные журналы генерируются стандартными операциями связанного компонента. В некоторых случаях у вас появятся дополнительные журналы для анализа, отладки и записи задач, связанных с администрированием;
- **Windows PowerShell** — записывает активность, связанную с использованием Windows PowerShell. Имя файла журнала по умолчанию — *%SystemRoot%*\System32\ Winevt\Logs\ Windows PowerShell.evtx.

Доступ к событиям в диспетчере серверов

Если при работе с диспетчером серверов выбрать узел **Локальный сервер**, **Все серверы** или группу серверов, на панели справа появится панель **СОБЫТИЯ** (рис. 3.13), которая отобразит события выбранного сервера. Эту панель можно использовать так:

- для локального сервера можно использовать панель **СОБЫТИЯ** в разделе **Локальный сервер** или **Все серверы** с целью просмотра последних предупреждений и ошибок в журналах приложений и системы;
- для автоматически созданной группы серверов: узлы группируются по ролям сервера, таким как AD DS или DNS, и администратор может просмотреть последние события, относящиеся к роли сервера, если это возможно. Не у всех ролей есть ассоциированный журнал, но зато у некоторых ролей, например у AD DS, есть несколько ассоциированных журналов;
- для пользовательских групп серверов, созданных администраторами, используется панель **СОБЫТИЯ** для просмотра последних событий и ошибок в журналах приложений и системы.

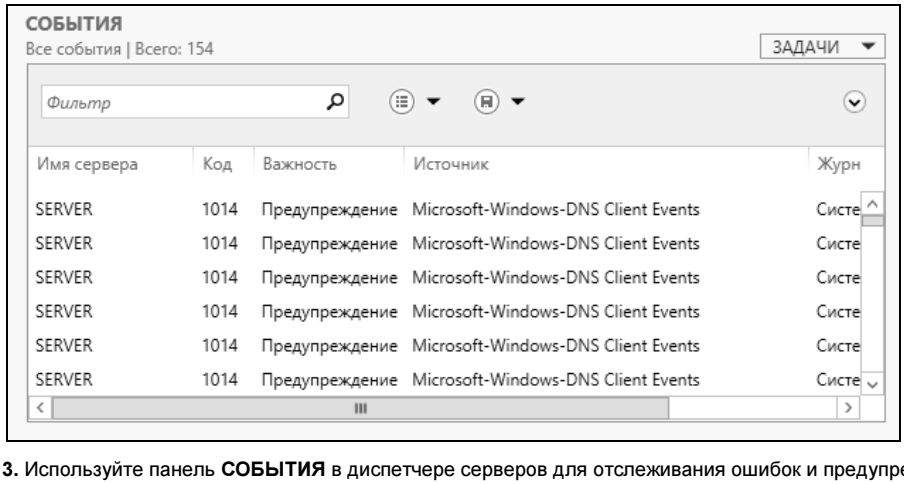


Рис. 3.13. Используйте панель **СОБЫТИЯ** в диспетчере серверов для отслеживания ошибок и предупреждений

Столбцы панели **СОБЫТИЯ** можно настроить так: щелкните правой кнопкой мыши по заголовку таблицы, выберите столбцы, которые нужно добавить или удалить. Столбцы могут быть следующими:

- **Имя сервера** (Server Name) — имя сервера, на котором запущена служба;
- **Полное доменное имя** (FQDN) — полное доменное имя сервера, на котором запущена служба;
- **Код** (ID) — числовой идентификатор определенного события, который может быть полезен при поиске описания событий в различных базах знаний;
- **Важность** (Severity) — уровень важности события, например, ошибка или предупреждение;
- **Источник** (Source) — приложение, служба или компонент, который зарегистрировал событие;
- **Журнал** (Log) — журнал, в котором было зарегистрировано событие;
- **Дата и время** (Date And Time) — дата и время записанного события.

> ***Совет***
>
> При работе со многими серверами используйте опции группировки, позволяющие эффективнее управлять событиями. Можно группировать события по имени сервера, полному доменному имени, коду, важности, источнику, журналу, дате и времени. Для этого щелкните правой кнопкой мыши по заголовку и выберите команду **Группировать по**, а затем выберите критерий группировки.

Доступ к событиям в средстве *Просмотр событий*

Для работы с журналами на удаленных серверах нужно включить удаленное управление и входящие исключения для приложения **Удаленное управление журналом событий** (Remote Event Log Management). Более детальную информацию *см. в главе 2*.

Получить доступ к журналам событий можно с помощью следующих действий:

1. В диспетчере серверов выберите группу **Все серверы** или любую группу серверов на панели слева.
2. В панели **СЕРВЕРЫ** щелкните правой кнопкой мыши по серверу, к которому нужно подключиться.
3. Выберите команду **Управление компьютером** (Computer Management) для автоматического подключения к выбранному серверу.
4. В оснастке **Управление компьютером** можно просматривать и работать с журналами событий, развернув узел **Служебные программы** (System Tools) и выбрав элемент **Просмотр событий** (Event Viewer), как показано на рис. 3.14.
5. Разверните узел **Просмотр событий**. Работать с журналами событий сервера можно примерно так.
   - Для просмотра всех ошибок и предупреждений по всем журналам разверните узел **Настраиваемые представления** (Custom Views), затем выберите **События управления** (Administrative Events). На главной панели будет отображен список всех предупреждений и ошибок для сервера.
   - Для просмотра всех ошибок и предупреждений для конкретной роли разверните **Настраиваемые представления** (Custom Views), затем разверните **Роли сервера**

(Server Roles) и выберите интересующую вас роль. На главной панели будет отображен список всех предупреждений и ошибок для выбранной роли.

- Для просмотра событий в конкретном журнале разверните узел **Журналы Windows** (Windows Logs) или **Журналы приложений и служб** (Applications And Services Logs) (или оба узла). Затем выберите интересующий вас журнал, например **Приложение** (Application) или **Система** (System).

6. Используйте информацию в колонке **Источник** (Source) для определения, какая служба (или какой процесс) зарегистрировала конкретное событие.

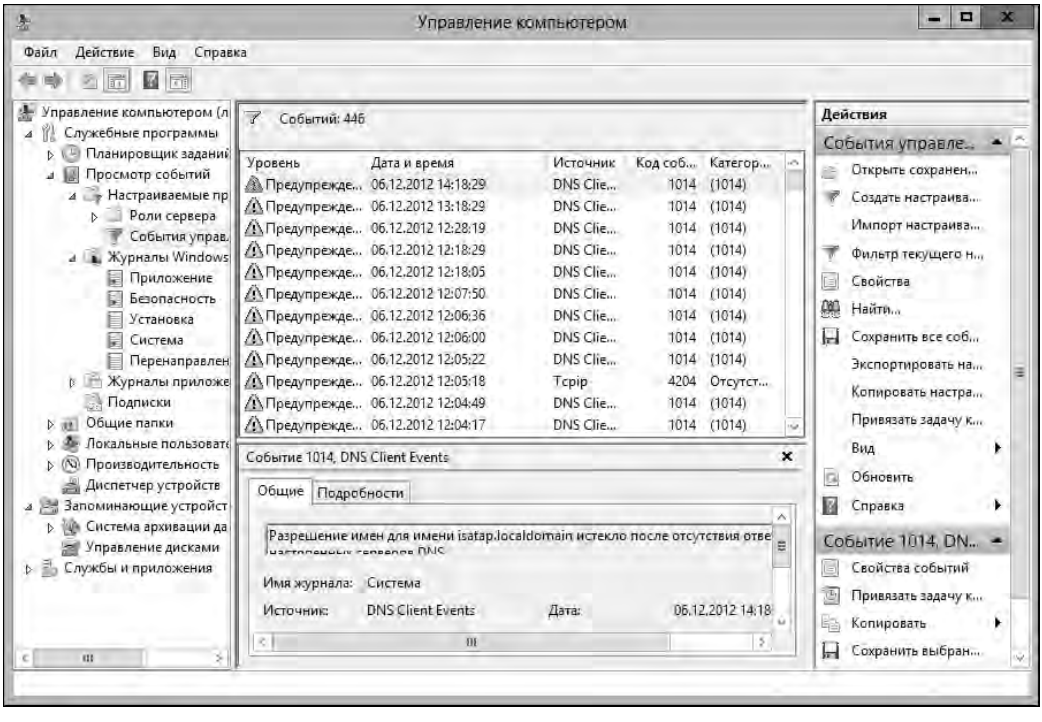


Рис. 3.14. Средство **Просмотр событий** отображает события выбранного журнала или пользовательского представления

Как показано на рис. 3.14, записи на главной панели средства **Просмотр событий** предоставляет быстрый обзор того, когда, где и как произошло событие. Чтобы получить подробную информацию о событии, просмотрите подробности на вкладке **Общие** (General) в нижней части главной панели. Там же выводится уровень события, ключевое слово и дата и время события. Уровни события могут быть:

- **Информация** (Information) — информационное событие, относится к успешному выполнению действия;
- **Аудит успеха** (Audit Success) — событие, относящееся к успешному выполнению действия;
- **Аудит отказа** (Audit Failure) — событие, относящееся к неудачному выполнению действия;
- **Предупреждение** (Warning) — предупреждение. Описания предупреждений часто могут быть полезны для предотвращения будущих проблем;

- **Ошибка** (Error) — некритическая ошибка, например, ошибка передачи зоны на DNS-сервере;
- **Критическое** (Critical) — критическая ошибка, например, завершение работы службы кластера из-за потери кворума.

> ***Примечание***
>
> Предупреждения и ошибки — два ключевых типа событий, которые нужно тщательно изучать. Каждый раз, когда происходят такие ошибки и их причина не ясна, внимательно просмотрите описание события.

В дополнение к уровню, дате и времени предоставляется общее описание события:

- **Источник** (Source) — приложение, служба или компонент, который зарегистрировал событие;
- **Код** (Event ID) — числовой идентификатор определенного события, который может быть полезен при поиске события в базах знаний;
- **Категория задачи** (Task Category) — категория события, которая часто не заполняется, но иногда может быть использоваться для описания связанного действия;
- **Пользователь** (User) — учетная запись пользователя, которая была зарегистрирована в системе, когда произошло событие, если это возможно;
- **Компьютер** (Computer) — имя компьютера, на котором произошло событие;
- **Описание** (Description) — текстовое описание события;
- **Данные** (Data) — любые данные или код ошибки, переданные событием.

Фильтрация журналов событий

Средство **Просмотр событий** автоматически создает несколько фильтров представлений журналов событий. Фильтры представлений находятся в узле **Настраиваемые представления** (Custom Views). Если выбрать узел **События управления** (Administrative Events), станет доступен список всех ошибок и предупреждений для всех журналов. Если развернуть узел **Роли сервера** (Server Roles) и выбрать представление, специфичное для роли, можно будет просмотреть все события для выбранной роли.

Для создания собственного представления используются следующие действия в оснастке **Управление компьютером**:

1. На панели слева выберите узел **Настраиваемые представления**, затем нажмите кнопку **Создать настраиваемое представление** (Create Custom View) на панели справа. Откроется диалоговое окно, показанное на рис. 3.15.
2. Используйте раскрывающийся список **Дата** (Logged), чтобы задать период времени для события. Можно выбрать события за последний час, последние 12 часов, последние 24 часа, последние 7 дней или последние 30 дней. Альтернативно можно указать свой диапазон.
3. Используйте флажки в группе **Уровень события** (Event Level), чтобы указать, события какого уровня вас интересуют. Установите флажок **Подробности** (Verbose) для отображения дополнительных деталей события.
4. Можно создать настраиваемое представление, указав набор журналов или набор источников событий.

- Используйте раскрывающийся список **Журналы событий** (Event Logs), чтобы выбрать необходимые журналы событий. Чтобы выбрать несколько журналов событий, отметьте их переключатели.
- Раскрывающийся список **Источники событий** (Event Sources) служит для выбора источников событий. Чтобы выбрать несколько источников, отметьте их переключатели. Остальные источники будут исключены.

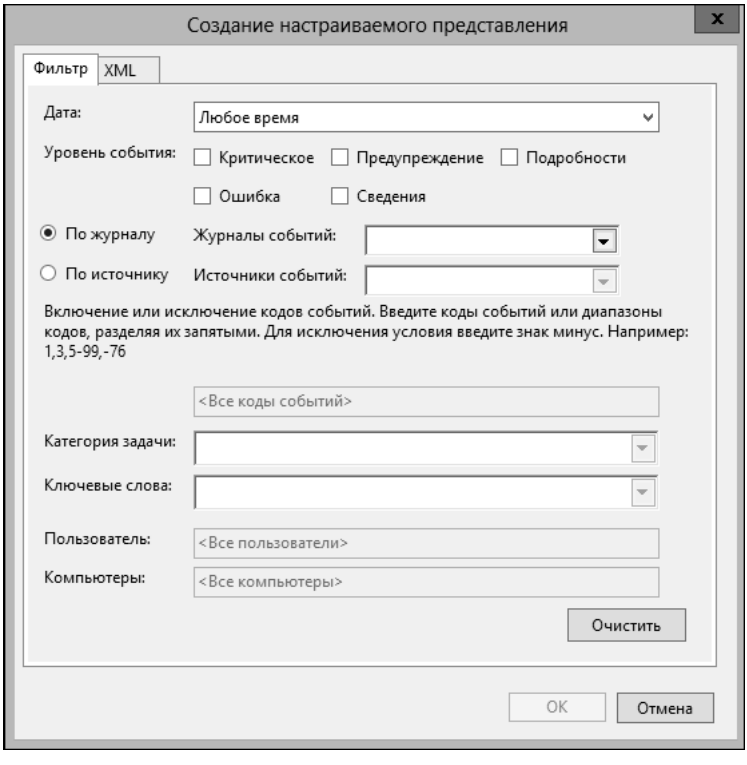


Рис. 3.15. Можно отфильтровать журналы, чтобы просмотреть только определенные события

5. Дополнительно можно использовать поля **Пользователь** (User) и **Компьютеры** (Computers) для указания пользователей и компьютеров, связанных с событиями. Если не указать эти параметры, будут выбраны события, относящиеся ко всем пользователям и компьютерам.
6. После нажатия кнопки **OK** Windows отобразит окно **Сохранить фильтр в настраиваемое представление** (Save Filter To Custom View) (рис. 3.16).
7. Введите имя и описание настраиваемого представления.
8. Выберите, где нужно сохранить настраиваемое представление. По умолчанию настраиваемые представления сохраняются в узле **Настраиваемые представления**. Можно создать новый узел, нажав кнопку **Создать папку** (New Folder), ввести имя папки. Затем нажмите кнопку **OK**.
9. Нажмите кнопку **OK** для закрытия окна **Сохранить фильтр в настраиваемое представление**. Теперь список событий будет отфильтрован. Просмотрите эти события и исправьте существующие проблемы.

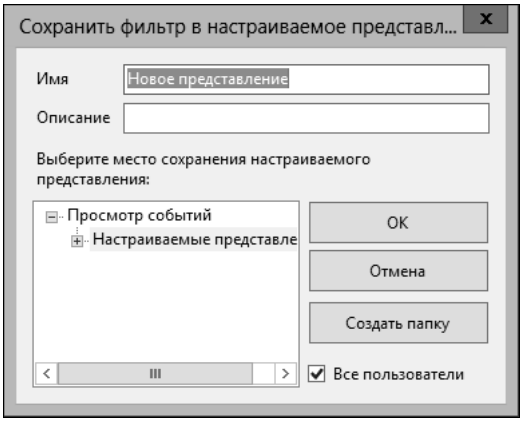


Рис. 3.16. Сохраните новое представление

Если нужно видеть только события определенного типа, можно отфильтровать журнал в оснастке **Управление компьютером** с помощью следующих действий:

1. Разверните узел **Журналы Windows** (Windows Logs) или **Журналы приложений и служб** (Applications And Services Logs). После этого будут показаны журналы событий.
2. Щелкните правой кнопкой мыши по журналу, с которым нужно работать, а затем выберите команду **Фильтр текущего журнала** (Filter Current Log), будет отображено окно, подобное представленному на рис. 3.15.
3. Используйте раскрывающийся список **Дата** для выбора диапазона времени для регистрируемых событий. Можно выбрать события за последний час, последние 12 часов, последние 24 часа, последние 7 дней или последние 30 дней.
4. Используйте флажки группы **Уровень события**, чтобы указать, события какого уровня вас интересуют. Установите флажок **Подробности** для отображения дополнительных деталей события.
5. Используйте раскрывающийся список **Источники событий** (Event Source) для выбора источников событий. Чтобы выбрать несколько источников, отметьте их переключатели. Остальные источники будут исключены.
6. Дополнительно можно использовать поля **Пользователь** и **Компьютеры** для указания пользователей и компьютеров, связанных с событиями. Если не указать эти параметры, будут выбраны события, относящиеся ко всем пользователям и компьютерам.
7. Нажмите кнопку **OK**. После этого список событий будет отфильтрован. Внимательно просмотрите эти события и примите меры для исправления любых существующих проблем. Чтобы очистить фильтр и увидеть все события, выберите действие **Очистить фильтр** (Clear Filter) на панели **Действия** (Actions) справа или в меню **Действие** (Action).

Установка параметров журнала событий

Параметры журнала позволяют управлять размером журналов событий, а также способом обработки журналирования. По умолчанию максимальный размер журнала событий — максимальный размер файла. Когда журнал достигнет этого предела, события будут перезаписаны, чтобы предотвратить превышение максимального размера файла.

Для установки параметров журналирования в оснастке **Управление компьютером** выполните следующие действия:

1. Разверните узел **Журналы Windows** или **Журналы приложений и служб** в зависимости от журнала, который нужно настроить. Будет отображен список журналов событий.
2. Щелкните правой кнопкой мыши на журнале, свойства которого нужно изменить, а затем выберите команду **Свойства** из контекстного меню. Откроется диалоговое окно, изображенное на рис. 3.17.

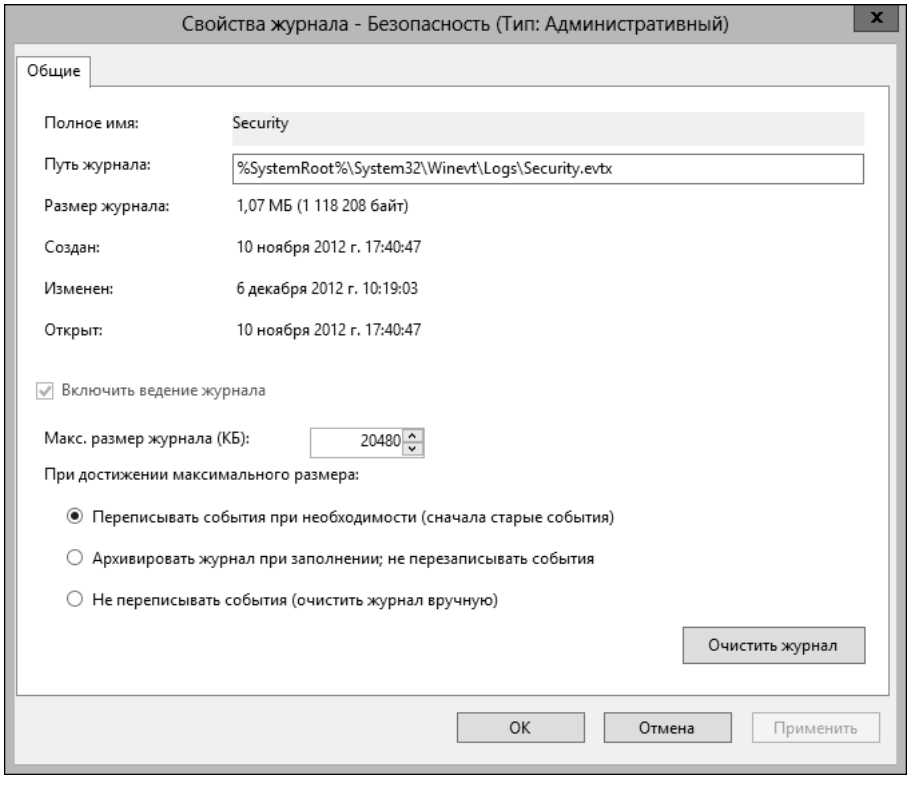


Рис. 3.17. Настройка параметров журнала в зависимости от уровня аудита системы

3. Введите или установите максимальный размер в килобайтах в поле **Макс. размер журнала (КБ)** (Maximum Log Size). Убедитесь, что диск, содержащий операционную систему, имеет достаточно свободного места для хранения файла журнала указанного вами размера. По умолчанию файлы журналов хранятся в каталоге *%SystemRoot%*\System32\Winevt\Logs.
4. Выберите действие при достижении максимального размера. Доступны опции:
   - **Переписывать события при необходимости (сначала старые события)** (Overwrite Events As Needed (Oldest Events First)) — при достижении максимального размера журнала события в журнале будут перезаписаны. Это лучший выбор для системы низкого приоритета;
   - **Архивировать журнал при заполнении; не перезаписывать события** (Archive The Log When Full, Do Not Overwrite Events) — когда будет достигнут максимальный

размер файла, Windows заархивирует события путем сохранения текущего журнала в каталоге по умолчанию. Затем Windows создаст новый журнал для хранения текущих событий;

- **Не переписывать события (очистить журнал вручную)** (Do Not Overwrite Events (Clear Logs Manually)) — когда будет достигнут максимальный размер файла, система сгенерирует сообщения об ошибке ввиду того, что журнал событий полон.

5. Нажмите кнопку **OK**, как только установите параметры.

Примечание

На критических системах, где безопасность и протоколирование событий очень важны, нужно установить переключатель **Архивировать журнал при заполнении; не перезаписывать события**. При использовании этого метода можно быть уверенным, что сохранена вся история событий.

Очистка журналов событий

После заполнения журнала событий его нужно очистить. Для этого в оснастке **Управление компьютером** выполните следующие действия:

1. Разверните узел **Журналы Windows** или **Журналы приложений и служб** в зависимости от журнала, который необходимо настроить. Будет показан список журналов событий.
2. Щелкните правой кнопкой мыши на журнале, свойства которого нужно изменить, а затем выберите команду **Очистить журнал** (Clear Log) из контекстного меню.
3. Выберите команду **Сохранить и очистить** (Save And Clear) для сохранения копии журнала перед его очисткой. Также можно выбрать команду **Очистить** (Clear) для очистки файла журнала без его сохранения.

Архивирование журналов событий

На ключевых системах вроде контроллеров домена и серверов приложений нужно хранить журналы несколько месяцев. Однако обычно не следует задавать для этой цели огромный размер журналов. Вместо этого необходимо позволить Windows периодически архивировать журналы событий или же архивировать журналы вручную.

Форматы архивов журналов

Журналы могут храниться в четырех форматах:

- формат файлов событий (evtx), который можно просмотреть с помощью средства **Просмотр событий**;
- текстовый формат с разделителем табуляции (txt), который можно просмотреть в текстовых редакторах и текстовых процессорах или импортировать в электронную таблицу или базу данных;
- текст, разделенный запятой (csv), удобный для импорта в электронную таблицу или базу данных;
- текст формата XML (xml) для сохранения в XML-файле.

При экспорте файлов журналов в формат CSV каждую колонку в таком файле будет разделять запятая. Записи будут примерно такими:

```
Information,07/21/14 3:43:24 PM,DNS Server,2,None,The DNS server has started.
Error,07/21/14 3:40:04 PM,DNS Server,4015,None,The DNS server has encountered a
critical error from the Directory Service (DS). The data is the error code.
```

Формат записи следующий:

```
Уровень, Дата и время, Источник, Код, Категория задачи, Описание
```

Архивирование журналов

ОС Windows создает архивы журналов автоматически, если выбрана опция **Архивировать журнал при заполнении; не перезаписывать события** (см. ранее). При желании архив можно создать вручную с помощью следующих действий:

1. Разверните **Журналы Windows** или **Журналы приложений и служб** в зависимости от журнала, который нужно настроить. Будет показан список журналов событий.
2. Щелкните правой кнопкой мыши по журналу, который необходимо заархивировать, и выберите команду **Сохранить все события как** (Save all events as) из контекстного меню.
3. В окне **Сохранение** (Save As) выберите каталог и введите имя файла журнала.
4. В списке **Тип файла** (Save as type) значением по умолчанию является **Файлы событий (.evtx)** (Event Files (*.evtx)). Выберите необходимый формат журнала и нажмите кнопку **Сохранить** (Save). Заметьте, что нельзя использовать формат EVTX при сохранении событий удаленного компьютера в локальную папку. В этом случае нужно сохранить события на локальный компьютер в любом другом формате, например XML. Если нужен формат EVTX, сохраните журнал на удаленном компьютере.
5. Если планируется просматривать журналы на других компьютерах, в окне (которое появится после нажатия кнопки **Сохранить**) нужно установить флажок **Отображать сведения для следующих языков** (Display information for these languages), задайте нужный язык и нажмите кнопку **OK**. В противном случае просто нажмите кнопку **OK** — сведения не будут отображаться.

> ***Примечание***
>
> Если планируется архивировать журналы регулярно, необходимо создать отдельный каталог для архивов, в котором можно быстро найти архивы журналов. Также необходимо присваивать архивам осмысленные имена, чтобы было просто определить, где и какой журнал находится. Например, если архивируется системный журнал за январь 2014 года, его можно назвать System Log Jan 2014.

> ***Совет***
>
> Лучший формат для архивов — формат EVTX. Используйте его, если планируете просматривать старые журналы в средстве **Просмотр событий**. Однако, если планируете просматривать журналы в других приложениях, нужно сохранить журналы в текстовом формате с разделением табуляцией или CSV-форматах. В этих случаях можно отредактировать журналы (при необходимости) в текстовом редакторе. Если журнал сохранен в формате EVTX, всегда можно сохранить другую копию в текстовом или CSV-форматах, используя команду **Сохранить как** после открытия EVTX-журнала в оснастке **Просмотр событий**.

Просмотр архивов журналов

Архивы журналов, сохраненные в текстовом или CSV-форматах, можно просмотреть в любом текстовом редакторе или текстовом процессоре. В формате EVTX архивы можно просмотреть в оснастке **Просмотр событий**.

Для этого выполните следующие действия:

1. В оснастке **Управление компьютером** щелкните правой кнопкой мыши на узле **Просмотр событий**. Из появившегося меню выберите команду **Открыть сохраненный журнал** (Open Saved Log).
2. В одноименном окне выберите каталог и имя журнала. По умолчанию выбран формат **Файлы журнала событий** (Event Logs Files). Будет отображен список журналов, сохраненных в форматах EVTX, EVT, ETL. Можно также отфильтровать список файлов, выбрав другой формат файла.
3. Нажмите кнопку **Открыть** (Open). Если увидите запрос о необходимости конвертирования журнала в новый формат, нажмите кнопку **Да** (Yes).
4. ОС Windows отобразит окно **Открыть сохраненный журнал** (Open Saved Log). Введите имя и описание сохраненного журнала.
5. Укажите, где нужно сохранить журнал. По умолчанию сохраненные журналы помещаются в узел **Сохраненные журналы** (Saved Logs). Можно создать новый узел, нажав кнопку **Создать папку** (потребуется ввести имя новой папки и нажать кнопку **OK**).
6. Нажмите кнопку **OK** для закрытия окна **Открыть сохраненный журнал**. После этого будет отображено содержимое сохраненного журнала.

> ***Совет***
>
> Для удаления сохраненного журнала из оснастки **Просмотр событий** выберите действие **Удалить** на панели **Действия**. Появится запрос на подтверждение ваших действий, нажмите кнопку **Да**. Сохраненный журнал все еще будет находиться в своем исходном каталоге.

Мониторинг производительности и активности сервера

Контроль сервера должен осуществляться в соответствии с четким планом — ряда целей, которых надеетесь достигнуть. Давайте разберемся, почему нужно контролировать сервер и какие инструменты можно использовать для этого.

Почему нужно контролировать сервер?

Проблемы производительности сервера — ключевая причина мониторинга. Например, у пользователей могут быть проблемы с подключением к серверу, и администратору нужно контролировать сервер для решения этих проблем. Цель администратора — найти и устранить проблему с помощью доступных инструментов для мониторинга.

Другая частая причина мониторинга сервера — повышение его производительности. Этого можно достичь путем улучшения дискового ввода-вывода, снижения использования процессора и сетевой нагрузки на сервер. К сожалению, когда дело доходит до использования ресурсов, часто приходится идти на компромиссы. Например, когда число пользователей, получающих доступ к серверу, растет, нельзя уменьшить загрузку сети, но можно улучшить производительность сервера посредством выравнивания нагрузки или распределения ключевых файлов данных на отдельных дисках.

Готовимся к мониторингу

Прежде чем начать контролировать сервер, установите базовые показатели производительности сервера. Определите производительность сервера в разное время и при разной нагрузке. Затем можно будет сравнить базовые показатели с производительностью сервера после внесенных изменений. Такая техника укажет на области, требующие оптимизации или настройки.

После определения базовых метрик нужно сформулировать план мониторинга. Всесторонний план мониторинга включает следующие шаги:

1. Определите, какие события сервера должны контролироваться (в зависимости от поставленной цели).
2. Установите фильтры для уменьшения потока собираемой информации.
3. Настройте счетчики производительности, чтобы просмотреть использование ресурсов.
4. Регистрируйте данные событий, чтобы можно было их проанализировать.
5. Анализируйте данные событий, чтобы найти решения проблемы.

Все эти процедуры рассматриваются далее в этой главе. Несмотря на то, что обычно необходимо разработать план мониторинга, не всегда нужно проходить через все эти шаги, чтобы контролировать сервер. Например, можно контролировать и анализировать действие, когда оно происходит, вместо мониторинга журнала и анализа данных после выполнения действия.

Основные утилиты, использующиеся для мониторинга серверов, таковы.

- **Системный монитор** (Performance Monit) — используется для настройки счетчиков производительности, которые служат для получения информации об использовании ресурсов. Эту информацию можно применять для построения графика производительности сервера и определения областей, которые могут быть оптимизированы.
- **Монитор стабильности работы** (Reliability Monitor) — отслеживает изменения в системе и сравнивает их с изменениями стабильности работы. Предоставляет график зависимости стабильности работы от внесенных изменений в конфигурацию системы.
- **Монитор ресурсов** (Resource Monitor) — предоставляет подробную информацию об использовании ресурсов сервера. Информация предоставляется примерно в таком же виде, как и в диспетчере задач (чуть более расширенно).
- **Просмотр событий** (Event logs) — используйте информацию в журналах событий для решения глобальных проблем системы, в том числе проблем операционной системы и приложений. Основные журналы, с которыми придется работать, — **Система** (System), **Безопасность** (Security), **Приложение** (Application), а также журналы настроенных ролей сервера.

Использование консолей мониторинга

Монитор ресурсов, Монитор стабильности работы и Системный монитор — утилиты, использующиеся для тюнинга производительности. Открыть Монитор ресурсов можно так: нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc>, а затем — кнопку **Открыть монитор ресурсов** (Open Resource Monitor) на вкладке **Производительность** (Performance) диспетчера задач.

Статистика использования ресурсов разделена на четыре категории (рис. 3.18).

- **ЦП** (CPU) — текущее использование центрального процессора и его максимальная частота (связано с бездействием процессора). Если развернете запись в этой категории, то увидите список работающих в данное время процессов (выводится имя исполняемого файла, ID процесса, описание, состояние, используемое число потоков, текущее и среднее использование ЦП).
- **Диск** (Disk) — показывает число килобайтов, считанных с диска или записанных на диск, за одну секунду. Также можно просмотреть наивысший процент использования. Если развернуть запись в этой категории, будет отображен список запущенных исполняемых файлов и указано, как они работают с диском. В списке содержится следующая информация: имя исполняемого файла, ID процесса, файл, с которым работает процесс, среднее число записанных/прочитанных байтов в секунду, общее число записанных/прочитанных байтов, приоритет ввода-вывода и время ответа диска.

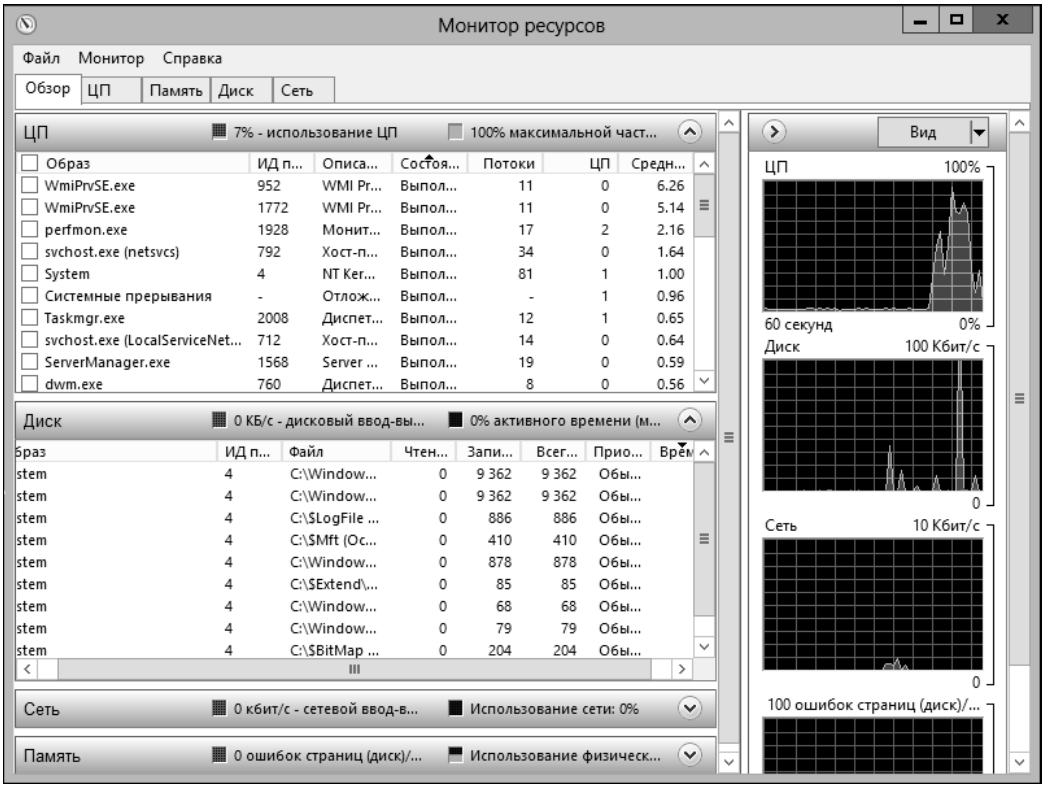


Рис. 3.18. Использование ресурсов сервера

- **Сеть** (Network) — показывает, как используется пропускная способность сети. Эти данные выражены в килобайтах и в процентах от общей "ширины" пропускной способности. Если развернуть эту категорию, будут отображены сведения о том, как работающие процессы используют сеть. В таблице есть следующая информация: имя исполняемого файла, передающего или принимающего данные в этот момент, ID процесса, IP-адрес или имя сервера, с которым связывается процесс, среднее и общее число отправленных/прочитанных байтов в секунду.

- **Память** (Memory) — предоставляет информацию о текущем использовании памяти, а также числе жестких ошибок в секунду. Если развернуть эту категорию, то можно увидеть список работающих процессов, имя исполняемого файла, ID процесса, количество жестких ошибок в секунду, потребление памяти в килобайтах, рабочий набор памяти в килобайтах, разделяемую и неразделяемую память в килобайтах.

Системный монитор графически отображает статистику для набора выбранных вами параметров. Эти параметры так же известны, как *счетчики*. При установке определенных приложений в системе Системный монитор должен обновить набор счетчиков для отслеживания производительности сервера. Эти счетчики можно обновить при установке дополнительных служб и расширений для приложений.

Существуют разные способы запуска Системного монитора. В диспетчере серверов в меню **Средства** (Tools) можно выбрать команду **Системный монитор** (Performance Monitor). В оснастке **Управление компьютером** данная утилита вызывается как оснастка из узла **Служебные программы**: **Служебные программы\Производительность\Средства наблюдения\Системный монитор** (System Tools\Performance\Monitoring Tools\Performance Monitor).

На рис. 3.19 показано, как Системный монитор создает графики в зависимости от отслеживаемых счетчиков. Интервал обновления для этого графика — 1 секунда, но можно использовать и другие значения. Самой ценной является информация, которая записывается в журнал так, чтобы она могла быть воспроизведена. Кроме того, Системный монитор полезен для настройки уведомлений, возникающих при определенных событиях.

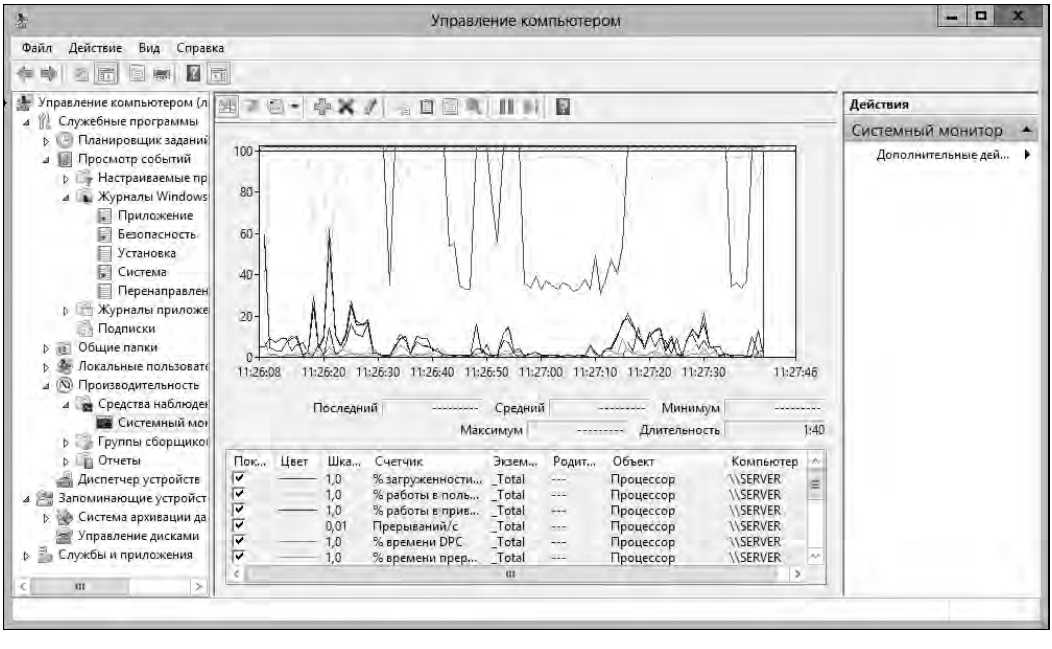


Рис. 3.19. Системный монитор в действии

В ОС Windows Server 2012 также имеется Монитор стабильности работы (Reliability Monitor). Чтобы открыть его, выполните следующие действия:

1. В категории **Система и безопасность** (System And Security) Панели управления щелкните по ссылке **Проверка состояния компьютера** (Review Your Computer's Status).

2. В Центре поддержки (Action Center) разверните панель **Обслуживание** (Maintenance) и щелкните по ссылке **Показать журнал стабильности работы** (View Reliability History).

Альтернативно, Монитор стабильности работы может быть запущен с помощью команды `perfmon /rel` из командной строки или в поле поиска приложений.

Монитор стабильности работы отслеживает изменения, внесенные в сервер, и сравнивает их с изменениями в стабильности системы. Он предоставляет графическое представление зависимости стабильности системы от внесенных в конфигурацию системы изменений. Системой записываются следующие изменения: установка нового программного обеспечения (ПО), удаление ПО, отказы приложений, отказы оборудования, отказы Windows и ключевые события относительно настройки сервера, а администратор увидит временную шкалу этих изменений в надежности работы сервера и затем будет ее использовать для определения изменений, которые вызвали проблемы с устойчивостью.

Хотя мониторинг устойчивости включен по умолчанию для Windows-клиентов, он выключен для Windows-серверов. При запуске утилиты Монитор стабильности на сервере, на котором мониторинг устойчивости выключен, будет отображена панель, подсказывающая, где нужно щелкнуть, чтобы включить или настроить RACTask — запланированное фоновое задание, собирающее данные стабильности.

Выбор счетчиков

Системный монитор отображает информацию только по отслеживаемым счетчикам. Доступны тысячи счетчиков, и можно найти счетчики для любой установленной вами роли сервера. Простейший путь изучить назначение того или иного счетчика — прочитать его описание в окне **Добавление** (Add Counters). Запустите Системный монитор и нажмите кнопку **Добавить** (Add) на панели инструментов, а потом разверните объект в списке **Имеющиеся счетчики** (Available Counters). Чтобы получить информацию о счетчике, установите переключатель **Отображать описание** (Show Description).

Когда Системный монитор контролирует определенный объект, он отслеживает все инстанции всех счетчиков для этого объекта. Инстанции (экземпляры) — разные варианты одного и того же счетчика. Например, при отслеживании счетчиков для объекта **Процессор** на многопроцессорной системе можно отслеживать либо все экземпляры процессоров, либо отдельную инстанцию процессора. Если думаете, что есть проблемы с каким-то определенным процессором, можно наблюдать только за ним.

Для выбора контролируемых счетчиков выполните следующие действия:

1. У Системного монитора есть несколько представлений и типов представлений. Убедитесь, что выбрана текущая активность (кнопка **Просмотр текущей активности** (View Current Activity)), или нажмите комбинацию клавиш <Ctrl>+<T>. Можно переключаться между типами представлений (**Строка** (Line), **Линейчатая гистограмма** (Histogram Bar) и **Отчет** (Report)), нажав кнопку **Изменить тип диаграммы** (Change Graph Type) или комбинацию клавиш <Ctrl>+<G>.
2. Для добавления счетчиков нажмите кнопку **Добавить** на панели инструментов или комбинацию клавиш <Ctrl>+<N>. Откроется окно **Добавление** (Add Counters) (рис. 3.20).
3. В списке **Выбрать счетчики для компьютера** (Select Counters From Computer) введите UNC-имя (Universal Naming Convention) сервера, с которым нужно работать, например \\CorpServer84, или выберите **<локальный компьютер>** для работы с локальным компьютером.

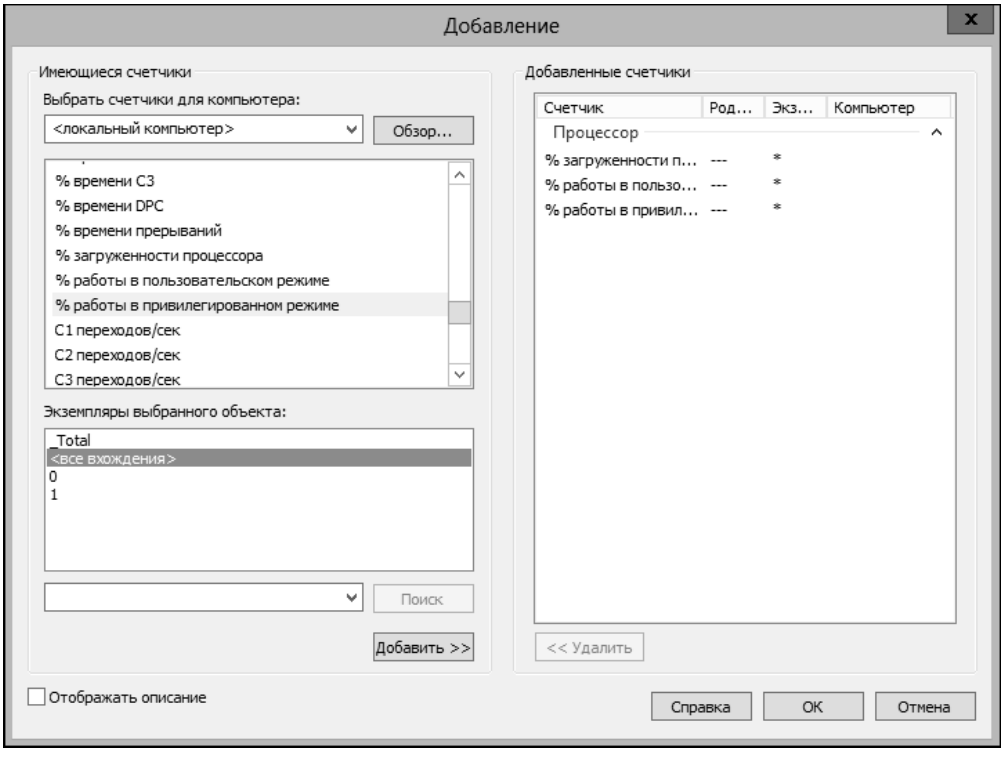


Рис. 3.20. Выберите объекты и счетчики, которые нужно контролировать

Примечание

Для мониторинга нужно быть членом группы **Пользователи системного монитора** (Performance Monitor Users) домена или локального компьютера. Для протоколирования производительности нужно быть членом группы **Пользователи журналов производительности** (Perfomance Log Users) домена или локального компьютера для работы с журналами производительности на удаленных компьютерах.

4. В группе **Имеющиеся счетчики** (Available Counters) все объекты выводятся в алфавитном порядке. Если выбрать запись объекта, автоматически будут выбраны все относящиеся к ней счетчики. Если развернуть запись объекта, будут отображены его счетчики, и можно будет их выбрать отдельно. Например, если развернуть объект **Процессор**, в нем будут счетчики **% загруженности процессора**, **Процент времени бездействия** и т. д.
5. После выбора объекта или любого из его счетчиков будут отображены все экземпляры выбранного объекта. Можно выбрать **<все вхождения>** для выбора всех экземпляров счетчиков или же указать один или более экземпляров для мониторинга. Например, можно выбрать **_Total** для общей загрузки процессора или **0**/**1** для построения графика загрузки по конкретному ядру процессора (в случае с двухъядерным процессором).
6. Когда выберете объект или группу счетчиков объекта (или экземпляров объекта), нажмите кнопку **OK** для добавления счетчиков на график.
7. Повторите шаги 4—6 для добавления других параметров производительности.
8. Нажмите кнопку **OK**, когда закончите.

Совет

Не пытайтесь добавить на график слишком много счетчиков или экземпляров счетчиков. Это сделает график слишком сложным для чтения, а также займет слишком много системных ресурсов (а именно ресурсов ЦП и памяти), что снизит скорость отклика сервера.

Журналирование производительности

В Windows Server 2008 R2 появились группы сборщиков данных и отчеты. *Группы сборщиков данных* позволяют собрать данные с объектов и отслеживаемых счетчиков производительности. Когда будет создан сборщик данных, можно легко начать и остановить мониторинг объектов и счетчиков, включенных в группу. В некотором смысле, это делает группы сборщиков данных подобными журналам производительности, которые использовались в более ранних выпусках Windows. Однако группы сборщиков данных намного сложнее. Можно использовать единственную группу данных, чтобы генерировать многократные счетчики производительности и журналы трассировки. Также можно делать следующее:

- определить, кто может получить доступ к собранным данным;
- создать множественные задачи планировщика и условия остановки мониторинга;
- использовать диспетчеры данных для контроля размера собранных данных и отчетов;
- генерировать отчеты на основании собранных данных.

В утилите **Производительность** (Performance) можно просмотреть настроенные в данный момент группы сборщиков данных и отчеты в узлах **Группы сборщиков данных** (Data Collector Sets) и **Отчеты** (Reports) соответственно. Доступны как пользовательские (узел **Особые** (User Defined)), так и системные группы сборщиков данных (рис. 3.21). Пользовательские группы создаются пользователями для общего мониторинга и тюнинга производи-

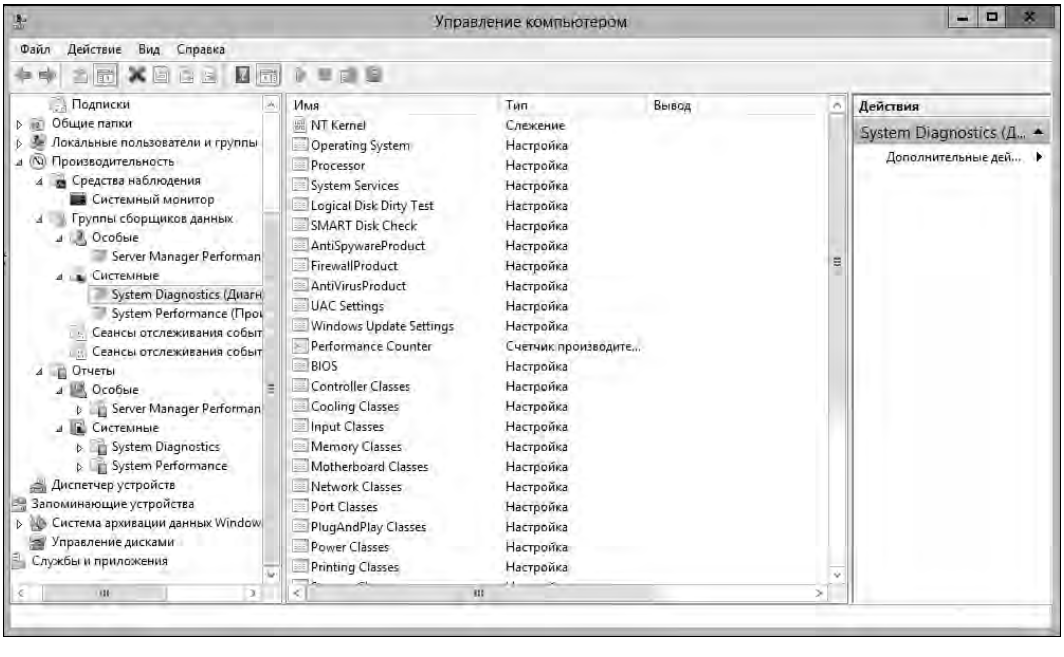


Рис. 3.21. Доступ к сборщикам данных и отчетам

тельности. Системные группы сборщиков данных создаются операционной системой для автоматической диагностики.

Группы сборщиков данных: создание и управление

Для просмотра созданных групп сборщиков данных запустите Системный монитор и перейдите к узлу **Группы сборщиков данных**. Работать со сборщиками данных можно поразному:

1. Можно просматривать пользовательские или системные группы сборщиков данных, выбрав узел **Особые** (User Defined) или **Системные** (System) соответственно. При выборе группы сборщиков данных на панели слева, на панели справа будут показаны сборщики данных, входящие в эту группу (выводится имя и тип сборщика). Тип **Слежение** (Trace) используется для сборщиков данных, которые записывают сведения о производительности каждый раз, когда возникают связанные события. Тип **Счетчик производительности** (Performance Counter) используется для сборщиков данных, которые записывают данные по выбранным счетчикам, когда предопределенный интервал истек. А тип **Настройка** (Configuration) — для коллекторов данных, которые записывают изменения в определенных путях реестра.
2. Можно просматривать текущие сеансы отслеживания событий, выбрав узел **Сеансы отслеживания событий** (Event Trace Sessions). Для остановки сборщика данных, выполняющего отслеживания, щелкните по нему правой кнопкой мыши и выберите команду **Стоп** (Stop).
3. В узле **Сеансы отслеживания событий запуска** (Startup Event Trace Sessions) доступны состояния трассировок события (включено или выключено), запускаемых автоматически при загрузке компьютера. Можете запустить трассировку, щелкнув правой кнопкой мыши по сборщику данных и выбрав команду **Запустить как сеанс отслеживания событий** (Start As Event Trace Session). Для удаления сборщика данных используется команда **Удалить** (Delete) в контекстном меню.
4. Можно сохранить сборщик данных как шаблон, который будет использоваться в качестве основы других сборщиков данных, для этого щелкните правой кнопкой мыши по сборщику и выберите команду **Сохранить шаблон** (Save Template). В окне **Сохранить как** (Save As) выберите каталог, введите имя файла шаблона, а затем нажмите **Сохранить** (Save). Сборщик данных сохраняется как XML-файл, который можно скопировать на другие системы.
5. Для удаления пользовательского сборщика данных щелкните правой кнопкой мыши на нем и выберите команду **Удалить**. Если сборщик данных запущен, сначала нужно его остановить, а уже после этого — удалять. Удаление сборщика удалит относящиеся к нему отчеты.

Сбор данных счетчиков производительности

Сборщики данных могут использоваться для записи данных производительности по выбранным счетчикам с определенной периодичностью. Например, можно получать данные производительности ЦП каждые 15 минут.

Для сбора данных со счетчика производительности выполните следующие действия:

1. В Системном мониторе перейдите в узел **Группы сборщиков данных** (Data Collector Sets), щелкните правой кнопкой мыши на узле **Особые**, выберите команду **Создать | Группа сборщиков данных** (New | Data Collector Set).

2. В мастере **Создать новую группу сборщиков данных** (Create New Data Collector Set Wizard) введите имя сборщика данных, например Монитор производительности системы или Монитор состояния процессора. Обратите внимание, что нельзя ввести неправильное имя, например, содержащее неалфавитно-цифровые символы, иначе вы не сможете продолжить настройку.
3. Выберите опцию **Создать вручную** (Create Manually) и нажмите кнопку **Далее**.
4. На странице **Какой тип данных вы хотите использовать** (What Type Of Data Do You Want To Include) опция **Создать журналы данных** (Create Data Logs) выбрана по умолчанию. Выберите **Счетчик производительности** (Performance Counter) и нажмите кнопку **Далее**.
5. На странице **Какие счетчики производительности следует записывать в журнал** (Which Performance Counters Would You Like To Log) нажмите кнопку **Добавить**. Будет отображено окно **Добавление**, которое было рассмотрено ранее. Когда выберете счетчики, нажмите кнопку **OK**.
6. На странице **Какие счетчики производительности следует записывать в журнал** (Which Performance Counters Would You Like To Log) введите интервал выборки и задайте единицы измерения времени (секунды, минуты, часы, дни или недели). Интервал выборки определяет периодичность выборки данных. Например, если установлен интервал 15 минут, то данные будут обновляться каждые 15 минут. Нажмите кнопку **Далее**, когда будете готовы продолжить.
7. На странице **Где необходимо сохранить данные** (Where Would You Like The Data To Be Saved) введите каталог, в котором будут храниться собранные данные. Можно также нажать кнопку **Обзор** и использовать окно **Обзор папок** (Browse For Folder) для выбора каталога. Нажмите кнопку **Далее**, когда будете готовы продолжить.

   Рекомендации

   Путь по умолчанию для сохранения собранных данных — *%SystemDrive%*\PerfLogs\Admin. Файлы журналов могут расти в размере очень быстро. Если планируется собирать данные на протяжении долгого периода времени, убедитесь, что на диске есть достаточно свободного пространства. Помните, чем чаще обновляется журнал, тем больше будет использование дискового пространства и ресурсов ЦП.

8. На странице **Создать группу сборщиков данных** (Create Data Collector Set) поле **Пользователь** (User) содержит значение **<По умолчанию>**, т. е. сбор данных будет происходить с правами и привилегиями системной учетной записи по умолчанию. Для запуска сбора данных с правами другого пользователя нажмите кнопку **Изменить** (Change). В появившемся окне введите имя пользователя и пароль для используемой учетной записи и нажмите кнопку **OK**. Имя пользователя можно ввести в формате "домен\имя", например, cpandl\williams для учетной записи Williams в домене Cpandl.
9. Выберите опцию **Открыть свойства группы сборщиков данных** (Open Properties For This Data Collector Set) и нажмите кнопку **Готово** (Finish). В результате группа сборщиков данных будет сохранена, мастер ее создания закрыт и открыто окно **Свойства**.
10. По умолчанию журналирование запускается вручную. Для настройки запуска журналирования по расписанию перейдите на вкладку **Расписание** (Schedule) и затем нажмите кнопку **Добавить**. Теперь можно установить параметры **Активный диапазон** (Active Range), **Начальная дата** (Start Time) и др.
11. По умолчанию журналирование останавливается, как только закончится его срок действия. Используя параметры на вкладке **Условие остановки** (Stop Condition), можно

настроить автоматический останов журналирования по другому условию (через определенный период времени или при заполнении файла журнала, если установлен лимит размера файла).

12. Нажмите кнопку **OK**, когда закончите устанавливать параметры и условия остановки задачи журналирования. Управлять сборщиком данных можно так, как было показано ранее.

> ***Примечание***
>
> Можно настроить Windows так, чтобы ОС автоматически запускала запланированное задание при останове сбора данных. Такие задания можно указать на вкладке **Задача** окна **Свойства**.

Сбор данных трассировки производительности

Сборщики данных используются для записи данных трассировки производительности каждый раз, когда возникают события, связанные с их исходными поставщиками. Исходный поставщик — прикладная служба или служба операционной системы, у которой есть отслеживаемые события.

Для сбора данных трассировки производительности выполните следующие действия:

1. В Системном мониторе перейдите в узел **Группы сборщиков данных** (Data Collector Sets), щелкните правой кнопкой мыши на узле **Особые**, выберите команду **Создать | Группа сборщиков данных**.
2. В мастере **Создать новую группу сборщиков данных** введите имя сборщика данных, например, Logon Trace (трассировка входа) или Disk IO Trace (трассировка ввода-вывода диска). Обратите внимание, что нельзя ввести неправильное имя, например, содержащее неалфавитно-цифровые символы, иначе вы не сможете продолжить настройку.
3. Выберите опцию **Создать вручную** и нажмите кнопку **Далее**.
4. На странице **Какой тип данных вы хотите использовать** опция **Создать журналы данных** (Create Data Logs) выбрана по умолчанию. Установите флажок **Данные отслеживания событий** (Event Trace Data) и нажмите кнопку **Далее**.
5. На странице **Какие службы трассировки должны быть включены** (Which Event Trace Providers Would You Like To Enable) нажмите кнопку **Добавить**. Выберите поставщика отслеживания событий и затем нажмите кнопку **OK**. Выберите отдельные свойства в списке **Свойства** и нажмите кнопку **Изменить**: можно будет указать определенные значения свойства вместо выбора всех значений поставщика. Повторите этот процесс для выбора других событий трассировки поставщика для отслеживания. Нажмите кнопку **Далее** для продолжения.
6. Повторите шаги 7—12 процедуры, описанной в *разд. "Сбор данных счетчиков производительности" ранее в этой главе*.

Сбор данных сведений о конфигурации системы

Использовать сборщики данных можно для записи изменений в конфигурации реестра. Для сбора данных конфигурации выполните следующие действия:

1. В Системном мониторе перейдите в узел **Группы сборщиков данных** (Data Collector Sets), щелкните правой кнопкой мыши на узле **Особые**, выберите команду **Создать | Группа сборщиков данных**.

2. В мастере **Создать новую группу сборщиков данных** введите имя сборщика данных, например, AD Registry или Registry Adapter Info.
3. Выберите опцию **Создать вручную** и нажмите кнопку **Далее**.
4. На странице **Какой тип данных вы хотите использовать** опция **Создать журналы данных** выбрана по умолчанию. Установите флажок **Сведения о конфигурации системы** (System Configuration) и нажмите кнопку **Далее**.
5. На странице **Какие разделы реестра следует записывать** (Which Registry Keys Would You Like To Record) нажмите кнопку **Добавить**. Введите путь реестра, который нужно отслеживать. Повторите этот процесс для добавления других путей реестра. Нажмите кнопку **Далее**, когда будете готовы продолжить
6. Выполните шаги 7—12 процедуры, описанной в *разд. "Сбор данных счетчиков производительности" ранее в этой главе*.

Просмотр отчетов сборщика данных

При решении проблемы часто нужно записывать данные производительности за обширный период времени, а затем просматривать их для анализа результатов. Для каждого активного сборщика данных имеются связанные с ним отчеты сборщика данных. Как и сборщики данных, отчеты сборщиков данных разбиты на две общие категории: **Особые** (определенные пользователем) и **Системные** (определенные системой).

Отчеты сборщика данных можно просмотреть в Системном мониторе. Раскройте узел **Отчеты** (Reports), а затем раскройте узел отчета, связанный со сборщиком данных, который нужно проанализировать. В узле отчета сборщиков данных можно найти отдельные отчеты для каждого сеанса входа: с момента начала протоколирования и до его завершения.

У самых последних журналов номер журнала — самый большой. Если сборщик данных активен, то нельзя просмотреть самый последний журнал. Нужно остановить сбор данных (для этого щелкните правой кнопкой мыши по сборщику данных и выберите команду **Стоп**), после этого можно будет просмотреть последний журнал. Для счетчиков производительности собранные данные по умолчанию представлены в виде графика, с момента запуска сбора данных до его окончания (рис. 3.22).

Для модификации подробностей отчетов выполните следующие действия:

1. Находясь на панели монитора, нажмите комбинацию клавиш <Ctrl>+<Q> или кнопку **Свойства** на панели инструментов. Это действие отобразит окно **Свойства: Системный монитор** (Performance Monitor Properties).
2. Выберите вкладку **Источник** (Source).
3. Выберите источники данных для анализа. В области **Источник данных** (Data Source) нажмите кнопку **Файлы журнала** (Log Files), а затем — кнопку **Добавить** (Add) для открытия окна **Выбор файла журнала** (Select Log File). Теперь можно выбрать дополнительные файлы журналов для анализа.
4. Укажите временной диапазон, который нужно проанализировать. Нажмите кнопку **Диапазон времени** (Time Range) и затем с помощью ползунка **Весь диапазон** (Total Range) укажите время начала и окончания.
5. Перейдите на вкладку **Данные** (Data). Теперь можно выбрать счетчики для просмотра. Выберите счетчик и затем нажмите кнопку **Удалить** (Remove), чтобы удалить счетчик с графика. Чтобы снова добавить счетчик на график, нажмите кнопку **Добавить** для отображения окна **Добавление** — оно используется для выбора счетчиков данных для анализа.

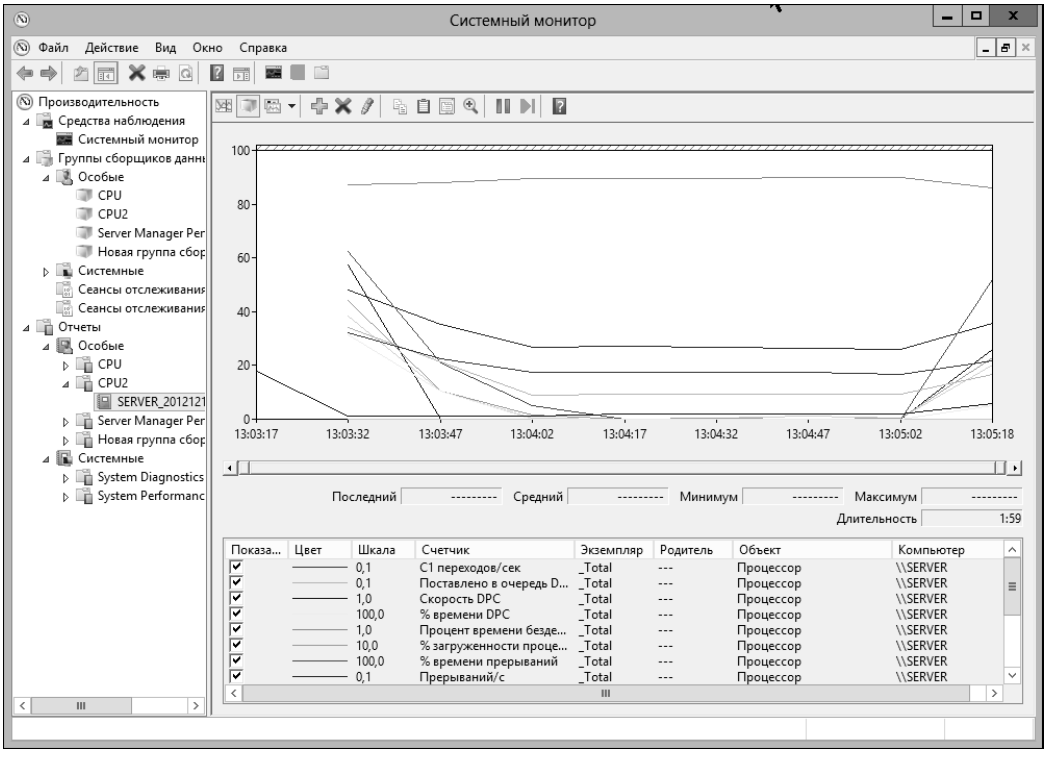


Рис. 3.22. Просмотр отчетов сборщика данных

Примечание

Доступны только счетчики, выбранные для протоколирования. Если в списке нет нужного счетчика, модифицируйте свойства сборщика данных, перезапустите процесс протоколирования и затем просмотрите журналы за последнее время.

6. Нажмите кнопку **OK**. На панели монитора нажмите кнопку **Изменить тип диаграммы** (Change Graph Type) для выбора типа графика.

Настройка оповещений счетчиков производительности

Можно настроить оповещения, когда произойдут определенные события или когда будет достигнут определенный порог производительности. Также можно настроить оповещения для запуска приложений и протоколирования производительности.

Для настройки оповещений выполните следующие действия:

1. В Системном мониторе перейдите в узел **Группы сборщиков данных**, щелкните правой кнопкой мыши на узле **Особые**, выберите команду **Создать | Группа сборщиков данных**.
2. В мастере **Создать новую группу сборщиков данных** введите имя сборщика данных, например, Оповещение процессора или Оповещение дискового ввода-вывода.
3. Выберите опцию **Создать вручную** и нажмите кнопку **Далее**.
4. На странице **Какой тип данных вы хотите использовать** выберите опцию **Оповещение счетчика производительности** (Performance Counter Alert) и нажмите кнопку **Далее**.

5. На странице **Какие счетчики производительности следует контролировать** (Which Performance Counters Would You Like To Monitor) нажмите **Добавить**, чтобы отобразить окно **Добавление**. Это окно идентично ранее рассмотренному одноименному окну. Нажмите кнопку **OK**, когда закончите.
6. На панели **Системные счетчики** (Performance Counters) выберите первый счетчик, затем в поле **Оповещение при** (Alert When Value) укажите, когда будет генерироваться оповещение для этого счетчика. Оповещения могут быть сгенерированы, когда значение счетчика становится выше или ниже определенного значения. Выберите элемент списка **Выше** (Above) или **Ниже** (Below), а затем установите значение **Порог** (значение триггера). Задайте ту единицу измерения, которая целесообразна для выбранного в настоящее время счетчика или счетчиков. Например, чтобы сгенерировать предупреждение, когда загрузка процессора составит более 95%, выберите вариант **Выше** (Above) и установите значение 95. Повторите этот процесс, чтобы настроить другие выбранные вами счетчики.
7. Выполните шаги 7—12 процедуры, описанной в *разд. "Сбор данных счетчиков производительности" ранее в этой главе*.

Тюнинг производительности системы

Теперь, когда было показано, как контролировать систему, давайте разберемся, как можно выполнить тюнинг производительности операционной системы и аппаратных средств. Необходимо исследовать следующие области:

- использование памяти и кэширование;
- использование процессора;
- дисковый ввод-вывод;
- пропускная способность сети.

Мониторинг и тюнинг использования памяти

Память — частый источник проблем производительности, и всегда нужно исследовать проблемы памяти перед тестированием других областей системы. Системы используют физическую и виртуальную память. Чтобы исключить проблемы памяти, необходимо сконфигурировать производительность приложений, использование памяти и настройки пропускной способности, а затем контролировать использование памяти сервера, чтобы проверить, есть ли проблемы.

Производительность приложений и использование памяти определяют, как выделены системные ресурсы. В большинстве случаев нужно отдать львиную долю ресурсов операционной системе и фоновым приложениям. Это особенно важно для Active Directory, файлового сервера, сервера печати и коммуникационного сервера. С другой стороны, для серверов приложений, баз данных и потоковых медиасерверов нужно предоставить больше ресурсов программам, запущенных на сервере, как было показано в *главе 2*.

С помощью мониторинга, описанного ранее в этой главе, можно определить, как система использует память, и проверить наличие ошибок. В табл. 3.1 приведен обзор счетчиков, которые понадобится отслеживать, чтобы найти узкие места памяти, кэширования и виртуальной памяти.

Таблица 3.1. *Узкие места памяти*

Проблема	Счетчики, которые нужно отследить	Описание
Использование физической и виртуальной памяти	**Память\Доступно КБ** (Memory\Available Kbytes) **Память\Байт выделенной виртуальной памяти** (Memory\Committed Bytes)	**Память\Доступно КБ** — это количество физической памяти, доступной процессам, запущенным на сервере. **Память\Байт выделенной виртуальной памяти** — это число выделенной виртуальной памяти. Если у сервера мало доступной памяти, нужно добавить память в систему. В целом, должно быть не меньше 5% доступной памяти от общего количества физической памяти сервера. Если у сервера более высокое соотношение занятых байтов к физической памяти, как правило, и в этой ситуации нужно добавить память. В целом, соотношение выделенной виртуальной памяти к физической памяти должно быть не больше 75%
Ошибки страниц памяти	**Память\ Ошибок страниц/с** (Memory\Page Faults/sec) **Память\Ввод страниц/с** (Memory\Pages Input/sec) **Память\Чтений страниц/с** (Memory\Page Reads/sec)	Ошибки страниц возникают, когда процесс запрашивает страницу в памяти и система не может найти запрашиваемую локацию. Если запрошенная страница есть в любом другом месте памяти, то ошибка считается мягкой (soft page fault). Если запрашиваемая страница должна быть получена с диска, ошибка называется жесткой (hard page faults). Большинство процессоров могут обрабатывать огромное число мягких ошибок. Жесткие ошибки могут привести к значительным задержкам. Показатель **Ошибок страниц/с** — это общая частота обработки процессором ошибок страниц всех типов. **Ввод страниц/с** — общее число страниц, прочитанных с диска для разрешения жестких ошибок страниц. **Чтений страниц/с** — общее число чтений с диска, необходимое для разрешений жестких ошибок страниц. Значение **Ввод страниц/с** должно быть больше или равно значению **Чтений страниц/с** и может дать представление о частоте ваших жестких ошибок страниц. Большое число жестких ошибок страниц говорит о необходимости увеличения памяти или уменьшения размера кэша на сервере
Подкачка памяти	**Память\Байт в выгружаемом страничном пуле** (Memory\Page Reads/sec) **Память\Байт в невыгружаемом страничном пуле** (Memory\Pool Nonpaged Bytes)	Эти счетчики отслеживают число байтов в выгружаемом и невыгружаемом пуле. Выгружаемый пул — это область системной памяти для объектов, которые могут быть записаны на диск, когда они не используются. Невыгружаемый пул — это область системной памяти для объектов, которые не могут быть записаны на диск. Если размер выгружаемого пула большой относительно количества общего количества физической памяти в системе, нужно добавить дополнительную память в систему. Если размер невыгружаемого пула большой относительно количества виртуальной памяти, выделенной на сервере, нужно увеличить размер виртуальной памяти

Мониторинг и тюнинг использования процессора

Процессор занимается обработкой информации на сервере. Поскольку исследуется производительность сервера, нужно сфокусироваться на процессоре после того, как будут ликвидированы узкие места памяти. Если процессоры сервера являются узким местом производительности, то добавлением памяти, дисков и сетевых соединений решить проблемы не получится. Вместо этого нужно установить процессоры с более высокой тактовой частотой или добавить дополнительные процессоры. Также можно переместить приложения, интенсивно использующие процессор, например SQL Server, на другой сервер.

Перед принятием решения модернизировать или добавить процессоры нужно исключить проблемы с памятью и кэшированием. Если проблема все еще указывает на процессор, нужно контролировать счетчики производительности, перечисленные в табл. 3.2. Обязательно контролируйте эти счетчики для каждого ЦП, установленного на сервере.

Таблица 3.2. *Исследование узких мест процессора*

Проблема	Счетчики, которые нужно отследить	Описание
Очереди потоков	**Система\ Длина очереди процессора** (System\Processor Queue Length)	Этот счетчик отображает число потоков, ожидающих выполнения. Эти потоки находятся в области, общей для всех процессоров в системе. Если значение счетчика превышает 10 потоков на процессор, нужно либо модернизировать процессор, либо добавить дополнительные процессоры
Использование ЦП	**Процессор\% загруженности процессора** (Processor\% Processor Time)	Этот счетчик отображает процент времени выбранного ЦП. Нужно отслеживать этот счетчик для всех инстанций процессора на сервере. Если процент загруженности процессора высок при относительно низком использовании сети и диска, надо заменить процессор либо добавить дополнительные процессоры

Мониторинг и тюнинг дискового ввода-вывода

С сегодняшними высокоскоростными дисками пропускная способность дисковой системы ввода-вывода — редкая причина узкого места. Однако доступ к памяти намного быстрее, чем доступ к дискам. Так, если сервер должен часто обращаться к диску, общая производительность сервера может быть ухудшена. Чтобы уменьшить общее число операций ввода-вывода, нужно эффективно управлять памятью и выгружать страницы на диск только при необходимости. Можно контролировать и настроить использование памяти, как описано в *разд. "Мониторинг и тюнинг использования памяти" ранее в этой главе*.

В дополнение к тюнингу памяти можно контролировать некоторые счетчики для отслеживания активности дискового ввода-вывода. В частности должны контролироваться счетчики, перечисленные в табл. 3.3.

Таблица 3.3. *Исследование узких мест дисковой подсистемы*

Проблема	Счетчики, которые нужно отследить	Описание
Общая производительность диска	**Физический диск\% активности диска** (PhysicalDisk\% Disk Time) в сочетании со счетчиками **Процессор\% загруженности процессора** (Processor\% Processor Time) и **Сетевой интерфейс\Всего байт/с** (Network Interface Connection\Bytes Total/sec)	Если процент активности диска слишком высок, но загрузка процессора и сети не высокие, дисковая подсистема может быть узким местом. Убедитесь, что вы контролируете загрузку всех дисков сервера
Дисковый ввод-вывод	**Физический диск\ Обращений записи на диск/с** (PhysicalDisk\Disk Writes/sec) **Физический диск\ Обращений чтения с диска/с** (PhysicalDisk\Disk Reads/sec) **Физический диск\Средняя длина очереди записи на диск** (PhysicalDisk\Avg. DiskWrite Queue Length) **Физический диск\Средняя длина очереди чтения диска** (PhysicalDisk\Avg. DiskRead Queue Length) **Физический диск\ Текущая длина очереди диска** (PhysicalDisk\CurrentDisk Queue Length)	Количество попыток записи и чтения в секунду говорит о степени активности ввода-вывода. Длина очереди записи и чтения говорит о длине запросов, ожидающих обработки. В целом, должно быть немного ожидающих запросов. Имейте в виду, что задержки запроса пропорциональны длине очередей минус число дисков в RAID-массиве

Мониторинг и тюнинг пропускной способности сети и возможности соединения

Пользователь ощущает производительность сервера также и через сеть, соединяющую его компьютер с вашим сервером. Задержка, или латентность, между временем отправки запроса и временем получения ответа имеет огромное значение. Если даже у вас самый быстрый сервер на планете, но высокие задержки, пользователь ощутит это и сделает вывод, что ваши серверы медленные.

Вообще говоря, задержка, которую чувствует пользователь, неподконтрольна вам. Огромную роль имеет тип подключения, который использует пользователь, и маршрут, по которому запрос следует к вашему серверу. Однако общая способность вашего сервера обрабатывать запросы и пропускная способность ваших серверов — факторы, подконтрольные вам. Доступность пропускной способности сети — это функция инфраструктуры сети вашего предприятия. Пропускная способность сети — функция сетевых плат и интерфейсов, настроенных на серверах.

Пропускная способность сетевой карты может быть ограничивающим фактором в некоторых случаях. Несмотря на то, что сети 10 Гбит/с все больше и больше используются, как

правило, на серверах установлены сетевые платы 100 Мбит/с и 1 Гбит/с, которые могут быть сконфигурированы разными способами. Кто-то, возможно, сконфигурировал карту на 1 Гбит/с для работы на скорости 100 Мбит/с, или карта могла быть сконфигурирована для полудуплекса вместо полного дуплекса. Если возникают подозрения, что могут быть проблемы с сетевой платой, необходимо проверить конфигурацию.

Для определения пропускной способности и текущей активности сетевых карт сервера используйте следующие счетчики:

- **Сетевой адаптер\Получено байт/с** (Network\Bytes Received/sec);
- **Сетевой адаптер\Отправлено байт/с** (Network\Bytes Sent/sec);
- **Сетевой адаптер\Байт всего/с** (Network\Bytes Total/sec);
- **Сетевой адаптер\Текущая пропускная способность** (Network Current Bandwidth).

Если общее число байтов за секунду — более 50% от общей мощности при средней загрузке, у вашего сервера могут возникнуть проблемы при максимальной нагрузке. Убедитесь, что операции, которые занимают много сетевой пропускной способности, например создание резервных копий по сети, выполняются на отдельной сетевой плате. Имейте в виду, что эти значения нужно сравнить со значениями счетчиков **Физический диск\% активности диска** (PhysicalDisk\%Disk Time) и **Процессор\% загруженности процессора** (Processor\% Processor Time). Если загрузка сети и процессора низкая, а сетевая загрузка — высокая, налицо проблема с сетевой подсистемой. Проблему можно решить с помощью оптимизаций настроек сетевой платы или путем добавления еще одной сетевой платы. Помните, что планирование — это всё. Но оно не такое простое, как установка дополнительной сетевой карты и подключение ее к сети.

ГЛАВА 4

Автоматизация административных задач, политики и процедуры

Выполнение ежедневных рутинных задач — не очень эффективное использование рабочего времени. Намного эффективнее автоматизировать эту работу и сфокусироваться на более важных проблемах — на поддержке служб, на повышении производительности, а в результате меньше времени будет потрачено на приземленные вопросы и больше на то, что действительно важно. У Windows Server 2012 много ролей, ролевых служб и компонентов, которые помогают поддерживать инсталляции сервера. Можно легко установить и использовать некоторые из этих компонентов. Если нужны административные утилиты для управления ролью или компонентом на удаленном компьютере, можно выбрать утилиту для установки как части компонента **Средства удаленного администрирования сервера** (Remote Server Administration Tools). Если у сервера есть беспроводной адаптер, то можно установить компонент **Служба беспроводной локальной сети** (Wireless LAN Support), чтобы добавить поддержку беспроводных соединений. Кроме этих основных компонентов можно использовать много других компонентов, включая следующие.

- **Автоматические обновления** (Automatic Updates). Убедитесь, что операционная система обновлена и установлено большинство последних обновлений безопасности. При обновлении сервера с помощью Microsoft Update, а не стандартного обновления Windows, можно получить обновления для дополнительных продуктов. По умолчанию автоматические обновления установлены, но не включены на Windows Server 2012. Можно настроить автоматические обновления с помощью утилиты Центр обновления Windows (Windows Update) в Панели управления. В Панели управления перейдите в категорию **Система и безопасность** (System And Security), затем щелкните по ссылке **Включение или отключения автоматического обновления** (Turn Automatic Updating On Or Off). Далее в этой главе будет рассмотрено, как настроить автоматические обновления с помощью групповой политики.
- **Шифрование диска BitLocker** (BitLocker Drive Encryption) предоставляет дополнительный уровень безопасности для жестких дисков сервера. Это защищает диски от злоумышленников, которые получили физический доступ к серверу. Шифрование диска BitLocker может использоваться даже на серверах без TPM (Trusted Platform Module). После установки этого компонента на сервер с помощью мастера добавления ролей и компонентов им можно управлять посредством утилиты **Шифрование диска BitLocker** из Панели управления. Windows Server 2008 R2 (как и Windows 7/8) и более поздние версии ОС содержат BitLockerToGo, позволяющий шифровать USB-флешки. Если на

сервере не установлен BitLocker, запустите программу BitLocker To Go Reader, которая сохранена на незашифрованной области зашифрованного USB-диска.

- **Удаленный помощник** (Remote Assistance) предоставляет компонент, позволяющий администратору отправлять приглашение удаленного помощника более старшему администратору. Старший администратор может принять приглашение просмотреть рабочий стол пользователя и получить временный контроль над компьютером для решения проблемы. После установки этого компонента на сервер с помощью **Мастера добавления ролей и компонентов** управлять им можно с помощью вкладки **Удаленный доступ** (Remote) окна свойств системы. В Панели управления перейдите в категорию **Система и безопасность** и щелкните по ссылке **Настройка удаленного доступа** (Allow Remote Access) в заголовке **Система** (System) для просмотра соответствующих параметров.
- **Удаленный рабочий стол** (Remote Desktop) предоставляет функцию удаленной связи, позволяющую подключаться и управлять сервером с другого компьютера. По умолчанию удаленный рабочий стол установлен, но не включен на серверах под управлением Windows Server 2012. Управлять конфигурацией удаленного рабочего стола можно на вкладке **Удаленный доступ** окна свойств системы. Чтобы просмотреть относящиеся к компоненту параметры, перейдите в категорию **Система и безопасность** Панели управления и щелкните по ссылке **Настройка удаленного доступа**. Установить удаленные соединения можно с помощью утилиты **Подключение к удаленному рабочему столу** (Remote Desktop Connection).
- **Планировщик заданий** (Task Scheduler) разрешает запланированное выполнение одноразовых и повторяющихся задач, например, задач по рутинному обслуживанию. ОС Windows Server 2012 предполагает широкое применение средств запланированных заданий. С запланированными заданиями можно работать в оснастке **Управление компьютером**. Разверните узел **Служебные программы** (System Tools), затем — **Планировщик заданий | Библиотека планировщика заданий** (Task Scheduler | Task Scheduler Library) для просмотра настроенных заданий.
- **Возможности рабочего стола** (Desktop Experience) — это подкомпонент компонента **Пользовательские интерфейсы и инфраструктура** (User Interfaces And Infrastructure), позволяющий установить функциональность рабочего стола Windows на сервере. Этот компонент можно установить, если Windows Server 2012 используется в качестве настольной операционной системы. После добавления этого компонента с помощью **Мастера добавления ролей и компонентов** функциональность рабочего стола сервера будет расширена, а также будут установлены следующие программы: Проигрыватель Windows Media (Windows Media Player), темы оформления рабочего стола, Видео для Windows (поддержка AVI) (Video for Windows), Защитник Windows (Windows Defender), Очистка диска (Disk Cleanup), Звукозапись (Sound Recorder), Таблица символов (Character Map), Ножницы (Snipping Tool).
- **Брандмауэр Windows** (Windows Firewall) помогает защитить компьютер от атаки неавторизированными пользователями. В состав Windows Server входит базовый брандмауэр, называемый **Брандмауэр Windows** (Windows Firewall), и расширенный брандмауэр, который называется **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall With Advanced Security). По умолчанию брандмауэры не включены на серверных инсталляциях. Чтобы получить доступ к базовому брандмауэру, запустите утилиту **Брандмауэр Windows** из Панели управления. Для получения доступа к расширенному брандмауэру выберите команду **Брандмауэр Windows в режиме повышенной безопасности** в меню **Средства** (Tools) диспетчера серверов.

- **Служба времени Windows** (Windows Time) синхронизирует системное время с мировым временем, чтобы убедиться в точности системного времени. Можно настроить компьютеры на синхронизацию времени с определенным сервером времени. Способ работы службы времени Windows зависит от того, является ли компьютер членом домена или рабочей группы. В домене для синхронизации времени используются контроллеры домена, и можно управлять этой функцией с помощью групповой политики. В рабочей группе для синхронизации времени применяются серверы времени Интернета, и можно управлять этой функцией через утилиту **Дата и время** (Date And Time).

Настройка этих компонентов и управление ими происходит так же, как в Windows 8. Подробное описание и этих компонентов представлено в книге "Microsoft® Windows 8. Справочник администратора"[1].

Много других компонентов предоставляют службы поддержки. Однако нужны эти дополнительные службы только в определенных сценариях. Например, нужно использовать IPAM-серверы (IP Address Management) для управления пространством IP-адресов и отслеживания тенденции использования IP-адресов. Службы удаленного рабочего стола используются, когда нужно позволить пользователям запускать приложения на удаленном сервере. Службы развертывания Windows (Windows Deployment Services) нужны, когда требуется автоматизированное развертывание операционных систем на базе Windows. Однако есть одна служба, которую нужно освоить при работе с Windows Server 2012, — это групповая политика.

> ***ПРАКТИЧЕСКИЙ СОВЕТ***
>
> Панель параметров экрана **Пуск** содержит опцию **Поиск**, с помощью которой можно найти приложения, параметры и файлы. При нажатии клавиши <Windows> и вводе текста, он вводится в поле **Поиск**. Поскольку по умолчанию производится поиск приложений, это позволит быстро найти программу, установленную на сервере.
>
> В этой книге, когда написано, что происходит ввод чего-либо в поле поиска, то имеется в виду поле поиска приложений. Во время ввода текста соответствующие результаты будут выведены на экран. При нажатии клавиши <Enter> Windows выполнит выбранный в настоящий момент результат. Можно использовать поиск приложений, чтобы выполнять программу с определенными параметрами — просто введите команду вместе с ее параметрами и опциями, как будто вы работаете в командной строке.
>
> Нужно запустить команды Windows PowerShell из окна поиска приложений? Просто введите `powershell`, а затем введите команду.

Групповая политика

Групповые политики упрощают администрирование, предоставляя администраторам централизованное управление привилегий, прав и возможностей, как пользователей, так и компьютеров. С помощью групповых политик можно сделать следующее:

- контролировать доступ к Windows-компонентам, системным ресурсам, сетевым ресурсам, утилитам Панели управления, рабочему столу и экрану **Пуск** *(см. разд. "Использование административных шаблонов для установки политик" далее в этой главе)*;
- создать централизованно-управляемые каталоги для специальных папок, например, для пользовательской папки Документы *(см. разд. "Централизованное управление специальными папками" далее в этой главе)*;

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

- определить сценарии пользователя и сценарии компьютера, которые будут запускаться в конкретное время *(см. разд. "Управление сценариями пользователя и компьютера" далее в этой главе)*;
- настроить политики для блокировки учетных записей, параметры паролей, аудита, назначения прав пользователей и безопасности. Большая часть этих тем раскрыта в *главе 8*.

Далее объясняется, как можно применять групповые политики.

Основы групповой политики

Можете думать о политике как о ряде правил, которые помогают управлять пользователями и компьютерами. Групповые политики можно применить к нескольким доменам сразу, отдельным доменам, подгруппам в домене или отдельным системам. Политики, которые применяются к отдельным системам, называются *локальными групповыми политиками* и хранятся только на локальном компьютере. Остальные групповые политики соединены в объекты и хранятся в хранилище данных Active Directory.

Чтобы понять групповые политики, необходимо понимать структуру Active Directory. В Active Directory сайты представляют физическую структуру сети. Сайт — это группа TCP/IP-подсетей, где каждая подсеть представляет физический сегмент сети. Домен — это логическая группа объектов для централизованного управления, подгруппа в домене называется *организационным подразделением*, или организационной единицей (Organizational Unit, OU). В сети могут быть сайты с названиями NewYorkMain, CaliforniaMain и WashingtonMain. В сайте WashingtonMain могут быть домены SeattleEast, SeattleWest, SeattleNorth и SeattleSouth. В домене SeattleEast могут быть организационные подразделения с названиями Information Services (IS), Engineering и Sales.

Групповые политики применяются только к системам, работающим под управлением ОС Windows 2000 и более поздних версий Windows. Настройки групповой политики сохранены в объекте групповой политики (Group Policy Object, GPO). Можно думать о GPO как о контейнере для применяющихся политик и для их настроек. Несколько GPO можно применить к одному сайту, домену или организационному подразделению. Поскольку групповая политика описана с использованием объектов, применяется много объектно-ориентированных понятий. Если думать об объектно-ориентированном программировании, можно предположить, что понятия родительских/дочерних отношений и наследования применимы к GPO, и это действительно так.

Контейнер — высокоуровневый объект, содержащий другие объекты. Посредством наследования политика, которая применялась к родительскому контейнеру, наследуется дочерним контейнером. По существу это означает, что установка политики, применяемой к родительскому объекту, будет передана и дочернему объекту. Например, если применяете установку политики в домене, ее установка будет наследована организационными подразделениями в домене. В этом случае GPO домена — родительский объект, а GPO организационных подразделений — дочерние объекты.

Порядок наследования — сайт, домен, организационное подразделение. Это означает, что настройки групповой политики для сайта будут переданы доменам этого сайта, затем настройки домена будут переданы организационным подразделениям в этом домене.

Наследование можно переопределить. Для этого можно присвоить настройку политики дочернему контейнеру, которая отличается от настройки политики для родительского контейнера. Пока переопределение разрешено (т. е. пока оно не заблокировано), будет применяться установка политики дочернего контейнера. Дополнительную информацию о переопреде-

лении и блокировании GPO *см. в разд. "Блокирование, переопределение и отключение политик" далее в этой главе.*

Порядок применения множественных политик

Когда существуют множественные политики, они применяются в следующем порядке:

1. Локальные групповые политики.
2. Групповые политики сайта.
3. Групповые политики домена.
4. Групповые политики организационного подразделения.
5. Групповые политики дочернего организационного подразделения.

Если настройки политики конфликтуют, приоритет имеют настройки политики, которые применялись позже — они перезаписывают более ранние настройки. Например, политики организационного подразделения имеют приоритет над другими групповыми политиками домена. Однако есть исключения для этих правил приоритета. Эти исключения рассматриваются в *разд. "Блокирование, переопределение и отключение политик" далее в этой главе.*

Когда применяются групповые политики?

Настройки групповой политики разделены на две категории:

- политики, применяемые к компьютерам;
- политики, применяемые к пользователям.

Политики компьютера обычно применяются во время запуска системы, а политики пользователя — во время входа в систему. Точная последовательность событий часто важна при поиске и устранении неисправностей поведения системы. События, возникающие во время запуска системы и при входе в систему, следующие:

1. Запускается сеть, и Windows Server применяет политики компьютера. По умолчанию политики компьютера применяются по одной в указанном ранее порядке. При обработке политик компьютера на экран не выводятся какие-либо сообщения, свидетельствующие об этом.
2. Windows Server выполняет загрузочные сценарии. По умолчанию загрузочные сценарии выполняются по одному: следующий сценарий запускается с небольшим тайм-аутом после завершения работы предыдущего сценария. О выполнении сценариев также ничего не сообщается пользователю, если не определено обратное.
3. Пользователь входит в систему. После проверки пользователя Windows Server загружает его профиль.
4. Windows Server применяет политики пользователя. По умолчанию пользовательские политики применены по одной в указанном ранее порядке. При обработке пользовательских политик интерфейс пользователя выводит соответствующие сообщения.
5. Windows Server выполняет сценарии входа в систему. По умолчанию сценарии входа в систему для групповой политики выполняются одновременно. О выполнении сценариев входа в систему пользователю ничего не сообщается, если не определено обратное. Сценарии из ресурса Netlogon выполняются последними в окне командного процессора.
6. Windows Server выводит на экран интерфейс оболочки, настроенный в групповой политике.

7. По умолчанию групповая политика обновляется, когда пользователь выходит из системы, во время перезапуска компьютера и автоматически каждые 90—120 минут. Можно изменить это поведение, устанавливая интервал обновления групповой политики *(см. разд. "Обновление групповой политики" далее в этой главе)*. Чтобы сделать это, откройте окно командной строки и введите команду `gpupdate`.

> ***Практический совет***
>
> Некоторые настройки пользователя, например перенаправление папок, не могут быть обновлены, пока пользователь зарегистрирован в системе. Пользователь должен выйти из системы и затем зайти заново для применения этих настроек. Для автоматического выхода пользователя из системы после обновления можно ввести команду `gpupdate /lofogg` в командной строке или в поле поиска. Аналогично, некоторые настройки компьютера могут быть определены только при его запуске. Для применения этих настроек компьютер должен быть перезагружен. Для этого можно ввести в командной строке или в поле поиска команду `gpupdate /boot`.

Требования групповой политики и совместимость версий

Групповые политики поддерживаются только профессиональными и серверными версиями Windows. Каждая новая версия Windows вносила свои изменения в групповую политику. Иногда эти изменения делают бессмысленными старые политики на более новых версиях Windows. В этом случае политика работает только в определенных версиях Windows, например в Windows XP Professional и Windows Server 2003.

Вообще говоря, большинство политик прямо совместимо. Это означает, что, как правило, политики, представленные в Windows Server 2003, могут использоваться на Windows 7 и более поздних версиях, а также на Windows Server 2008 и более поздних версиях. Это также означает, что политики для Windows 8 и Windows Server 2012 обычно не применимы к более ранним версиям Windows. Если политика не применима к определенной версии операционной системы Windows, нельзя применить ее на компьютерах, работающих под этими версиями Windows.

Как узнать, поддерживается ли политика на определенной версии Windows? Очень просто. Для каждой настройки политики в окне ее свойств есть поле **Поддерживается** (Supported On). В нем и описаны разные версии Windows, на которых эта политика будет работать. Окно свойств не нужно открывать, если в редакторе политики выбрана вкладка **Расширенный** (Extended) (а не вкладка **Стандартный** (Standard)). Слева от списка политик выводится запись **Требования** (Requirements), которая содержит сведения совместимости.

Также можно установить новые политики при добавлении пакета обновлений (Service Pack), установке приложений и компонентов Windows. Это означает, что будет виден широкий диапазон записей совместимости.

Изменение групповой политики

Чтобы оптимизировать управление групповой политикой, Microsoft удалила функции управления из инструментов Active Directory и переместила их в основную консоль — **Управление групповой политикой** (Group Policy Management Console, GPMC), которая впервые появилась в Windows Vista и Windows Server 2008. GPMC — это компонент, который можно добавить в любую установку Windows Server 2008 (или более позднюю версию)

с помощью мастера добавления ролей и компонентов. Консоль GPMC будет доступна в Windows Vista (и более поздних версиях), если установить Remote Server Administration Tools (RSAT). Как только консоль GPMC будет установлена, ее команда будет доступна в меню **Средства** в диспетчере серверов.

Если нужно отредактировать объект групповой политики в GPMC, консоль GPMC открывает редактор **Управление групповой политикой** (Group Policy Management Editor), который используется для управления настройками политики. Если бы Microsoft остановилась на этих двух инструментах, у нас была бы замечательная и простая в использовании среда управления политикой. К сожалению, на самом деле все не так, и существуют почти идентичные редакторы.

- **Редактор стартового объекта групповой политики** (Group Policy Starter GPO Editor) — редактор, который можно использовать для создания и управления стартовыми объектами групповой политики. Как подразумевает имя, стартовый GPO призван обеспечить начальную точку для объектов политики, которые используются всюду по своей организации. При создании объекта политики можно определить стартовый GPO как источник или фундамент объекта.
- **Редактор локальной групповой политики** (Local Group Policy Object Editor) — применяется для создания и управления объектами политики для локального компьютера. Как подразумевает имя, локальный GPO призван обеспечить настройки политики для определенного компьютера в противоположность настройкам для сайта, домена или организационного подразделения.

Пользователи, работавшие с более ранними версиями Windows, могут быть знакомы с редактором объекта групповой политики (Group Policy Object Editor, GPOE). В Windows Server 2003 и более ранних версиях Windows, GPOE — основной инструмент редактирования объектов политики. Редактор объекта групповой политики, Управление групповой политикой, Редактор стартового объекта групповой политики, Редактор локальной групповой политики — очень похожи за исключением набора объектов политики, к которым предоставляется доступ. По этой причине мы не будем специально различать их, если в этом нет особой необходимости. Автор данной книги предпочитает обращаться к этим инструментам "коллективно" и называет их *редакторами политик*. Иногда мы будем использовать акроним GPOE, чтобы явно отличить этот редактор от консоли управления GPMC.

Управлять настройками политики для Windows Vista (и более поздними версиями) можно только с компьютеров под управлением ОС Windows Vista или более поздней версии Windows. Причина заключается в том, что GPOE и GPMC для Vista используют новый формат административных шаблонов, основанный на XML — ADMX.

> ***Примечание***
>
> Нельзя использовать старые версии редакторов политик для работы с ADMX. Можно редактировать GPO на базе ADMX-файлов только на компьютере с Windows Vista или более поздними версиями.

У Microsoft было много причин для того, чтобы перейти на формат ADMX. Основные причины заключались в обеспечении большей гибкости и расширяемости. Поскольку ADMX-файлы создаются на языке XML, они строго структурированы и могут быть легко и быстро проанализированы во время инициализации. Это поможет улучшить производительность при обработке групповых политик при запуске, входе в систему, выходе из системы и фаз завершения работы, а также во время обновления политики. Также строгая структура ADMX-файлов помогает Microsoft в вопросах интернационализации.

ADMX-файлы делятся на две группы: с расширением admx (не зависят от языка) и с расширением adml (зависят от языка). Не связанный с языком файл (admx) описывает структуру категорий и параметров политики административных шаблонов, отображаемых в редакторе политик. В зависящих от языка файлах (adml) находятся локализованные фрагменты, отображаемые в редакторе политик. Каждый adml-файл представляет один язык, для которого требуется поддержка. Это позволяет просматривать и редактировать одни и те же политики одному пользователю, скажем, на английском языке, а другому — на испанском. Механизм, который определяет используемый язык, — это языковый пакет, установленный на компьютере.

На компьютерах с Windows Vista (и более поздними версиями) не связанные с языком файлы (admx) устанавливаются в каталог *%SystemRoot%*\PolicyDefinitions. В Windows 7 и 8, а также Windows Server 2008 R2 и Windows Server 2012 adml-файлы устанавливаются в папку *%SystemRoot%*\PolicyDefinitions\LanguageCulture. Каждая подпапка именуется в соответствии со стандартами ISO, например, EN-US для U.S. English.

При запуске редактора политики он автоматически читает admx-файлы из папок политик. Поэтому можно скопировать admx-файлы, которые нужно использовать, в папку политик, чтобы сделать их доступными при редактировании GPO. Если редактор политики запущен, необходимо его перезапустить, чтобы он считал файл или файлы.

В доменах admx-файлы могут храниться в центральном хранилище — в каталоге SYSVOL (*%SystemRoot%*\Sysvol\Domain\Policies). При использовании центрального хранилища административные шаблоны больше не хранятся в каждом GPO. Вместо этого в GPO находится только текущее состояние настройки, а admx-файлы хранятся централизованно. Это позволяет уменьшить используемое дисковое пространство, а также объем данных, тиражируемых всюду на предприятии. Более подробную информацию можно получить в *главе 2* книги "Windows Group Policy Administrator's Pocket Consultant" (Microsoft Press, 2009).

При использовании Windows Server 2008 или более старших версий серверы под управлением этой серверной ОС используют службу репликации распределенной файловой системы (DFS) для тиражирования групповой политики. При этом тиражируются лишь изменения в GPO, избавляя от необходимости тиражировать весь GPO после его изменения.

В отличие от Windows XP и Windows Server 2003, Windows Vista и более поздние версии используют клиентскую службу групповой политики, чтобы изолировать уведомление и обработку групповой политики от процесса входа в Windows. Отделение групповой политики от процесса входа в Windows уменьшает ресурсы, используемые для фоновой обработки политики. В результате увеличивается общая производительность и становится возможным применение новых файлов групповой политики как части процесса обновления без необходимости перезагрузки системы.

Компьютеры под управлением Windows Vista (или более поздних версий) не используют функциональность журналирования трассировки в Userenv.dll и вместо этого записывают сообщения о событиях групповой политики в журнал **Система** (System). Далее, вместо журнала Userenv используется операционный журнал групповой политики. В оснастке **Просмотр событий** можно получить доступ к операционному журналу так: **Журналы приложений и служб\Microsoft\Windows\GroupPolicy** (Applications And Services Logs\ Microsoft\Windows\GroupPolicy).

Компьютеры под управлением Windows Vista (и более поздних версий) используют службу NLA (Network Location Awareness) вместо протокола ICMP (Internet Control Message Protocol, ping). Благодаря NLA, компьютер знает тип сети, к которой он подключен, и может быстро реагировать на изменения состояния системы или конфигурации сети. Исполь-

зуя NLA, клиент групповой политики может определить состояние компьютера, состояние сети и доступность пропускной способности сети для определения медленного соединения.

Управление локальными групповыми политиками

Компьютеры под управлением Windows Vista и более поздних версий позволяют использовать несколько локальных GPO на одном компьютере (пока компьютер не является контроллером домена). Ранее у компьютеров был только один локальный GPO. Windows позволяет присваивать отдельный локальный GPO каждому локальному пользователю или типу пользователей. Это дает возможность сделать применение политики более гибким и поддерживает более широкий диапазон сценариев реализации.

Локальные объекты групповой политики

Когда компьютеры используются в автономной конфигурации, а не в конфигурации домена, можно обнаружить, что множественный локальный GPO полезен, поскольку больше не нужно явно отключать или удалять настройки, которые вмешиваются в управление компьютером перед выполнением административных задач. Вместо этого можно реализовать один локальный GPO для администраторов и другой локальный GPO для обычных пользователей. В конфигурации домена, однако, нельзя использовать множественный GPO. В доменах большинство компьютеров и пользователей уже имеют множественные GPO, примененные к ним, а добавление множественных локальных GPO сделает управление групповой политикой слишком запутанным.

Компьютеры под управлением Windows Vista и более поздних выпусков имеют три уровня локальных объектов групповой политики.

- **Локальная групповая политика** (Local Group Policy). Это только локальный GPO, позволяющий конфигурациям компьютера и пользователя применяться ко всем пользователям компьютера.
- **Административная и неадминистративная локальная групповая политика** (Administrators and Non-Administrators local Group Policy). Содержит только настройки конфигурации пользователя и применяется на основании того, является ли учетная запись членом локальной группы **Администраторы**.
- **Пользовательская локальная групповая политика** (User-specific local Group Policy). Содержит только конфигурацию пользователя и применяется к отдельным пользователям и группам.

Эти уровни локальных GPO обрабатываются в следующем порядке: локальная групповая политика, административная и неадминистративная локальная групповая политика и пользовательская групповая политика.

Поскольку доступные настройки пользовательской конфигурации одинаковы для всех локальных GPO, настройки в одном GPO могут конфликтовать с настройками в другом GPO. ОС Windows разрешает конфликты в настройках, перезаписывая любые предыдущие настройки настройками, считанными последними. Windows использует последнее установленное значение. Когда Windows разрешает конфликты, имеет значение только включенное/выключенное состояние настроек. Значение **Не задано** (Not Configured) не оказывает никакого эффекта на состояние настройки из предыдущего приложения политики. Чтобы

упростить администрирование домена, можно отключить обработку локальных GPO на компьютерах под управлением Windows Vista и более поздних версий, включив политику **Выключение обработки локальных объектов групповой политики** (Turn Off Local Group Policy Objects Processing) в GPO домена. Эта настройка находится в узле **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика** (Computer Configuration\ Administrative Templates\System\Group Policy) групповой политики.

Получение доступа к настройкам локальной политики верхнего уровня

На всех компьютерах под управлением текущих выпусков Windows есть локальный GPO, доступный для редактирования. Хотя на контроллере домена тоже есть локальный GPO, его настройки редактировать не нужно.

Самый быстрый способ получить доступ к локальному GPO компьютера — это ввести следующую команду в командной строке или поле поиска приложений:

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

> ***Примечание***
>
> Поскольку команде передаются дополнительные аргументы, команду в таком виде нельзя использовать в оболочке PowerShell. Чтобы выполнить ее в оболочке PowerShell, нужно заключить ее аргументы в одинарные кавычки и в таком виде передать команду, например: `gpedit.msc '/gpcomputer: "%ComputerName%"'`.

Эта команда запускает GPOE в консоли управления Microsoft (MMC), а в качестве цели выступает локальный компьютер. Здесь `"%ComputerName%"` — переменная окружения, содержащая имя локального компьютера. Она должна быть заключена в двойные кавычки, как показано выше. Для получения доступа к локальному GPO верхнего уровня удаленного компьютера введите следующую команду в командной строке или поле поиска приложений:

```
gpedit.msc /gpcomputer: "RemoteComputer"
```

Здесь `RemoteComputer` — имя или полное имя (FQDN) удаленного компьютера. Снова необходимо использовать двойные кавычки, как показано в следующем примере:

```
gpedit.msc /gpcomputer: "corpsvr82"
```

Также можно управлять локальным GPO верхнего уровня с помощью следующих действий:

1. В командной строке или поле поиска приложений введите `mmc`.
2. В консоли управления Microsoft (MMC) выберите команду **Файл | Добавить или удалить оснастку** (File | Add/Remove Snap-In).
3. В диалоговом окне **Добавление или удаление оснасток** (Add Or Remove Snap-Ins) выберите оснастку **Редактор объектов групповой политики** (Group Policy Object Editor) и нажмите кнопку **Добавить** (Add).
4. В окне **Выбор объекта групповой политики** (Select Group Policy Object) нажмите кнопку **Готово**, поскольку по умолчанию будет использоваться объект локального компьютера. Нажмите кнопку **OK**.

Теперь можно управлять локальными настройками политики (рис. 4.1).

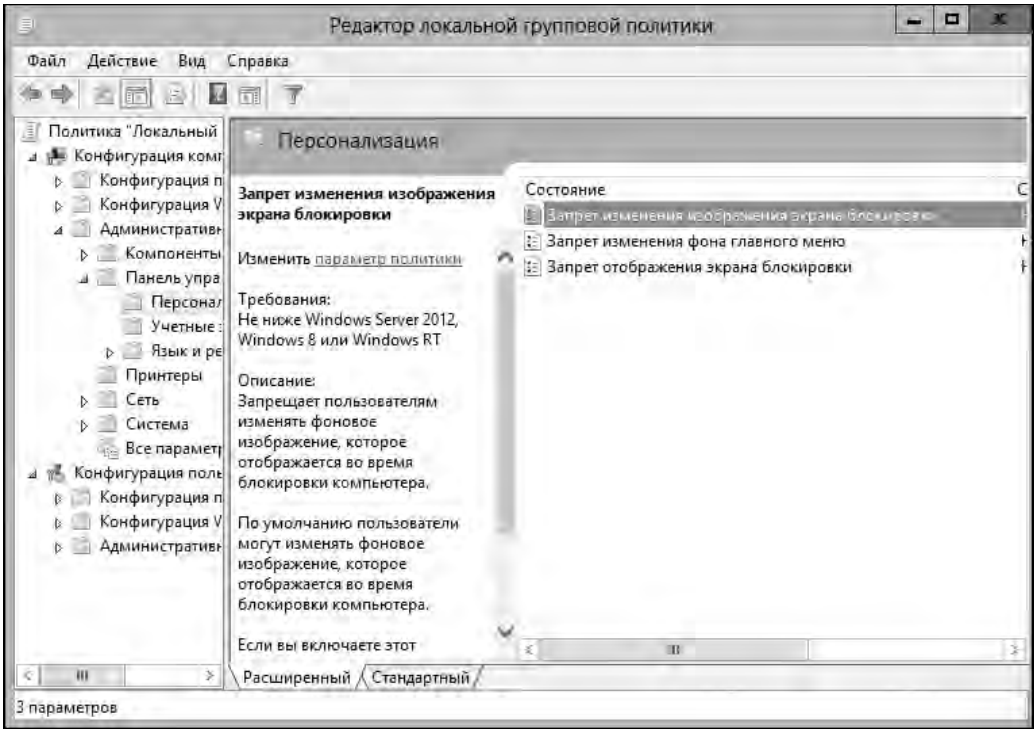


Рис. 4.1. Используйте редактор политики для управления настройками локальной политики

Совет

Можно использовать одну и ту же оснастку MMC для управления более чем одним локальным GPO. В диалоговом окне **Добавление или удаление оснасток** просто добавьте по одному экземпляру оснастки **Редактор объектов групповой политики** (Group Policy Object Editor) для каждого объекта, с которым нужно работать.

Настройки локального объекта групповой политики

Локальные групповые политики хранятся в папке *%SystemRoot%*\System32\GroupPolicy на каждом компьютере с Windows Server. В этой папке находятся следующие подпапки:

- Machine — содержит сценарии компьютера в папке Script и информацию политики на базе реестра для раздела `HKEY_LOCAL_MACHINE` (`HKLM`) в файле Registry.pol;
- User — хранит сценарии пользователя в папке Script и информацию политики на базе реестра для раздела `HKEY_CURRENT_USER` (`HKCU`) в файле Registry.pol.

Внимание!

Не нужно редактировать эти папки и файлы вручную! Вместо этого используйте соответствующие функции одной из утилит групповой политики. По умолчанию эти файлы и папки скрыты. Если нужно просмотреть скрытые файлы и папки в Проводнике Windows, перейдите на вкладку **Вид** (View) окна **Параметры папок** (Folder Options) и установите флажок **Показать или скрыть | Скрытые элементы** (Hidden Items). Также можно отметить флажок **Расширения имен файлов** (File Name Extensions). Открыть это окно можно, выбрав команду меню **Вид | Параметры**.

Получение доступа к административной и неадминистративной политике и пользовательской политике

По умолчанию единственный локальный объект политики, существующий на компьютере, является локальным объектом групповой политики. Можно создать и управлять другими объектами при необходимости (за исключением объектов на контроллерах доменов). Можно создать или получить доступ к административному объекту локальной групповой политики, к неадминистративному объекту локальной групповой политики и объекту пользовательской локальной групповой политики так:

1. В командной строке или в поле поиска приложений введите `mmc` и нажмите клавишу <Enter>. В консоли управления Microsoft выберите команду меню **Файл | Добавить или удалить оснастку**.
2. В диалоговом окне **Добавление или удаление оснасток** выберите оснастку **Редактор объектов групповой политики** и нажмите кнопку **Добавить**.
3. В окне **Выбор объекта групповой политики** нажмите кнопку **Обзор**. В окне **Поиск объекта групповой политики** (Browse For A Group Policy Object) перейдите на вкладку **Пользователи** (Users).
4. На вкладке **Пользователи** (Users) в колонке **Объект групповой политики существует** (Group Policy Object Exists) приводятся сведения о том, существует ли объект групповой политики для того или иного пользователя. Выполните следующие действия.
   - Выберите запись **Администраторы** (Administrators) для создания или получения доступа к объекту административной локальной групповой политики.
   - Выберите запись **Не администраторы** (Non-Administrators) для создания или получения доступа к объекту административной локальной групповой политики.
   - Выберите локального пользователя для создания или получения доступа к пользовательскому локальному GPO.
5. Нажмите кнопку **OK**. Если выбранный объект не существует, он будет создан. В противном случае будет открыт существующий объект для просмотра и редактирования.

Параметры политики для администраторов, неадминистраторов и пользователей хранятся в папке *%SystemRoot%*\System32\GroupPolicyUsers на каждом компьютере под управлением Windows Server. Поскольку эти локальные GPO применяются только к конфигурации пользователя, в папке *%SystemRoot%*\System32\GroupPolicyUsers находится подпапка User, а в ней будут сценарии в папке Script, а также информация реестра для раздела `HKEY_CURRENT_USER` в файле Registry.pol.

Управление политиками сайта, домена и организационного подразделения

При разворачивании сервисов Active Directory (AD DS) можно использовать групповую политику на базе Active Directory. Каждый сайт, домен и организационное подразделение могут иметь одну или больше групповых политик. У групповых политик, перечисленных выше в списке групповой политики, более высокий приоритет, чем у политик, перечисленных ниже в списке. Это позволяет удостовериться, что политики применены всюду по связанным сайтам, доменам и организационным подразделениям.

Политики домена и политики по умолчанию

У каждого домена в организации по умолчанию есть два GPO.

- **GPO политики контроллера домена по умолчанию** (Default Domain Controllers Policy GPO) создается и связывается для организационного подразделения контроллера домена. Этот GPO применим ко всем контроллерам домена в домене (до тех пор, пока они не будут перемещены из этого организационного подразделения). Используйте его для управления параметрами безопасности для контроллеров доменов в этом домене.
- **GPO политики домена по умолчанию** (Default Domain Policy GPO) создается и связывается для всего домена в пределах Active Directory. Используйте этот GPO для установки базовых значений для широкого круга настроек политик, которые применяются ко всем пользователям и компьютерам в домене.

Как правило, GPO политики домена по умолчанию — GPO высшего приоритета, связанный с уровнем домена. GPO политики контроллеров домена по умолчанию — GPO высшего приоритета, связанный с контейнером контроллеров домена. Можно присоединить дополнительные GPO уровня домена и контроллеров домена. При этом настройки в GPO наивысшего приоритета переопределяют настройки в объектах групповой политики более низкого приоритета. Эти GPO не предназначены для общего управления групповой политикой.

GPO политики домена по умолчанию используется только для управления настройками дефолтовых политик учетных записей, и, в частности, есть три области применения политик учетных записей: политика паролей, политика блокировки учетной записи и политика Kerberos. Через этот GPO можно управлять несколькими параметрами безопасности: **Учетные записи: Переименование учетной записи администратора** (Accounts: Rename Administrator Account), **Учетные записи: Состояние учетной записи 'Администратор'** (Accounts: Administrator Account Status), **Учетные записи: Состояние учетной записи 'Гость'** (Accounts: Guest Account Status), **Учетные записи: Переименование учетной записи гостя** (Accounts: Rename Guest Account), **Сетевая безопасность: Принудительный вывод из сеанса по истечению допустимых часов** (Network Security: Force Logoff When Logon Hours Expire), **Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля** (Network Security: Do Not Store LAN Manager Hash Value On Next Password Change).

Один из способов перезаписи этих настроек — создать GPO с соответствующими настройками и присоединить его к контроллеру домена с более высоким приоритетом.

Объект GPO политики контроллера домена по умолчанию содержит параметры **Назначение прав пользователя** (User Rights Assignment) и **Параметры безопасности** (Security Options), которые ограничивают способы использования контроллеров домена. Один из способов перезаписи этих настроек — создать GPO с перезаписывающимися настройками и присоединить его к контейнеру контроллеров домена с более высоким приоритетом.

Для управления другими областями политики нужно создать GPO и присоединить его к домену или соответствующему организационному подразделению в пределах домена.

Групповые политики сайта, домена и организационного подразделения хранятся в папке *%SystemRoot%*\Sysvol\Domain\Policies на контроллере домена. В этой папке находится по одной подпапке для каждой политики, определенной на контроллере домена. Имя папки политики — это уникальный глобальный идентификатор политики (GUID). Можно найти GUID политики на странице **Свойства** (Properties) вкладки **Общие** (General) раздела **Сводка** (Summary).

Внутри этих отдельных папок политик находятся следующие подпапки:

- Machine — содержит сценарии компьютера в папке Script и информацию реестра для раздела `HKEY_LOCAL_MACHINE` (`HKLM`) в файле Registry.pol;
- User — содержит сценарии пользователя в папке Script и информацию реестра для раздела `HKEY_CURRENT_USER` (`HKCU`) в файле Registry.pol.

> ***Внимание!***
>
> Не редактируйте эти папки и файлы вручную. Вместо этого используйте соответствующие компоненты одной из утилит управления групповой политикой.

Консоль управления групповой политикой

Запустить консоль управления групповой политикой (GPMC) можно из меню **Средства** (Tools) диспетчера серверов. Также можно в командной строке или в поле поиска приложений ввести `gpmc.msc` и нажать клавишу <Enter>.

Как показано на рис. 4.2, корневой узел консоли называется **Управление групповой политикой** (Group Policy Management), а ниже есть узел **Лес** (Forest). Узел **Лес** представляет лес, к которому консоль подключена в настоящий момент, и называется именем корневого домена этого леса (на рис. 4.2 — **Лес: HOME.DOMAIN**). Если существуют соответствующие учетные данные, можно добавить соединения с другими лесами. Для этого щелкните пра-

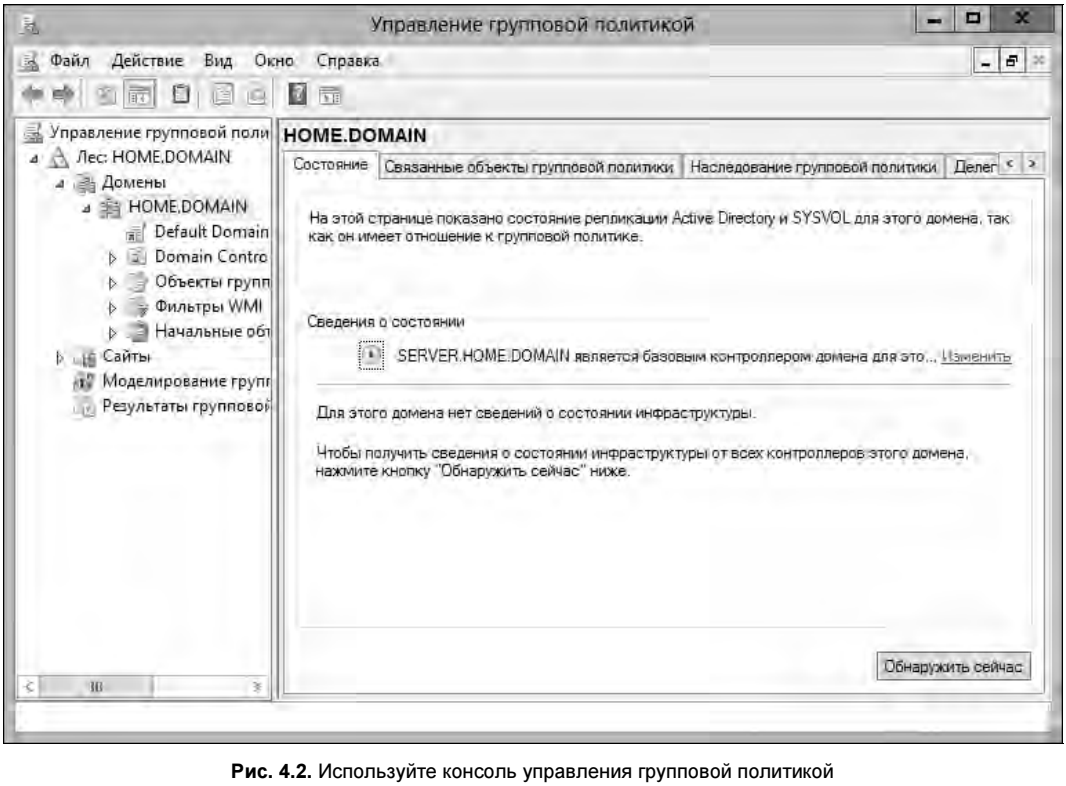


Рис. 4.2. Используйте консоль управления групповой политикой для работы с объектом групповой политики сайта, леса и домена

вой кнопкой мыши по узлу **Управление групповой политикой** и выберите команду **Добавить лес** (Add Forest). В диалоговом окне **Добавление леса** (Add Forest) введите имя корневого домена леса в поле **Домен** (Domain) и нажмите кнопку **OK**.

В узле **Лес** находятся следующие узлы.

- **Домены** (Domains) — предоставляет доступ к параметрам политики для доменов в соответствующем лесе. По умолчанию консоль подключена к домену входа в систему. Если есть другие учетные данные, можете добавить соединения с другими доменами в связанном лесу. Для этого щелкните правой кнопкой мыши по узлу **Домены** и выберите команду **Показать домены** (Show Domains). В окне **Отображение доменов** (Show Domains) выберите домены, которые нужно добавить, и нажмите кнопку **OK**.
- **Сайты** (Sites) — предоставляет доступ к настройкам политики для сайтов в соответствующем лесе. Сайты скрыты по умолчанию. Если есть соответствующие учетные данные, можно подключиться к сайтам. Для этого щелкните правой кнопкой мыши на узле **Сайты** и выберите команду **Показать сайты** (Show Sites). В окне **Отображение сайтов** (Show Sites) выберите сайты, которые нужно добавить, и нажмите кнопку **OK**.
- **Моделирование групповой политики** (Group Policy Modeling) — предоставляет доступ к мастеру моделирования групповой политики (Group Policy Modeling Wizard), который поможет спланировать развертывание групповой политики и симулировать настройки с целью тестирования. Также доступны любые сохраненные модели.
- **Результаты групповой политики** (Group Policy Results) — предоставляет доступ к мастеру результатов групповой политики (Group Policy Results Wizard). Для каждого домена, к которому подключена консоль, все связанные объекты групповой политики и организационные подразделения доступны для работы в одном месте.

Объекты GPO, перечисленные в контейнерах **Домены**, **Сайты** в GPMC, являются ссылками на GPO, а не самими GPO. Доступ к фактическому GPO можно получить через контейнер **Объекты групповой политики** (Group Policy Objects) выбранного домена. Обратите внимание на то, что у значков ссылок на GPO есть небольшие стрелки в левом нижнем углу, подобно ярлыку, а на значках самих GPO таких стрелок нет.

При запуске консоль GPMC подключится к Active Directory, запущенному на контроллере домена, который работает как PDC-эмулятор для домена входа и получает список всех объектов групповой политики и организационных подразделений в этом домене. Это возможно благодаря протоколам LDAP (Lightweight Directory Access Protocol) для доступа к хранилищу каталогов и SMB (Server Message Block) для доступа к каталогу SYSVOL. Если PDC-эмулятор недоступен по какой-то причине, например, когда сервер находится в режиме оффлайн, GPMC отобразит подсказку, чтобы можно было работать с настройками политик на любом другом доступном контроллере домена. Для смены контроллера домена щелкните правой кнопкой мыши на узле домена, для которого нужно сменить активный контроллер домена, затем выберите команду **Сменить контроллер домена** (Change Domain Controller). В окне **Смена контроллера домена** (Change Domain Controller) текущий контроллер домена приведен в области **Текущий контроллер домена** (Current Domain Controller). Используйте область **Изменить на** (Change To), выберите другой контроллер домена и нажмите кнопку **OK**.

Знакомство с редактором политик

С помощью консоли GPMC можно отредактировать GPO, щелкнув на нем правой кнопкой мыши и выбрав команду **Изменить** (Edit).

Как показано на рис. 4.3, у редактора политики есть два основных узла:

- **Конфигурация компьютера** (Computer Configuration) — разрешает использовать политики, которые будут применены к компьютерам, вне зависимости от того, какой пользователь вошел в систему;
- **Конфигурация пользователя** (User Configuration) — позволяет установить политики, которые будут применены к пользователям, вне зависимости от того, на каких компьютерах они входят в домен.

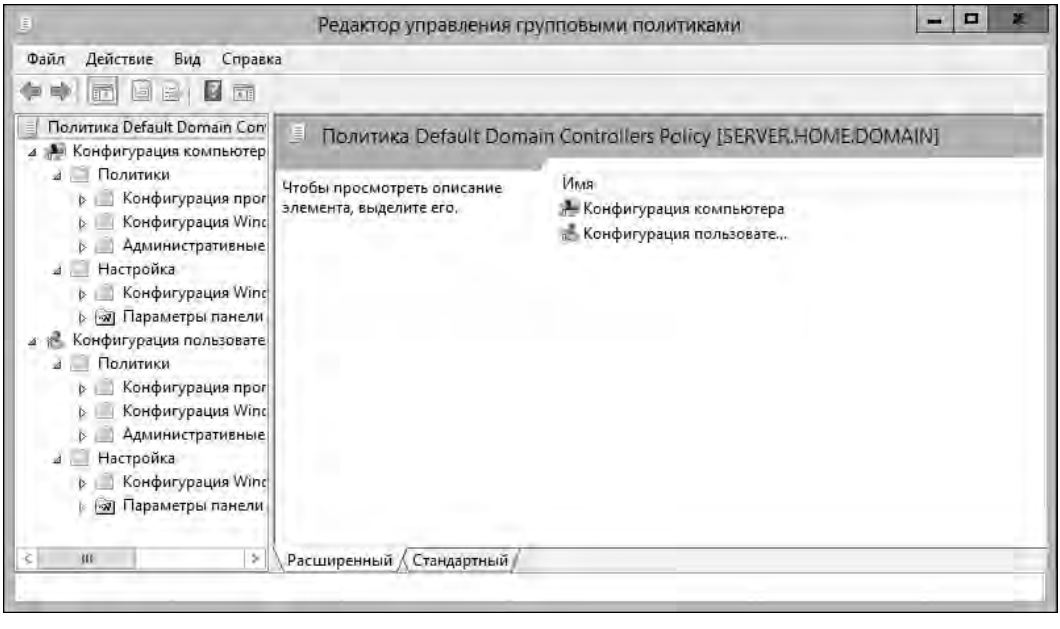


Рис. 4.3. Конфигурация редактора политики зависит от типа создаваемой политики и от установленных дополнений

В узлах **Конфигурация компьютера** и **Конфигурация пользователя** находятся узлы **Политики** (Policies) и **Настройки** (Preferences). Настройки общих политик находятся в узле **Политики**. Параметры общих настроек — в узле **Настройки**.

> ***Примечание***
>
> Когда автор этой книги ссылается на настройки в узле **Политики**, иногда используется сокращение **Конфигурация пользователя\Административные шаблоны\Компоненты Windows** (User Configuration\Administrative Templates\Windows Components) вместо **Конфигурация пользователя\Политики\Административные шаблоны** (User Configuration\Policies\Administrative Templates: Policy Definitions\Windows Components). То есть рассматриваемая политика находится в узле **Конфигурация пользователя** (User Configuration), а не в узле **Конфигурация компьютера** (Computer Configuration) и далее может быть найдена в узле **Административные шаблоны\Компоненты Windows** (Administrative Templates\Windows Components).

Точная конфигурация узлов **Конфигурация компьютера** (Computer Configuration) и **Конфигурация пользователя** (User Configuration) зависит от установленных расширений и типа созданной политики. В узлах **Конфигурация компьютера** и **Конфигурация пользователя** есть следующие подузлы:

- **Конфигурация программ** (Software Settings) — политики для настроек программного обеспечения. При установке программного обеспечения в узле **Конфигурация программ** появятся новые подузлы;
- **Конфигурация Windows** (Windows Settings) — набор политик для перенаправления папок, сценариев и безопасности;
- **Административные шаблоны** (Administrative Templates) — набор политик для операционной системы, компонентов Windows и программ. Административные шаблоны настраиваются с помощью файлов шаблонов. При необходимости можно добавить или удалить файлы шаблонов.

> ***Примечание***
>
> Полное обсуждение всех доступных параметров выходит за рамки этой книги. Разделы, которые призваны использоваться для перенаправления папок, административных шаблонов и сценариев, рассматриваются в *разд. "Управление сценариями пользователя и компьютера" далее в этой главе*. Безопасность будет обсуждаться в последующих главах этой книги.

Использование административных шаблонов для установки политик

Административные шаблоны предоставляют легкий доступ к настройкам реестра, которые можно изменить. Набор административных шаблонов по умолчанию настроен в редакторе политик для пользователей и компьютеров. При необходимости можно добавить/удалить административные шаблоны. Любые изменения, вносимые в политики, доступны через административные шаблоны, сохранены в реестре. Конфигурации компьютера хранятся в разделе `HKEY_LOCAL_MACHINE`, а конфигурации пользователя — в разделе `HKEY_CURRENT_USER`.

Просмотреть настроенные в данный момент шаблоны можно в узле **Административные шаблоны** редактора политик. Этот узел содержит политики, которые можно сконфигурировать для локальных систем, организационных подразделений, доменов и сайтов. В конфигурации пользователя и конфигурации компьютера находятся разные наборы групповой политики. При установке новых компонентов Windows можно добавить шаблоны с новыми политиками.

Административные шаблоны могут использоваться для управления следующими настройками:

- **Панель управления** (Control Panel) — содержит настройки Панели управления и ее утилит;
- **Рабочий стол** (Desktop) — настраивает рабочий стол Windows и доступные опции рабочего стола;
- **Сеть** (Network) — настраивает сеть и параметры сетевых клиентов для оффлайн-файлов, DNS-клиентов и сетевых соединений;
- **Принтеры** (Printers) — настраивает параметры принтера, просмотра сети, спула и каталога;
- **Общие папки** (Shared folders) — разрешает публикацию общих файлов и распределенной файловой системы (DFS);
- **Меню "Пуск" и панель задач** (Start screen and taskbar) — контролирует доступные опции и конфигурацию экрана **Пуск** и панели задач;

- **Система** (System) — настраивает параметры системы для дисковых квот, профилей пользователей, входа пользователя, восстановления системы, отчетов об ошибках и т. д.;
- **Компоненты Windows** (Windows components) — определяет доступные опции и конфигурацию различных Windows-компонентов, в том числе средства **Просмотр событий**, Internet Explorer, установщик Windows и обновления Windows.

Желаете узнать, какие административные шаблонные политики доступны? Просмотрите подузлы узла **Административные шаблоны**. Политики могут находиться в одном из трех состояний:

- **Не задано** (Not Configured) — политика не используется, и в реестр не записываются никакие значения;
- **Включено** (Enabled) — политика применена, ее значение сохранено в реестре;
- **Выключено** (Disabled) — политика выключена и не применяется, соответствующая настройка записана в реестре.

Для включения, выключения и настройки политики используются следующие действия:

1. В редакторе политик разверните узел **Конфигурация пользователя\Административные шаблоны** (User Configuration\ Administrative Templates) или **Конфигурация компьютера\Административные шаблоны** (Computer Configuration\Administrative Templates), в зависимости от типа политики, которую планируется использовать.
2. На панели слева выберите подпапку, содержащую политики, с которыми нужно работать. Соответствующие политики будут отображены на правой панели.
3. Дважды щелкните по политике, чтобы открыть окно **Свойства**. Описание политики можно прочитать на панели **Справка** (Help). Описание доступно, только если оно определено в соответствующем файле шаблона.
4. Чтобы установить состояние политики, выберите одну из опций:
   - **Не задано** (Not Configured) — политика не сконфигурирована;
   - **Включено** (Enabled) — политика включена;
   - **Выключено** (Disabled) — политика отключена.
5. Если политика включена, установите дополнительные параметры и нажмите кнопку **OK**.

> ***Примечание***
>
> Обычно в Windows Server у политик компьютера приоритет выше. Если есть конфликт между политикой компьютера и политикой пользователя, применяется политика компьютера.

Создание и связь объекта групповой политики

При работе с объектом политики создание и связь объекта со специфическим контейнером в пределах Active Directory — разные действия. Можно создать GPO и не соединять его ни с каким доменом, сайтом или организационным подразделением. Затем можно создать GPO и подсоединить его к определенному домену, сайту или организационному подразделению.

Также можно создать GPO и соединить его автоматически с доменом, сайтом или организационным подразделением. Выбранный метод зависит, прежде всего, от личных предпочтений и от того, как планируется работа с GPO. Имейте в виду, что при создании GPO и его соединении с доменом, сайтом, организационным подразделением, GPO будет применен

к объектам "пользователь" и "компьютер" в этом сайте, домене или организационном подразделении согласно параметрам Active Directory, порядку приоритета GPO и другим параметрам.

Для создания и подсоединения GPO к сайту, домену и организационному подразделению выполните следующие действия:

1. В консоли GPMC разверните узел леса, с которым нужно работать, а затем разверните соответствующий узел **Домены** и выберите нужный домен.
2. Щелкните правой кнопкой мыши на узле **Объекты групповой политики** (Group Policy Objects) и выберите команду **Создать** (New). В окне **Новый объект групповой политики** (New GPO) введите описывающее имя GPO, например, GPO безопасной рабочей станции. Если нужно использовать исходный GPO в качестве источника для начальных настроек, выберите исходный GPO из списка **Исходный объект групповой политики** (Source Starter GPO). После нажатия кнопки **OK** в контейнер **Объекты групповой политики** будет добавлен новый GPO.
3. Щелкните правой кнопкой мыши на созданном объекте и выберите команду **Изменить** (Edit). В редакторе политики установите необходимые параметры и закройте окно редактора политики.
4. В консоли GPMC выберите сайт, домен или организационное подразделение. Раскройте узел **Сайты**, если нужно работать с ним. На правой панели будет вкладка **Связанные объекты групповой политики** (Linked Group Policy Objects), которая показывает все GPO, связанные в данный момент с выбранным контейнером (если таковые есть).
5. Щелкните правой кнопкой мыши на сайте, домене или организационном подразделении, к которым нужно привязать GPO, а затем выберите команду **Связать существующий объект групповой политики** (Link An Existing GPO). В окне **Выбор объекта групповой политики** выберите GPO, который нужно связать, и нажмите кнопку **OK**. Когда групповая политика обновится для компьютеров и пользователей в выбранном сайте, домене или организационном подразделении, настройки политики в GPO будут применены.

Создать и связать GPO с помощью одной операции можно так:

1. В консоли GPMC щелкните правой кнопкой мыши на имени сайта, домена или организационного подразделения, к которым нужно привязать GPO, а затем выберите команду **Создать объект групповой политики для этого домена и связать его** (Create A GPO In This Domain, And Link It Here).
2. В окне **Новый объект групповой политики** введите описывающее имя GPO, например, GPO безопасной рабочей станции. Если нужно использовать исходный GPO в качестве источника для начальных настроек, выберите исходный GPO из списка **Исходный объект групповой политики**. После нажатия кнопки **OK** новый GPO будет добавлен в контейнер **Объекты групповой политики** и будет связан с ранее выбранным сайтом, доменом или организационным подразделением.
3. Щелкните правой кнопкой мыши (или нажмите) на новом GPO и выберите команду **Изменить**. В редакторе политики настройки задайте необходимые настройки и закройте редактор политики. Когда групповая политика обновится, будут применены настройки из GPO для сайта, домена или организационного подразделения.

Создание и использование исходных объектов групповой политики

При создании GPO в консоли GPMC в качестве базового объекта можно взять исходный GPO. Настройки из исходного GPO будут импортированы в новый GPO, что позволяет использовать исходный GPO для определения основных параметров конфигурации в новом GPO. В крупной организации нужно создать разные категории исходных объектов групповой политики на основе пользователей и компьютере, они будут использоваться на требуемой конфигурации безопасности.

Создать исходный GPO можно с помощью следующих действий:

1. В консоли GPMC разверните узел леса, затем с помощью двойного щелчка (или нажатия) разверните нужный подузел узла **Домены**.
2. Щелкните правой кнопкой мыши по узлу **Начальные объекты групповой политики** (Starter GPOs), затем выберите команду **Создать**. В окне **Новый стартовый объект групповой политики** введите описательное имя для GPO, например, General Management User GPO (имя может быть любым). Можно также ввести комментарии, описывающие назначение GPO. Нажмите кнопку **OK**.
3. Щелкните правой кнопкой мыши по новому GPO и затем выберите команду **Изменить**. В редакторе групповой политики настройте необходимые параметры и закройте окно редактора.

Делегирование полномочий для управления групповой политикой

В Active Directory все администраторы имеют некоторый уровень привилегий для осуществления задач управления групповой политикой. С помощью делегации можно предоставить другим пользователям полномочия, чтобы они могли выполнить любые из следующих задач:

- создание GPO и управление созданными GPO;
- настройка представления, изменение настроек, удаление GPO и изменение безопасности;
- управление ссылками на существующие GPO или генерирование RSoP (Resultant Set of Policy).

В Active Directory администраторы могут создавать GPO, и любой создавший GPO имеет право управлять им. В GPMC можно определить, кто может создавать GPO в домене, выбрав узел **Объекты групповой политики домена** (Group Policy Objects) и перейдя на вкладку **Делегирование** (Delegation). На этой вкладке отображается список групп и пользователей, которые могут создавать GPO в домене. Для предоставления разрешения на создание GPO пользователю или группе нажмите кнопку **Добавить**. В окне **Выбор: "Пользователь", "Компьютер" или "Группа"** (Select User, Computer, Or Group) выберите пользователя или группу и затем нажмите кнопку **OK**.

В GPMC есть несколько способов определить, кто имеет разрешение на управление групповой политикой. Для домена, сайта и организационного подразделения выберите домен/сайт/организационное подразделение, а затем активизируйте вкладку **Делегирование** на правой панели (рис. 4.4). В раскрывающемся списке **Разрешение** (Permission) выберите разрешение, которое нужно проверить.

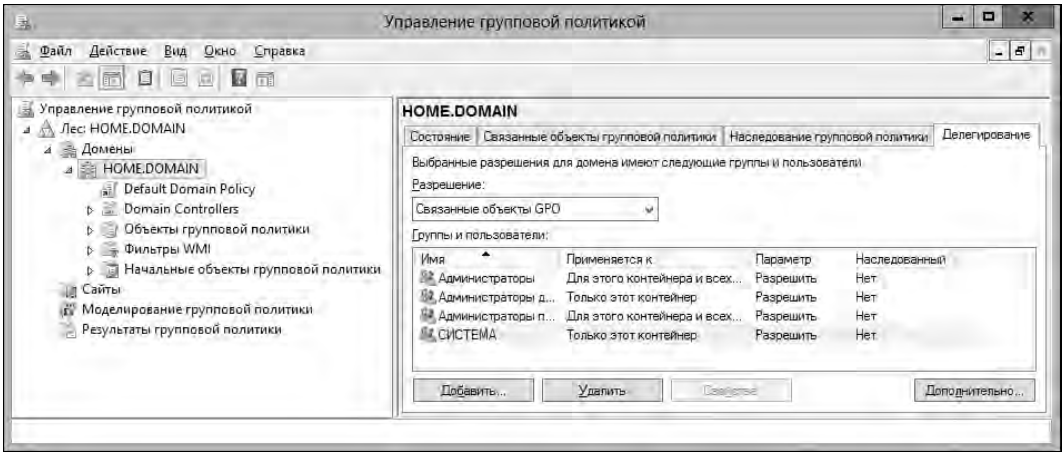


Рис. 4.4. Просмотр разрешений для управления групповой политикой

Доступны следующие опции:

- **Связанные объекты GPO** (Link GPOs) — выводит перечень пользователей и групп, которые могут создавать и управлять ссылками на GPO в выбранном сайте, домене или организационном подразделении;
- **Анализ моделирования групповой политики** (Perform Group Policy Modeling Analyses) — выводит перечень пользователей и групп, которые могут определять RSoP в целях планирования;
- **Чтение результирующих данных групповой политики** (Read Group Policy Results Data) — выводит перечень пользователей и групп, которые могут определять текущий RSoP для проверки или протоколирования.

Для предоставления разрешений домену, сайту или организационному подразделению выполните следующие действия:

1. В консоли GPMC выберите домен, сайт или организационное подразделение, с которым планируется работать, а затем перейдите на вкладку **Делегирование** на правой панели.
2. В раскрывающемся списке **Разрешения** выберите разрешение, которое нужно предоставить.
3. Нажмите кнопку **Добавить**. В окне **Выбор: "Пользователь", "Компьютер" или "Группа"** выберите пользователи или группу и нажмите кнопку **OK**.
4. В окне **Добавление группы или пользователя** (Add Group Or User) укажите, как должны применяться разрешения. Для применения разрешений к текущему контейнеру и всем его текущим контейнерам установите переключатель **Для этого контейнера и всех дочерних контейнеров** (This Container And All Child Containers). Для применения разрешений только к этому контейнеру установите переключатель **Только этот контейнер** (This Container Only). Нажмите кнопку **OK**.

Для отдельных разрешений GPO выберите GPO в консоли GPMC, а затем перейдите на вкладку **Делегирование** на правой панели. Далее выберите одно или несколько разрешений для отдельных пользователей и групп:

- **Чтение** (Read) — указывает, что пользователь или группа может просматривать объекты групповых политик и их настроек;

- **Изменение параметров** (Edit Settings) — указывает, что пользователь или группа могут просматривать GPO и изменять его настройки. Пользователь или группа не могут удалить GPO или изменить его параметры безопасности;
- **Изменение параметров, удаление и изменение параметров безопасности** (Edit Settings, Delete, Modify Security) — пользователь или группа могут просматривать GPO и изменять его настройки. Также пользователь или группа могут удалить GPO и параметры безопасности.

Чтобы предоставить разрешения для работы с GPO, выполните следующие действия:

1. В консоли GPMC выберите GPO, с которым нужно работать, а затем перейдите на вкладку **Делегирование** на правой панели. Нажмите кнопку **Добавить** (Add).
2. Для предоставления разрешений GPO пользователю или группе нажмите кнопку **Добавить** (Add). В окне **Выбор: "Пользователь", "Компьютер" или "Группа"** (Select User, Computer, Or Group) выберите пользователи или группу и нажмите кнопку **OK**.
3. В окне **Добавление группы или пользователя** (Add Group Or User) выберите уровень разрешений и нажмите кнопку **OK**.

Блокирование, переопределение и отключение политик

Наследование гарантирует, что каждый объект компьютера и пользователя в домене, сайте или организационном подразделении будет затронут групповой политикой. У большинства политик есть три параметра конфигурации: **Не задано** (Not Configured), **Включено** (Enabled), **Отключено** (Disabled). Состояние **Не задано** является состоянием по умолчанию для большинства настроек политики. Если политика включена, она применяется непосредственно или посредством наследования ко всем пользователям или компьютерам, которые относятся к политике. Если политика выключена, она не применяется.

Можно изменить способ наследования четырьмя способами:

- изменением порядка ссылки и приоритета;
- переопределением наследования;
- блокированием наследования (чтобы полностью предотвратить наследование);
- принудительным наследованием (чтобы заменить и предотвратить переопределение или блокирование).

Для групповой политики порядок наследования — от уровня сайта до уровня домена, а затем — по каждому уровню организационного подразделения. Помните следующее.

- Когда несколько объектов соединено с определенным уровнем, порядок ссылки определяет порядок применения настроек политики. Сначала применяются политики с низким значением приоритета, затем обрабатываются объекты политики с более высоким рангом. Приоритет — у последнего обработанного объекта политики, поэтому любая настройка политики, созданная в этом объекте политики, будет последней и перезапишет настройки, определенные во всех предыдущих объектах политики (за исключением, если не будет заблокировано наследование или не будет использоваться принудительное наследование).
- Когда несколько объектов политики наследуются от более высокого уровня, порядок приоритета точно показывает, как будут обрабатываться объекты политики. Как и с порядком ссылки, объекты с младшим рангом будут обработаны перед объектами с более высоким рангом. Наивысший приоритет — у последнего обработанного объекта поли-

тики, поэтому любая настройка политики, созданная в этом объекте политики, будет последней и перезапишет настройки, определенные во всех предыдущих объектах политики (если не будет заблокировано наследование или не будет использоваться принудительное наследование).

Когда несколько объектов политики связано с определенным уровнем, можно изменить порядок ссылки так:

1. В консоли GPMC выберите контейнер для сайта, домена или организационного подразделения, с которыми нужно работать.
2. На панели справа активизируйте вкладку **Связанные объекты групповой политики** (Linked Group Policy Objects) (рис. 4.5). Выберите объект политики, с которым нужно работать.

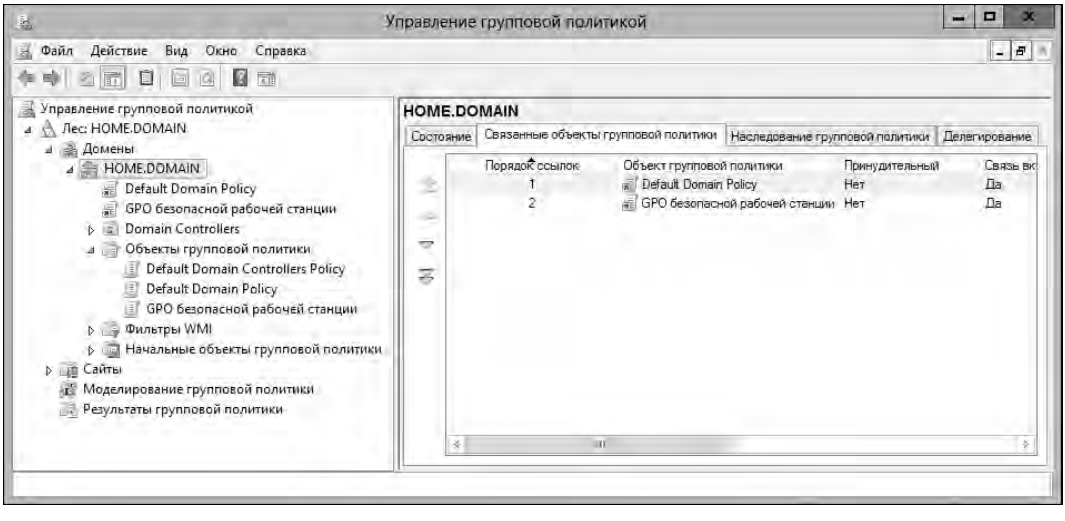


Рис. 4.5. Измените порядок ссылки для изменения порядка обработки и приоритета

3. Нажмите кнопку **Переместить связь вверх** (Move Link Up) или **Переместить связь вниз** (Move Link Down) для изменения порядка ссылки выбранного объекта политики.
4. После того как порядок ссылок будет изменен, проверьте, что объекты политики обрабатываются в ожидаемом порядке, это можно сделать на вкладке **Наследование групповой политики** (Group Policy Inheritance).

Переопределение наследования является основным методом изменения работы наследования. Когда политика включена в высокоуровневом объекте политики, переопределите наследование, отключив политику в объекте политики низшего уровня. Когда политика отключена в высокоуровневом объекте политики, можно переопределить наследование, включив политику в объекте политики низшего уровня. Пока политика не блокирована или не применяется принудительно, этот метод работает так, как нужно.

Иногда необходимо блокировать наследование так, чтобы никакие настройки политики от контейнеров более высокого уровня не были применены к пользователям и компьютерам в определенном контейнере. Когда наследование заблокировано, будут применены только сконфигурированные настройки политики от объектов политики, связанных с этим уровнем (пока нет принудительного применения политики).

Администраторы домена могут использовать блокирование наследования для блокирования настроек политики от уровня сайта. Администраторы организационных подразделений могут использовать блокирование наследования для блокирования настроек политики от уровня сайта или домена. С помощью блокирования можно обеспечить автономность домена или организационного подразделения, а также убедиться, что администраторы домена или организационного подразделения полностью контролируют политики, которые применяются к пользователям и компьютерам, администрируемым ими.

Для блокирования наследования выполните следующие действия: щелкните правой кнопкой мыши на домене или организационном подразделении, которые не должны наследовать настройки от высокоуровневых контейнеров, и выберите команду **Блокировать наследование** (Block Inheritance). Если эта команда уже выбрана, для отмены блокирования выберите ее еще раз. Когда наследование блокировано, в GPMC добавляется голубой кружок с восклицательным знаком к значку контейнера, для которого блокируется наследование. Такой значок позволяет быстро понять, блокируется ли наследование для домена/организационного подразделения или нет.

Чтобы администраторы других контейнеров не переопределяли и не блокировали настройки групповой политики, можно использовать принудительное наследование. Когда используется принудительное наследование, все сконфигурированные настройки политики из объектов политики более высокого уровня будут применены независимо от того, что определено в объектах более низкого уровня. Таким образом, блокирование наследования позволяет запретить переопределение или блокирование настроек политики.

Администраторы леса могут использовать принудительное наследование, чтобы убедиться, что настроенные параметры политики уровня сайта будут применены и не будут блокироваться или переопределяться администраторами домена или организационного подразделения. Администраторы домена могут использовать принудительное наследование, чтобы убедиться, что настроенные параметры политики уровня домена будут применены и не будут блокироваться или переопределяться администраторами организационного подразделения.

Используя консоль GPMC, можно принудительно применить наследование так: разверните контейнер высокого уровня, от которого начнется наследование, щелкните правой кнопкой мыши на GPO и выберите команду **Принудительный** (Enforced). Например, если нужно убедиться, что GPO уровня домена будет наследован всеми организационными подразделениями домена, разверните контейнер домена, щелкните правой кнопкой мыши на GPO контейнера и выберите команду **Принудительный**. Если команда уже выбрана, выберите ее снова для отмены принудительного наследования. В GPMC можно легко определить, какой GPO наследуется принудительно — к его значку будет добавлено изображение замка́. Также легко можно определить, какие политики вообще наследуются, а какие политики наследуются принудительно. Выберите объект политики в консоли GPMC и затем просмотрите вкладку **Область** (Scope) на правой панели. Если политика принудительная, в колонке **Принудительный** области **Связи** (Links) будет значение **Да** (Yes), как показано на рис. 4.6.

После того как объект политики будет выбран, можно щелкнуть правой кнопкой мыши на записи в колонке **Размещение** (Location) вкладки **Область** (Scope) для отображения контекстного меню, позволяющего управлять связями и принудительным наследованием. Включить или выключить связь можно включением/выключением команды **Связь включена** (Link Enabled). Включить/выключить принудительный режим наследования можно включением/выключением команды **Принудительный** (Enforced).

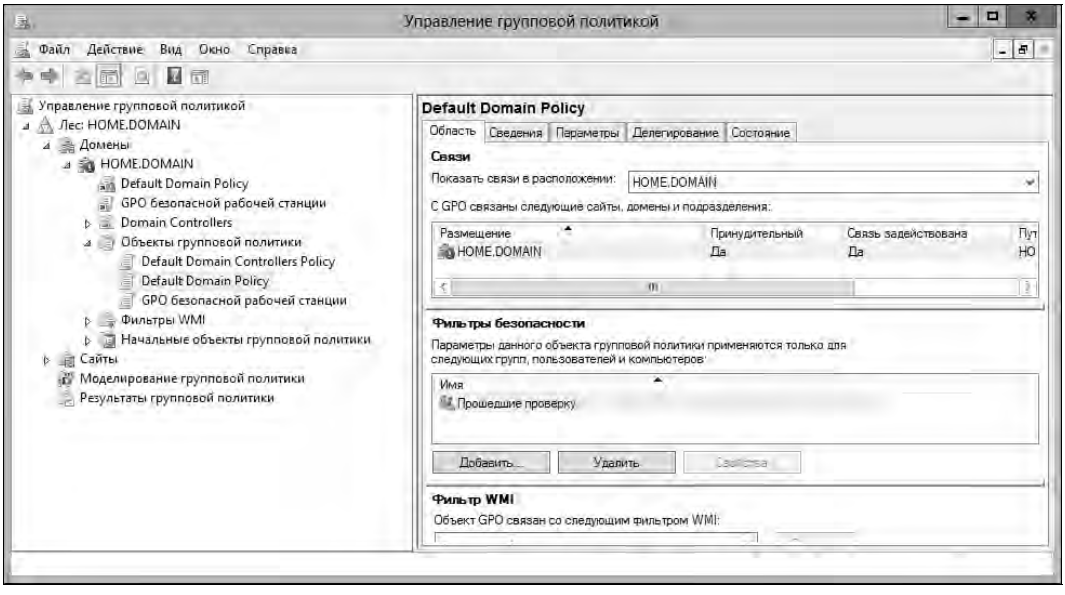


Рис. 4.6. Принудительный режим используется для того, чтобы можно было убедиться в применении настроек политики

Обслуживание, поиск и устранение неисправностей групповой политики

Групповая политика — широкая область администрирования, требующая внимательного управления. Как любая другая область администрирования, групповая политика предполагает осторожное обслуживание, чтобы можно было гарантировать ее надлежащее функционирование. Администратор должен диагностировать и решать любые возникающие проблемы. Чтобы диагностировать групповую политику, необходимо четко понимать, как политика обновляется и обрабатывается. Также нужно четко понимать задачи общего техобслуживания и поиска/устранения неисправностей.

Обновление групповой политики

При внесении изменения в политику эти изменения применяются немедленно. Однако они не распространяются автоматически. Клиентские компьютеры запрашивают политики в следующих случаях:

- при запуске компьютера;
- при входе пользователя;
- когда приложение или пользователь запрашивает обновления;
- когда истекает интервал обновления групповой политики, установленный для нее.

Настройки конфигурации компьютера применяются во время запуска операционной системы. Настройки конфигурации пользователя — при входе пользователя в систему. Если произошел конфликт между настройками пользователя и компьютера, у конфигурации компьютера более высокий приоритет, и именно ее настройки будут применены.

Как только настройки политики будут применены, настройки будут обновлены автоматически, чтобы можно было гарантировать, что они являются текущими. По умолчанию интервал обновления для контроллеров домена — 5 минут. Для других компьютеров интервал обновления — 90 минут с 30-минутными вариациями, чтобы избежать перегрузки контроллера домена многочисленными параллельными запросами клиентов. Это означает, что актуальный временной промежуток обновления для компьютеров, не являющихся контроллерами домена, составляет 90—120 минут.

Во время обновления групповой политики клиентский компьютер обращается к доступному контроллеру домена в его локальном сайте. Если есть изменения в одном или более объекте политики в домене, контроллер домена предоставляет список объектов политики, которые применяются к компьютеру и к пользователям, которые в данный момент вошли в систему. Контроллер домена делает это независимо от того, изменились ли номера версий на всех перечисленных объектах политики. По умолчанию компьютер обрабатывает объекты политики, только если изменился номер версии по крайней мере одного из объектов политики. Если какая-то из связанных политик изменилась, все политики должны быть обработаны снова из-за наследования и взаимозависимостей между политиками.

Настройки безопасности — известное исключение к правилу обработки. По умолчанию эти настройки обновляются каждые 16 часов (960 минут) независимо от того, содержат ли объекты политики изменения. Чтобы уменьшить влияние на контроллеры домена и сеть, во время обновлений добавляется случайное смещение до 30 минут (эффективное окно обновления 960—990 минут). Кроме того, если клиентский компьютер обнаруживает, что подключается по медленному сетевому соединению, он сообщает об этом контроллеру домена, и по сети передаются только настройки безопасности и административные шаблоны. Это означает, когда компьютер работает по медленному соединению, будут применены лишь настройки безопасности и административные шаблоны. Можно настроить способ обнаружения медленного соединения.

Необходимо тщательно сбалансировать частоту обновления политики с учетом частоты ее изменения. Если политика изменяется редко, можно увеличить окно обновления, чтобы уменьшить использование ресурсов. Например, можно установить интервал обновления 20 минут на контроллерах домена и 180 минут на других компьютерах.

Настройка интервала обновления

Интервал обновления групповой политики для каждого объекта политики можно настроить индивидуально. Для установки интервала обновления для контроллеров домена выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте групповой политики, который нужно изменить, и выберите команду **Изменить**. Этот GPO должен быть связан с контейнером, который содержит объекты компьютеров контроллера домена.
2. В узле **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика** дважды щелкните на политике **Установить интервал обновления групповой политики для контроллеров домена** (Set Group Policy Refresh Interval For Domain Controllers). В результате будет отображено окно **Свойства** (рис. 4.7).
3. Включите политику, выбрав переключатель **Включено** (Enabled). Установите базовый интервал обновлений в первом поле **Мин** (Minutes). Обычно интервал обновления устанавливают от 5 до 59 минут.
4. Во втором поле **Мин** (Minutes) установите случайную величину времени, которая будет добавлена к интервалу обновления. Эта случайная величина создает окно обновления,

что препятствует перегрузке сервера при многочисленных параллельных запросах групповой политики клиентами. Нажмите кнопку **OK**.

Примечание

Чем чаще обновляется политика, тем актуальнее конфигурация политики у компьютера. Чем реже обновляется политика, тем меньше используется системных ресурсов контроллера домена и сети, но в то же время у компьютера не будет самой актуальной конфигурации политики.

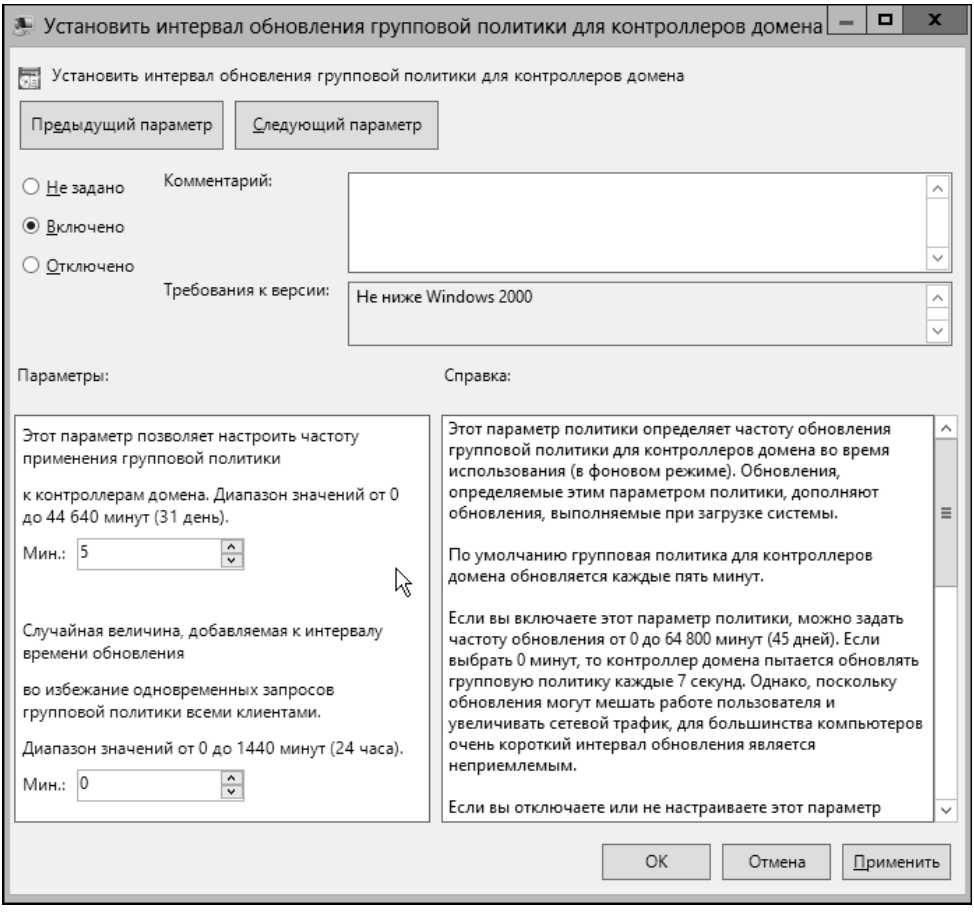


Рис. 4.7. Настраиваем интервал обновления групповой политики

Для установки интервала обновления для рабочих станций выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте групповой политики, который нужно изменить, и выберите команду **Изменить**. Этот GPO должен быть связан с контейнером, который содержит объекты компьютеров контроллера домена.
2. В узле **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика** дважды щелкните на политике **Установить интервал обновления групповой политики для компьютеров** (Set Group Policy Refresh Interval For Computers). В результате будет отображено окно **Свойства** (см. рис. 4.7).

3. Включите политику, отметив переключатель **Включено** (Enabled). Установите базовый интервал обновлений в первом поле **Мин** (Minutes). Обычно интервал обновления устанавливают от 60 до 240 минут.
4. Во втором поле **Мин** (Minutes) установите случайную величину времени, которая будет добавлена к интервалу обновления. Эта случайная величина создает окно обновления, что препятствует перегрузке сервера при многочисленных параллельных запросах групповой политики клиентами. Нажмите кнопку **OK**.

> ***Практический совет***
>
> Убедитесь, что обновления не происходят слишком часто и в то же время достаточно своевременны, чтобы оправдать ожидания и соответствовать требованиям. Чем чаще обновляется политика, тем больше сетевого трафика генерируется. В большой сети обычно нужно установить больший интервал обновления, чтобы уменьшить сетевой трафик, особенно когда политика затрагивает сотни пользователей или компьютеров. Если пользователи жалуются на периодическое снижение производительности своих компьютеров, также нужно увеличить интервал обновления. Рассмотрите обновления раз в день или даже раз в неделю, чтобы сохранить политики достаточно актуальными и в то же время соответствующими потребностям организации.
>
> Вам, как администратору, возможно, понадобится обновить групповую политику вручную. Например, если нет желания ждать, пока автоматически произойдет обновление или нужно решить проблему с обновлением. Вызвать обновление групповой политики вручную можно командой `gpupdate`.

Инициировать обновление можно несколькими способами. Можно ввести команду `gpupdate` в командной строке или в поле поиска приложений, в результате будут обновлены и конфигурация компьютера, и конфигурация пользователя на локальном компьютере. Будут обработаны и применены только измененные настройки политики. Для обновления всех настроек политики нужно использовать параметр `/Force`.

Также можно обновлять конфигурации пользователя и компьютера раздельно. Для обновления только конфигурации компьютера введите `gpupdate /target:computer` в командной строке. Для обновления только конфигурации пользователя предназначена другая команда — `gpupdate /target:user`.

Также можно использовать команду `gpupdate` для выхода пользователя или перезапуска компьютера после обновления групповой политики. Это полезно, поскольку некоторые политики могут быть применены лишь тогда, когда пользователь входит в систему или только при запуске компьютера. Для выхода пользователя после обновления добавьте параметр `/Logoff`, а для перезапуска компьютера после обновления — параметр `/Boot`.

Моделирование групповой политики для планирования

Моделирование групповой политики для планирования полезно, когда нужно протестировать различные реализации и сценарии конфигурации. Например, можно смоделировать эффект петлевой обработки или обнаружения медленного соединения. Также можно смоделировать эффект перемещения пользователей или компьютеров в другой контейнер в Active Directory или эффект изменения состава группы безопасности для пользователей и компьютеров.

У всех администраторов домена и предприятия есть разрешение моделировать групповую политику для планирования, также доступ к планированию есть у всех, кто обладает разрешением **Анализ моделирования групповой политики** (Perform Group Policy Modeling

Analyses). Для моделирования групповой политики и тестирования различных сценариев реализации и обновления выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши по узлу **Моделирование групповой политики** (Group Policy Modeling), выберите команду **Мастер моделирования групповой политики** (Group Policy Modeling Wizard), а затем нажмите кнопку **Далее**.
2. На странице **Выбор контроллера домена** (Domain Controller Selection) из списка **Контроллеры домена в этом домене** (Show Domain Controllers) выберите контроллер домена, который нужно моделировать. По умолчанию политика моделируется на любом доступном контроллере домена в выбранном домене. Если необходимо использовать определенный контроллер домена, установите переключатель **Указанный контроллер домена** (This Domain Controller). Затем выберите нужный контроллер домена и нажмите кнопку **Далее**.
3. На странице **Выбор компьютера и пользователя** (User And Computer Selection) можно выбрать контейнеры или отдельные учетные записи (рис. 4.8). Используйте один из двух методов выбора учетных записей и затем нажмите кнопку **Далее**.
   - Используйте контейнеры для имитации изменений для всего организационного подразделения или других контейнеров. В группе **Сведения о пользователе** (User Information) установите переключатель **Контейнер** (Container) и нажмите кнопку **Обзор**. Появится окно **Выбор контейнера пользователя** (Choose User Container). Используйте его для выбора любых доступных контейнеров пользователей в выбранном домене. В группе **Сведения о компьютере** (Computer Information) установите переключатель **Контейнер** (Container) и нажмите кнопку **Обзор**. В появившемся диалоговом окне **Выбор контейнера компьютера** (Choose Computer Container) выберите любой доступный контейнер компьютера в текущем домене.

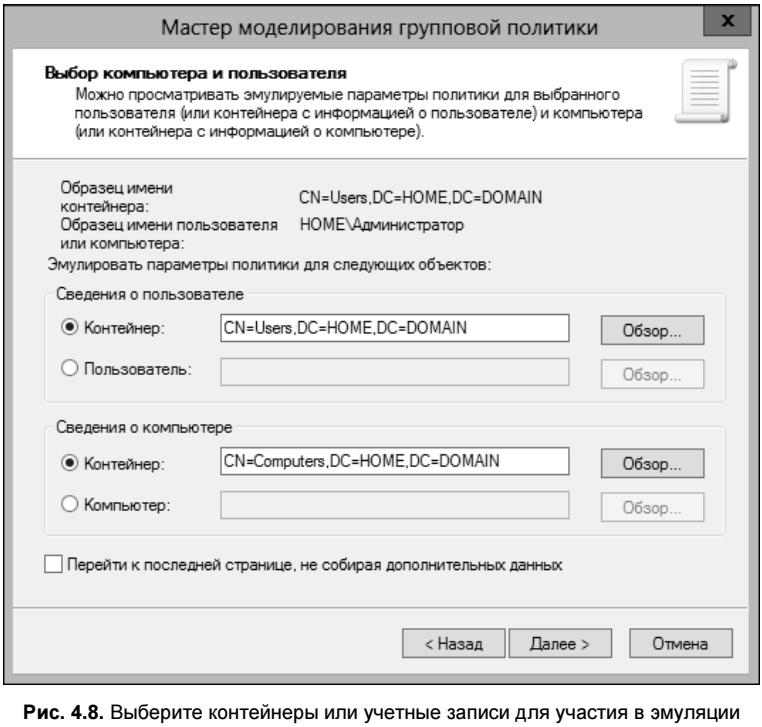


Рис. 4.8. Выберите контейнеры или учетные записи для участия в эмуляции

- Выберите определенные учетные записи для имитации изменений для отдельного пользователя и компьютера. В группе **Сведения о пользователе** установите переключатель **Пользователь** (User), затем нажмите кнопку **Обзор** и в окне **Выбор: "Пользователь"** (Select User) выберите учетную запись пользователя. В группе **Сведения о компьютере** установите переключатель **Компьютер** (Computer), нажмите кнопку **Обзор** и в окне **Выбор: "Компьютер"** (Select Computer) выберите учетную запись компьютера.

4. На странице **Дополнительные параметры эмуляции** (Advanced Simulation Options) выберите любые дополнительные параметры, например **Медленное сетевое подключение** (Slow Network Connections) или **Обработка петлевого адреса** (Loopback Processing), **Сайт** (Site), если это необходимо, и нажмите кнопку **Далее**.
5. На странице **Группы безопасности пользователя** (User Security Groups) можно эмулировать изменения в составе группы безопасности для одного или нескольких пользователей. Любые изменения, вносимые в состав группы, влияют на ранее выбранного пользователя или контейнер пользователя. Например, если нужно увидеть, что произойдет, если пользователь в контейнере пользователей — член группы **CorpManagers**, добавьте эту группу в список **Группы безопасности** (Security Groups) и нажмите кнопку **Далее**.
6. На странице **Группы безопасности компьютера** (Computer Security Groups) можно эмулировать изменения в составе группы безопасности для компьютера или компьютеров. Любые изменения, вносимые в состав группы, влияют на ранее выбранный компьютер или контейнер компьютеров. Например, если нужно увидеть, что произойдет, если компьютер в выбранном контейнере — член группы **RemoteComputers**, добавьте эту группу в список **Группы безопасности** и нажмите кнопку **Далее**.
7. Можно связать **Фильтры WMI** (Windows Management Instrumentation) с объектами групповой политики. По умолчанию предполагается, что выбранные пользователи и компьютеры соответствуют всем требованиям WMI-фильтра, который в большинстве случаев подходит для планирования. Нажмите кнопку **Далее** дважды, чтобы принять параметры по умолчанию.

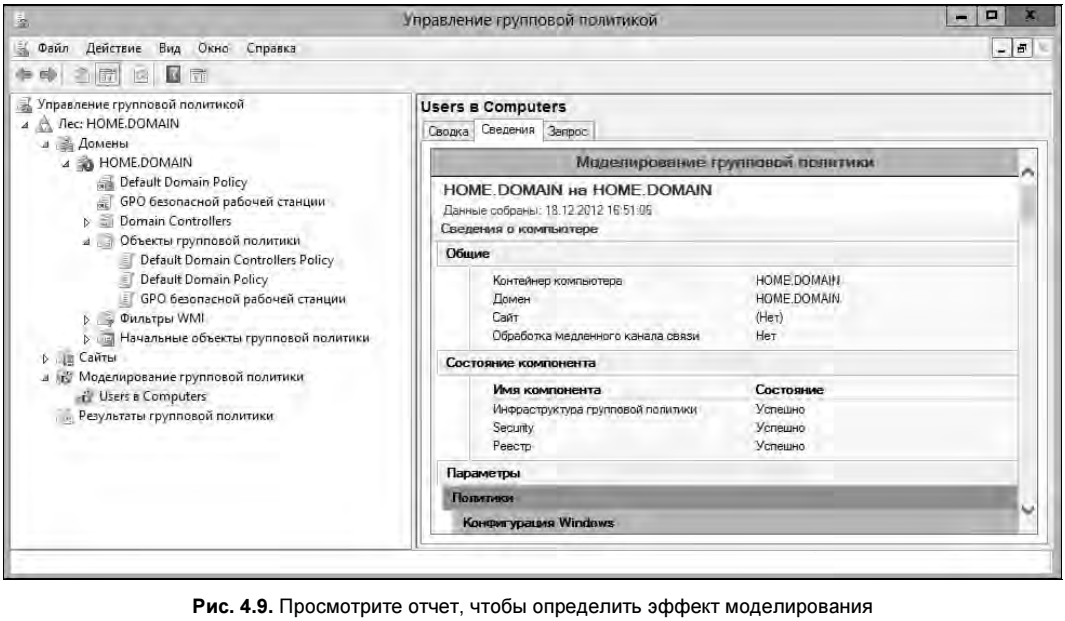


Рис. 4.9. Просмотрите отчет, чтобы определить эффект моделирования

8. Просмотрите указанные параметры и нажмите кнопку **Далее**. После того как мастер соберет необходимую информацию политики, нажмите кнопку **Готово**. Когда мастер закончит генерирование отчета, созданный отчет будет выбран в левой области окна, а его результаты — в правой области.
9. На вкладке **Сведения** (Details) (рис. 4.9), просматривая отчет, можно определить настройки, которые будут применены. Информация политики компьютера выводится в области **Сведения о компьютере** (Computer Details). Информация политики пользователя — в области **Сведения о пользователе** (User Details).

Копирование, вставка и импорт объектов политики

Консоль GPMC поддерживает встроенные операции копирования, вставки и импорта. Использование функций копирования и вставки довольно простое. Команды **Копировать** (Copy) и **Вставить** (Paste) доступны в контекстном меню объекта групповой политики. Можно скопировать GPO и все его настройки в одном домене, затем переместиться в другой домен и вставить копию объекта политики. Исходный и целевой домены могут быть любыми доменами, с которыми можно соединиться в GPMC и для которых существует разрешение управлять связанными объектами политики. В исходном домене требуется разрешение чтения (для создания копии объекта). В целевом домене — разрешение записи, чтобы вставить скопированный объект политики. Такое разрешение есть у администраторов, а также у тех, кто был специально делегирован создавать объекты политики.

Копирование объектов политики между доменами работает хорошо, если есть связь между доменами и надлежащие полномочия. Даже если администратор находится в удаленном офисе или имеет делегированные разрешения, он может не иметь доступа к исходному домену для создания копии объекта политики. В этом случае другой администратор может сделать резервную копию объекта политики и затем отправить ее администратору в удаленный офис. Когда первый администратор получит эту резервную копию, он может импортировать объект политики в домен для создания объекта политики с такими же настройками.

Любой пользователь с полномочиями **Изменение параметров** (Edit Settings) может осуществить операцию импорта. Операция импорта перезаписывает все настройки выбранного объекта политики. Для импортирования резервной копии объекта политики в домен выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши по узлу **Объекты групповой политики**, затем выберите команду **Создать**. В окне **Новый объект групповой политики** введите описательное имя нового GPO и нажмите кнопку **OK**.
2. Теперь в контейнере **Объекты групповой политики** появится новый GPO. Щелкните правой кнопкой мыши на созданном объекте и выберите команду **Импорт параметров** (Import Settings). Запустится мастер импорта параметров (Import Settings Wizard).
3. Нажмите кнопку **Далее** дважды, чтобы пропустить страницу **Архивирование объекта групповой политики** (Backup GPO). Не нужно архивировать текущий GPO, поскольку он новый и в нем ничего нет.
4. На странице **Расположение архива** (Backup Location) нажмите кнопку **Обзор**. В окне **Обзор папок** (Browse For Folder) выберите папку, содержащую резервную копию объекта политики, который нужно импортировать, затем нажмите кнопку **OK**. Нажмите кнопку **Далее**, чтобы продолжить.

5. Если в выбранной папке хранится несколько резервных копий, будет отображен их список на странице **Исходный объект групповой политики** (Source GPO). Выберите объект, который нужно использовать, и нажмите кнопку **Далее**.
6. Мастер импорта настроек просканирует объект политики в поисках ссылок на субъекты безопасности и путей UNC, которые должны быть перемещены. Если такие пути или субъекты будут найдены, будет предоставлена возможность составить или использовать существующие таблицы миграции.
7. Продолжите работу мастера, нажав кнопку **Далее**, а затем — кнопку **Готово** для начала процесса импорта. Когда импорт будет завершен, нажмите кнопку **OK**.

Резервное копирование и восстановление объектов политики

Для защиты GPO нужно сделать их резервные копии. Для создания резервных копий отдельных объектов политик домена или всех политик объекта в домене можно использовать консоль GPMC:

1. В консоли GPMC разверните и затем выберите узел **Объекты групповой политики**. Если нужно сделать резервную копию всех объектов политики в домене, щелкните правой кнопкой мыши на узле **Объекты групповой политики** и выберите команду **Архивировать все** (Back Up All). Если нужно сделать резервную копию определенного объекта в домене, щелкните на нем правой кнопкой мыши и выберите команду **Архивировать** (Back Up).
2. В окне **Архивация объекта групповой политики** (Back Up Group Policy Object) нажмите кнопку **Обзор**. В окне **Обзор папок** выберите папку, в которой будет сохранен объект GPO.
3. В поле **Описание** (Description) введите описание содержимого резервной копии. Нажмите кнопку **Архивировать** (Back Up) для начала резервного копирования.
4. Состояние процесса резервного копирования и индикатор хода архивирования отображается в окне **Архивирование** (Backup). Нажмите кнопку **OK** после создания резервной копии. Для создания резервной копии нужны разрешения чтения и записи. По умолчанию такие разрешения есть у групп **Администраторы домена** (Domain Admins) и **Администраторы предприятия** (Enterprise Admin).

Используя консоль GPMC, можно восстановить объект политики в состояние, в котором он был архивирован. Консоль GPMC отслеживает резервные копии каждого объекта политики отдельно, даже если архивируются сразу все объекты политик. Поскольку информация о версии тоже отслеживается по штампу времени резервной копии и описанию, можно восстановить последнюю версию каждого объекта политики или определенную версию любого объекта политики.

Для восстановления объекта политики выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на узле **Объекты групповой политики** и выберите команду **Управление архивацией** (Manage Backups). Появится одноименное диалоговое окно.
2. В поле **Расположение архива** (Backup Location) нажмите кнопку **Обзор**. В окне **Обзор папок** найдите папку, в которой находится резервная копия, и нажмите кнопку **OK**.
3. Все резервные копии объекта политики в выбранной папке перечислены в узле **Архивированные объекты групповой политики** (Backed Up GPOs). Чтобы увидеть только по-

следнюю версию объектов политики по метке времени, включите параметр **Показывать только последнюю версию каждого объекта групповой политики** (Show Only The Latest Version Of Each GPO).

4. Выберите GPO, который нужно восстановить. Если необходимо подтвердить его параметры, нажмите кнопку **Просмотреть параметры** (View Settings). После этого в окне Internet Explorer можно проверить параметры объекта политики. Когда будете готовы продолжить, нажмите кнопку **Восстановить** (Restore). Подтвердите свое намерение, нажав кнопку **OK**.
5. Диалоговое окно **Восстановление** (Restore) покажет состояние процесса восстановления и индикатор хода восстановления. Если операция восстановления завершилась неудачно, проверьте разрешения на объекте политики и папке, из которой осуществляется чтение резервной копии. Для восстановления GPO у пользователя должно быть разрешение **Изменение параметров, удаление и изменение параметров безопасности** (Edit Settings, Delete, and Modify Security) на объекте политики и разрешение на чтение из папки с архивом. По умолчанию такие разрешения имеют пользователи из групп **Администраторы домена** и **Администраторы предприятия**.

Определение текущих настроек групповой политики и статуса определения

Для анализа RSoP (Resultant Set of Policy) можно использовать моделирование групповой политики. Если моделирование групповой политики используется именно так, можно просмотреть все объекты политики, которые применяются к компьютеру, и время последней обработки (обновления) объектов политики. Доступ к моделированию групповой политики для анализа имеют все администраторы домена и предприятия, а также все пользователи, у которых есть разрешение **Чтение результирующих данных групповой политики** (Read Group Policy Results Data). В консоли GPMC можно моделировать групповую политику для анализа, щелкнув правой кнопкой мыши на узле **Результаты групповой политики** (Group Policy Results) и выбрав команду **Мастер результатов групповой политики** (Group Policy Results Wizard). Когда откроется окно мастера, следуйте его инструкциям.

Отключение неиспользуемой части групповой политики

Другой способ отключения политики — отключить неиспользуемую часть GPO. В результате будут заблокированы настройки конфигурации компьютера и конфигурации пользователя (или обе), и им будет запрещено применяться. При отключении неиспользуемой части политики применение GPO будет осуществляться быстрее.

Включить и отключить политики можно с помощью следующих действий:

1. В консоли GPMC выберите контейнер сайта, домена или организационного подразделения, с которыми нужно работать.
2. Выберите объект политики, с которым нужно работать, и затем перейдите на вкладку **Сведения** (Details) на правой панели.
3. Выберите одно из значений из списка **Состояние GPO** (GPO Status) и нажмите кнопку **OK**, когда консоль попросит подтвердить изменение состояния GPO:
   - **Все параметры отключены** (All Settings Disabled) — отключает обработку объекта политики и всех его параметров;

- **Параметры конфигурации компьютера отключены** (Computer Configuration Settings Disabled) — отключает параметры конфигурации компьютера. Это означает, что будут обработаны только параметры конфигурации пользователя;
- **Параметры конфигурации пользователя отключены** (User Configuration Settings Disabled) — отключает параметры конфигурации пользователя. Это означает, что будут обработаны только параметры конфигурации компьютера;
- **Включено** (Enabled) — разрешает обработку объекта политики и всех его параметров.

Изменение свойств обработки политики

В групповой политике параметры конфигурации компьютера обрабатываются при запуске компьютера и получении доступа к сети. Параметры конфигурации пользователя обрабатываются, когда пользователь входит в сеть. В случае конфликта между настройками в конфигурации компьютера и конфигурации пользователя будут применены параметры конфигурации компьютера. Также важно помнить, что параметры компьютера применяются из GPO компьютера, а параметры пользователя — из GPO пользователя.

В некоторых особых ситуациях данное поведение — не то, что нужно. Возможно, будет необходимо, чтобы на общем компьютере параметры пользователя применялись из GPO компьютера, и в то же время нужно разрешить применение настроек пользователя из GPO пользователя. В безопасной лаборатории нужно применять пользовательские настройки из GPO компьютера, чтобы настройки соответствовали строгим правилам безопасности или инструкциям лаборатории. Эти типы исключений можно получить с помощью замыкания групповой политики.

Для изменения режима обработки замыкания групповой политики выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте GPO, который необходимо модифицировать, и выберите команду **Изменить**.
2. В узле **Конфигурация компьютера\Политики\Административные шаблоны\Система\ Групповая политика** (Computer Configuration\Policies\ Administrative Templates\System\ Group Policy) выберите политику **Настройка режима обработки замыкания пользовательской групповой политики** (Configure User Group Policy Loopback Processing Mode). Будет отображено окно свойств этой политики.
3. Включите политику, выбрав переключатель **Включено** (Enabled). Выберите один из режимов обработки из списка **Режим** (Mode) и затем нажмите кнопку **OK**.
   - **Замена** (Replace) — параметры политики пользователя, определенные в GPO компьютера, заменят параметры политики пользователя, обычно применяемые для этого пользователя. Это означает, что пользовательские настройки из GPO компьютера заменят настройки пользователя, которые обычно к нему применялись.
   - **Слияние** (Merge) — выберите этот режим, чтобы убедиться, что сначала будут обработаны пользовательские настройки в GPO компьютера, а далее пользовательские настройки из GPO пользователя, а затем снова — пользовательские настройки в GPO компьютера. Эта техника обработки применяется для комбинации пользовательских настроек в GPO компьютера и GPO пользователя. В случае конфликта приоритет будет у пользовательских настроек в GPO компьютера: они перезапишут пользовательские настройки в GPO пользователя.

Настройка обнаружения медленного соединения

Обнаружение медленного соединения используется клиентами групповой политики для определения увеличения задержки и уменьшения скорости отклика в сети и принятия мер по ликвидации последствий, чтобы уменьшить вероятность прекращения применения групповой политики в сети. Как только обнаружено медленное соединение, клиенты групповой политики снижают свои запросы, чтобы уменьшить нагрузку на сеть, ограничивая количество обрабатываемых политик.

По умолчанию, если скорость соединения меньше 500 Кбит/с (это значение может быть интерпретировано как высокий уровень задержки/снижения скорости отклика в быстрой сети), клиентские компьютеры воспринимают это соединение как медленное и уведомляют об этом контроллер домена. В результате при обновлении политики будут применены только параметры безопасности и административные шаблоны.

За определение медленного соединения отвечает политика **Настройка определения медленных подключений** (Configure Group Policy Slow Link Detection), которая находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Система\Групповая политика** (Computer Configuration\Policies\Administrative Templates\System\Group Policy). Если отключить эту политику или не настраивать ее, клиенты будут использовать значение по умолчанию — 500 Кбит/с для определения, медленное ли соединение. Если включить эту политику, можно установить скорость, при которой соединение будет считаться медленным, например, 384 Кбит/с. Также помните, что 3G-соединения практически всегда будут считаться медленными. С другой стороны, если нужно полностью отключить обнаружение медленного соединения, установите параметр **Скорость подключения** (Connection Speed) в 0. Для клиента это будет сигналом, что больше не нужно определять медленные соединения, и все соединения будут рассмотрены как быстрые.

Практический совет

Microsoft называет сотовые и широкополосные соединения платными сетями. Разработано несколько политик, чтобы помочь указать, как должна использоваться сеть на мобильных устройствах, работающих через платные сети. Администратор может:

- контролировать синхронизацию автономных файлов на платных сетях с помощью политики **Включить синхронизацию файлов в платных сетях** (Enable File Synchronization On Costed Networks), которая находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Сеть\Автономные файлы** (Computer Configuration\Policies\Administrative Templates\Network\Offline Files);
- контролировать фоновую передачу по платным сетям с помощью политики **Установить логику загрузки по умолчанию для заданий BITS в тарифицируемых сетях** (Set Default Download Behavior For BITS Jobs On Costed Networks), которая находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Сеть\Фоновая интеллектуальная служба передачи (BITS)** (Computer Configuration\Policies\Administrative Templates\Network\Background Intelligent Transfer Services (BITS));
- указать стоимость платного соединения. Платные сети могут иметь фиксированную, переменную или неограниченную плату за соединение. Установить тип оплаты можно в узле **Конфигурация компьютера\Политики\Административные шаблоны\Сеть\Служба WLAN\Стоимость использования WLAN** (Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Media Cost) с помощью политики **Задать стоимость** (Set Cost policy);
- указать стоимость 3G/4G-соединения. Стоимость 3G- и 4G-доступа может отличаться и тоже может быть фиксированной, переменной и неограниченной. Задать тип стоимости можно с помощью политик **Задать стоимость 3G** (Set 3G Cost) и **Задать стоимость 4G** (Set 4G Cost) в узле **Конфигурация компьютера\Политики\Административные шаб-**

лоны\Сеть\Служба WWAN\Стоимость использования WWAN (Computer Configuration\Policies\Administrative Templates\Network\WWAN Service\WWAN Media Cost).

В случае необходимости можно оптимизировать механизм обнаружения медленного соединения для различных областей обработки групповой политики. По умолчанию следующие области групповой политики не обрабатываются, когда обнаружено медленное соединение:

- обработка политик дисковых квот;
- обработка политик восстановления EFS;
- обработка политик перенаправления папок;
- обработка политик установки программного обеспечения.

Обработка политик безопасности всегда включена для медленных соединений. По умолчанию политика обновляется каждые 16 часов, даже если политика безопасности не изменялась. Единственный способ остановить принудительное обновление — настроить обработку политики безопасности так, чтобы она не применялась во время периодических фоновых обновлений. Чтобы сделать это, установите опцию **Не применять во время периодической фоновой обработки** (Do Not Apply During Periodic Background Processing) (см. далее). Однако поскольку политики безопасности очень важна, отключение применения означает, что обработка политика безопасности будет остановлена, когда пользователь зарегистрирован и использует компьютер. Единственная причина, по которой нужно остановить обновление политики безопасности — если приложения перестали работать во время операций обновления.

Обнаружение медленного соединения и обработку соответствующих политик можно настроить так:

1. В консоли GPMC щелкните правой кнопкой мыши по объекту политики, который необходимо модифицировать, и выберите команду **Изменить**.
2. Дважды щелкните на политике **Настроить определения медленных подключений для групповой политики** (Configure Group Policy Slow Link Detection) в узле **Конфигурация компьютера\Политики\Административные шаблоны\Система\Групповая политика** (Computer Configuration\ Policies\Administrative Templates\System\Group Policy).
3. Установите переключатель **Включено** (Enabled), как показано на рис. 4.10. В поле **Скорость подключения** (Connection Speed) задайте скорость, которая будет считаться медленной. Также можно указать, будут ли считаться 3G-соединения медленными. Нажмите кнопку **OK**.

Для настройки медленного соединения и фоновой обработки ключевых областей групповой политики выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте политики, который нужно модифицировать, и выберите команду **Изменить**.
2. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\ Групповая политика**.
3. Дважды щелкните на политике обработки, которую необходимо настроить. Установите переключатель **Включено** для определения политики (рис. 4.11) и сделайте соответствующую настройку. Опции могут немного отличаться, в зависимости от выбранной политики:
   - **Разрешить обработку через медленное сетевое подключение** (Allow Processing Across A Slow Network Connection) — гарантирует, что политика будет обработана даже в медленной сети;

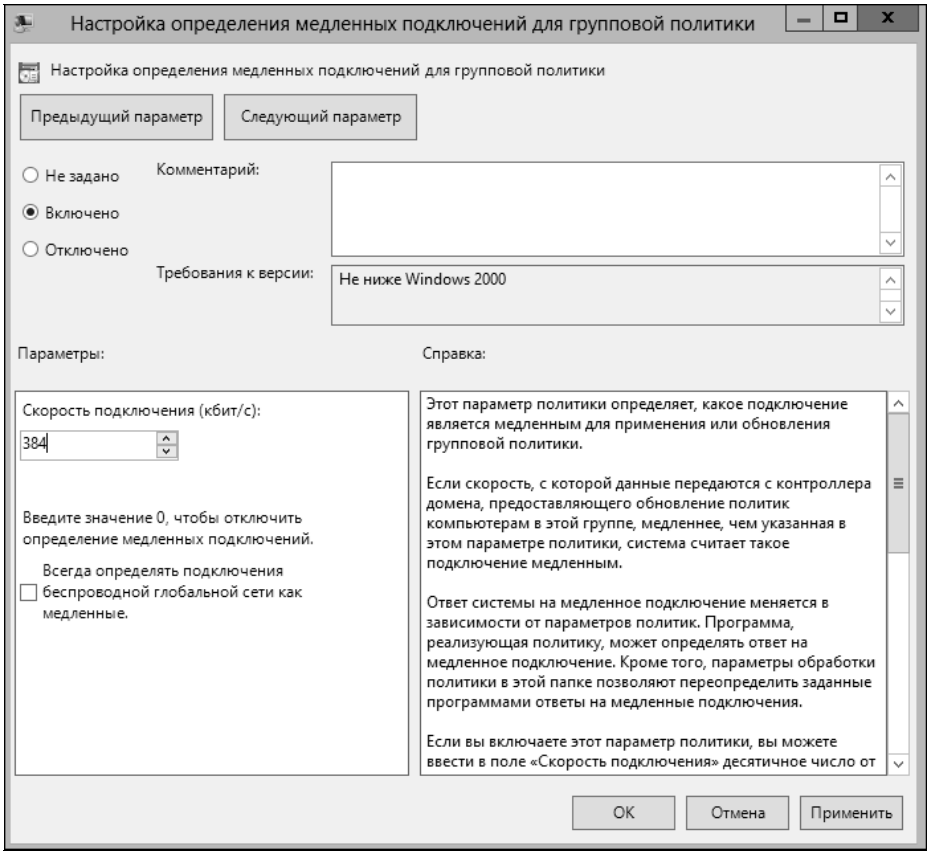


Рис. 4.10. Настройка определения медленного соединения

- **Не применять во время периодической фоновой обработки** (Do Not Apply During Periodic Background Processing) — переопределяет настройки обновления, когда связанные политики изменяются после запуска или входа в систему;
- **Обрабатывать, даже если объекты групповой политики не изменились** (Process Even If The Group Policy Objects Have Not Changed) — политика будет применена, даже если ее настройка не изменилась.

4. Нажмите кнопку **OK** для сохранения изменений.

Удаление ссылок и удаление GPO

В консоли GPMC можно остановить использование связанных объектов групповой политики двумя способами:

- ♦ удалить ссылку на GPO, но не удалять сам GPO;
- ♦ удалить GPO и все ссылки на него.

Удаление ссылки на GPO предотвращает использование соответствующих настроек политик в сайте, домене или организационном подразделении, но не удаляет сам GPO. Однако GPO остается соединенным с другими сайтами, доменами или организационными подразделениями. В GPMC можно удалить ссылку на GPO, щелкнув правой кнопкой мыши по

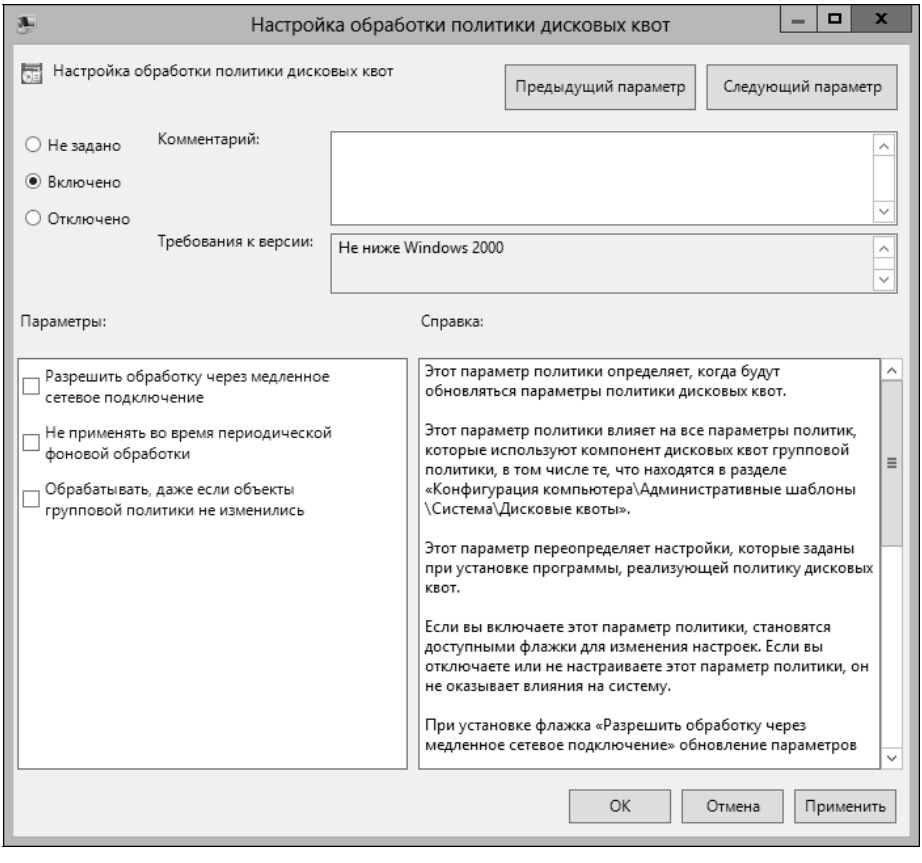


Рис. 4.11. Настройка политики обработки медленного соединения

ссылке на GPO в контейнере и выбрав команду **Удалить** (Delete). Когда консоль попросит подтвердить намерение, нажмите кнопку **OK**. Если удалить все ссылки на GPO с сайтов, доменов и организационных подразделений, GPO продолжит существование в контейнере **Объекты групповой политики**, но его настройки не будут иметь никакого эффекта в организации.

Удаление GPO означает удаление GPO и всех ссылок на него. GPO больше не будет существовать в контейнере **Объекты групповой политики** и не будет связан ни с одним сайтом, доменом или организационным подразделением. Есть только один способ восстановить удаленный GPO — это восстановить его из ранее созданной резервной копии (если она доступна). Удалить GPO и все ссылки на этот объект можно в консоли GPMC из узла **Объекты групповой политики**. Щелкните правой кнопкой мыши на GPO и выберите команду **Удалить**. Для подтверждения своего намерения нажмите кнопку **Да**.

Поиск и устранение неисправностей групповой политики

При попытке определить, почему политика не применяется, как ожидалось, первым делом нужно исследовать результаты групповой политики для пользователя и компьютера, чтобы понять суть проблемы.

Определить, что политики GPO применены, можно так:

1. В консоли GPMC щелкните правой кнопкой мыши по узлу **Результаты групповой политики** (Group Policy Results) и выберите команду **Мастер результатов групповой политики** (Group Policy Results Wizard). Когда мастер запустится, нажмите кнопку **Далее**.
2. На странице **Выбор компьютера** (Computer Selection) установите переключатель **Этот компьютер** (This Computer), чтобы просмотреть информацию для локального компьютера. Чтобы просмотреть информацию для удаленного компьютера, отметьте переключатель **Другой компьютер** (Another Computer) и затем нажмите кнопку **Обзор**. В окне **Выбор: "Компьютер"** (Select Computer) введите имя компьютера и нажмите кнопку **Проверить имена** (Check Names). После того как выберете правильное имя компьютера, нажмите кнопку **Далее**.
3. На странице **Выбор пользователя** (User Selection) выберите пользователя, чью информацию о политике нужно просмотреть. Можно просмотреть информацию о политике для любого пользователя, который ранее был зарегистрирован на компьютере. Нажмите кнопку **Далее**.
4. Просмотрите установленные параметры и нажмите кнопку **Далее**. После того как мастер получит необходимую информацию, нажмите кнопку **Готово**. По окончанию создания отчета он будет выбран в левой панели, а результаты будут отображены в правой панели.
5. Чтобы определить, какие параметры были применены, просмотрите отчет. Информация политики для компьютера и пользователя выводится отдельно: для компьютера — в разделе **Сводка о компьютере** (Computer Configuration Summary), для пользователя — в разделе **Сводка о пользователе** (User Configuration Summary).

Используя утилиту командной строки Gpresult, можно просмотреть RSoP. Эта утилита предоставляет следующие сводки:

- специальные параметры, примененные для перенаправления папок, установки программы, дисковых квот, IPsec и сценариев;
- время последнего применения групповой политики;
- контроллер домена, от которого была получена политика и членство группы безопасности для компьютера и пользователя;
- полный список всех примененных GPO, а также список GPO, которые не были использованы из-за фильтров.

Базовый синтаксис утилиты Gpresult следующий:

```
gpresult /s ComputerName /user Domain\UserName
```

Здесь *ComputerName* — имя компьютера, для которого нужно просмотреть результаты политики; Domain*UserName* — имя пользователя. Например, для просмотра RSoP для компьютера CorpPC85 и пользователя Tedg в домене Cpandl нужно ввести команду:

```
gpresult /s corppc85 /user cpandl\tedg
```

Дополнительную информацию можно получить, добавив две следующие опции. Параметр `/v` включает подробный вывод и отображает результаты только для актуальных настроек политик. Параметр `/z` также включает подробный вывод и отображает результаты только для актуальных политики и всех других GPO, где установлены политики. Поскольку вывод Gpresult очень длинный, нужно создать HTML-отчет, добавив параметр `/h` или XML-отчет, добавив параметр `/x`.

Примеры:

```
gpresult /s corppc85 /user cpandl\tedg /h gpreport.html
gpresult /s corppc85 /user cpandl\tedg /x gpreport.xml
```

Исправление объектов групповой политики по умолчанию

Объекты групповой политики Default Domain Policy и Default Domain Controller Policy жизненно важны для доменных служб Active Directory (AD DS). Если по некоторым причинам эти политики будут повреждены, то групповая политика перестанет функционировать должным образом. Для решения проблемы нужно восстановить эти объекты из резервной копии. Если резервные копии объектов Default Domain Policy и Default Domain Controller Policy отсутствуют, можно использовать утилиту Dcgpofix, чтобы восстановить настройки безопасности в этих политиках.

Состояние, к которому Dcgpofix восстанавливает эти объекты, зависит от того, как изменили безопасность, и от состояния безопасности контроллера домена перед запуском Dcgpofix. Для запуска утилиты нужно быть членом групп **Администраторы домена** или **Администраторы предприятия**.

При запуске Dcgpofix объекты групповых политик Default Domain Policy и Default Domain Controller Policy будут восстановлены со значениями по умолчанию, и любые изменения, внесенные в эти GPO, будут потеряны. Некоторые настройки политики сохраняются отдельно и не будут потеряны, в том числе Windows Deployment Services (WDS), параметры безопасности и Encrypting File System (EFS). Настройки безопасности, не являющиеся настройками по умолчанию, не обслуживаются, а это означает, что они могут быть потеряны. Все другие настройки политики будут восстановлены в их предыдущие значения, и любые сделанные вами изменения будут потеряны.

Для запуска Dcgpofix войдите в контроллер домена, где нужно починить групповую политику по умолчанию, а затем введите команду `dcgpofix` в командной строке. Утилита проверит версию схемы Active Directory, чтобы гарантировать совместимость версий Dcgpofix и конфигурации схемы Active Directory. Если версии не совместимы, Dcgpofix завершит работу без исправления GPO по умолчанию. При указании параметра `/Ignoreschema` Dcgpofix будет принудительно работать с другой версией Active Directory. Однако GPO по умолчанию могут быть не восстановлены в их исходное состояние. Поэтому убедитесь, что используете версию Dcgpofix, которая устанавливалась с текущей операционной системой.

Можно исправить только GPO Default Domain Policy или GPO Default Domain Controller Policy. Если нужно исправить объект Default Domain Policy, введите команду `dcgpofix /target:domain`. Если нужно исправить объект Default Domain Controller Policy, введите команду `dcgpofix /target:dc`.

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;
- 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 XP Professional и более ранних выпусков Windows: Application Data, Главное меню, Рабочий стол, Мои документы и Мои изображения. Для Windows Vista и более поздних версий: 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 12)*.

По умолчанию пользователи могут перенаправить папки независимо от того, какой компьютер они используют в домене. Windows 8 и Windows Server 2012 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 9*.

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.
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. 4.12).
4. В 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).

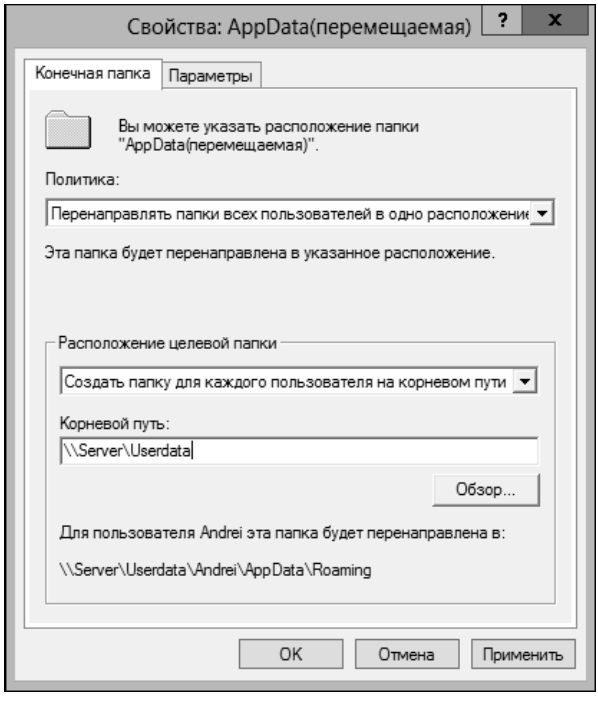


Рис. 4.12. Установите опции для перенаправления специальных папок

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 пользовательского домашнего каталога. Можно указать расположение пользовательского домашнего 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, 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 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%`.

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.

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. 4.13, 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 пользовательского домашнего каталога. Можно указать расположение пользовательского домашнего 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 отдельный 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%`.

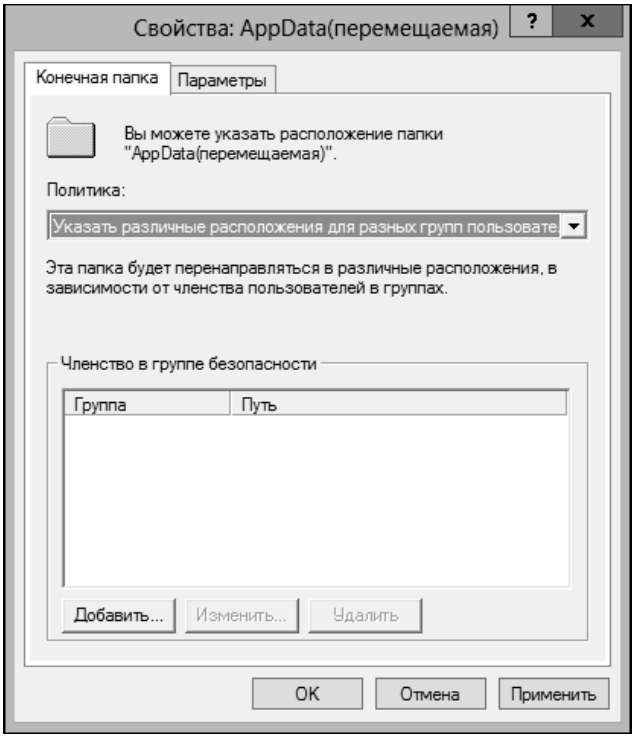


Рис. 4.13. Настройка расширенного перенаправления с использованием группы **Членство в группе безопасности**

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** (Windows Settings) и **Перенаправление папки** (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 нужна 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 будет скопировано 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 **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 расширением 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.

Операционные системы Windows 7, Windows 8, Windows Server 2008 R2 и Windows Server 2012 также 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.

Назначения 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. 4.14.
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, кото-

рый 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**.

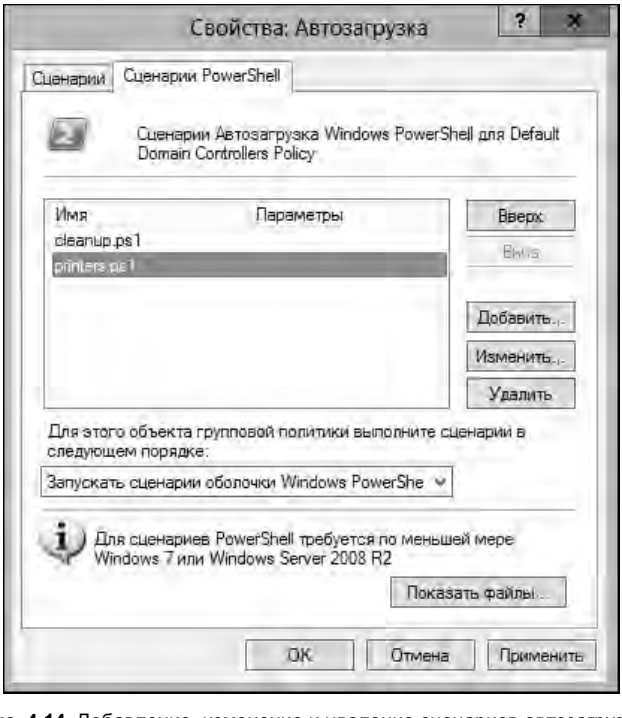


Рис. 4.14. Добавление, изменение и удаление сценариев автозагрузки

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. 4.15.

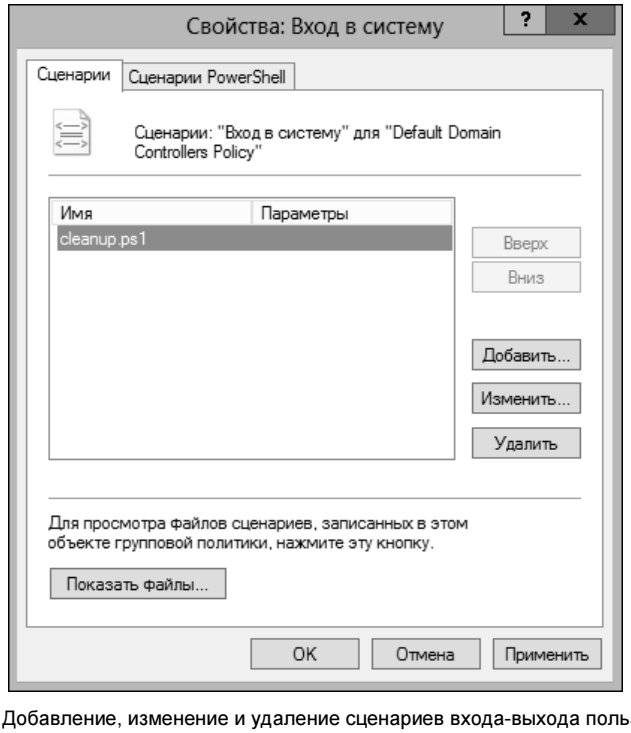


Рис. 4.15. Добавление, изменение и удаление сценариев входа-выхода пользователей

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\Startup или папку User\Scripts\Shutdown. В поле **Параметры сценария** введите любые параметры, которые нужно передать сценарию. Повторите этот шаг для других сценариев.
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 политики есть базовая функциональность, называемая *политикой установки программного обеспечения*. Хотя она не разработана для замены решений для предприятий вроде SMS (Systems Management Server), можно использовать ее для автоматизации развертывания и обслуживания ПО в организации практически любого размера при условии, что все компьютеры работают под управлением бизнес-выпусков Windows 2000 или более поздних версий.

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).
5. В окне **Развертывание программ** (Deploy Software), показанном на рис. 4.16, 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.

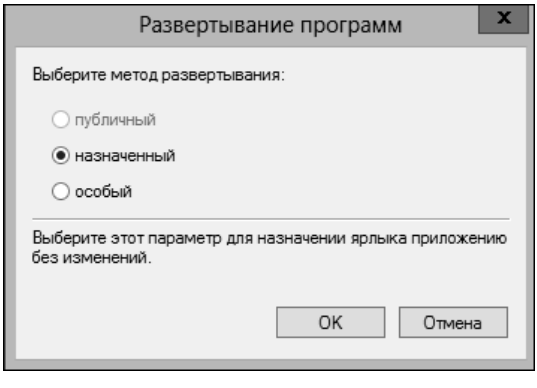


Рис. 4.16. Выберите метод развертывания

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)**.

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. 4.17) 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.

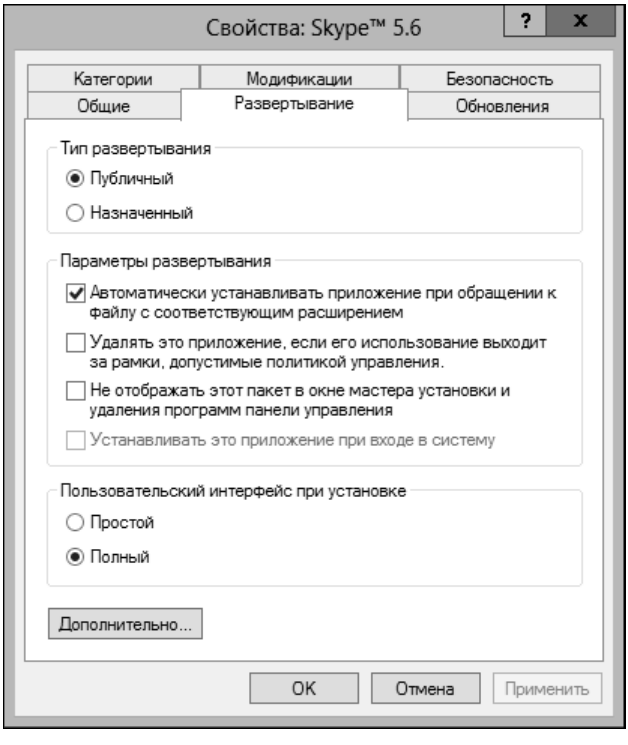


Рис. 4.17. Просмотрите и измените параметры развертывания в случае необходимости

- **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.
- **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 установочные 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. Альтернативно 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). Создайте 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 регистрация сертификатов компьютера и пользователя

Сервер, определенный как центр сертификации, отвечает за выпуск цифровых сертификатов и управление списками аннулированных сертификатов (Certificate Revocation Lists, CRLs). 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 и Windows Server 2012 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. Подробно об этом было рассказано в *главе 2*.

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** (Notify For Download And Notify For Install) — 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.
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.

Оптимизация автоматических обновлений

В целом, большинство автоматических обновлений устанавливается только при перезагрузке компьютера. Некоторые автоматические обновления могут быть установлены немедлен-

но 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 обнов-

ления 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, 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.
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.

> ***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.

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.

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 для 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 инсталляциях 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.

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).

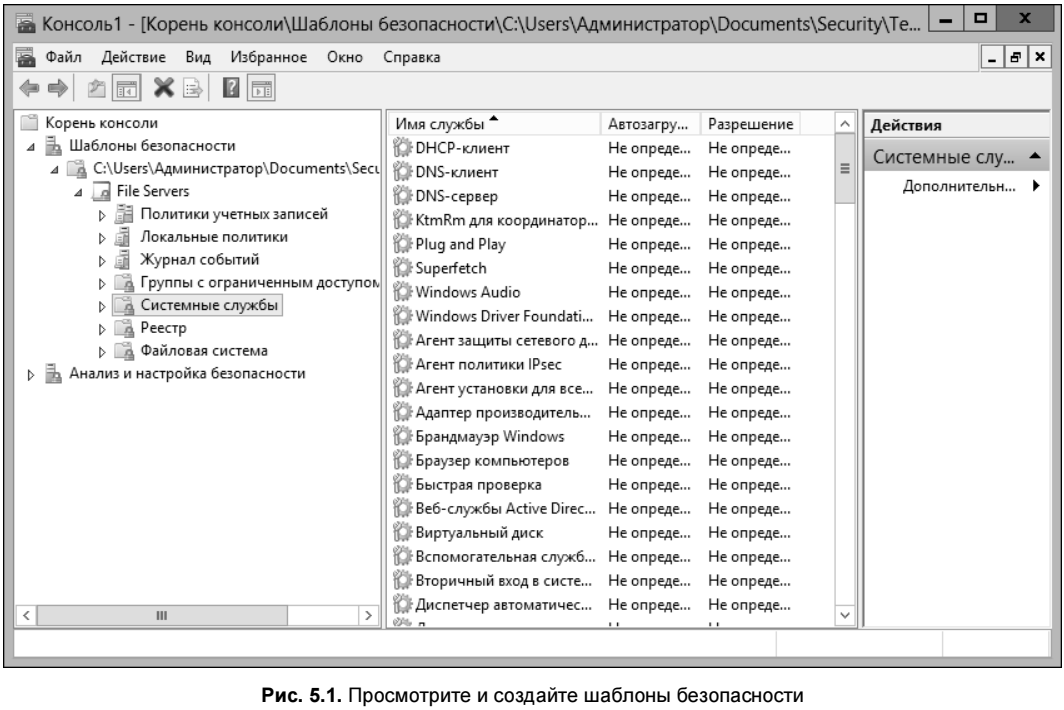


Рис. 5.1. Просмотрите и создайте шаблоны безопасности с помощью оснастки **Шаблоны безопасности**

> **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 используется 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). Альтернативно, 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 рассмотрены 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 поли-**

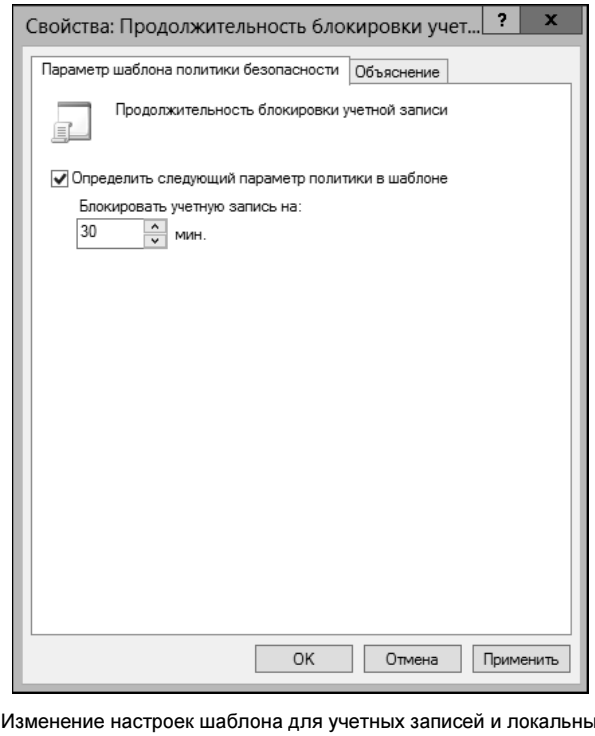


Рис. 5.2. Изменение настроек шаблона для учетных записей и локальных политик

тики 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).

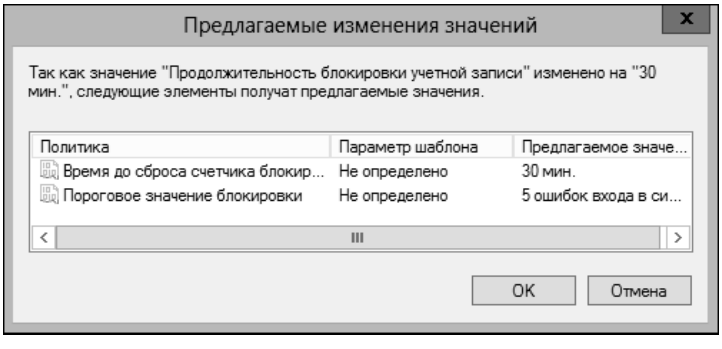


Рис. 5.3. Предлагаемые изменения значений

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.

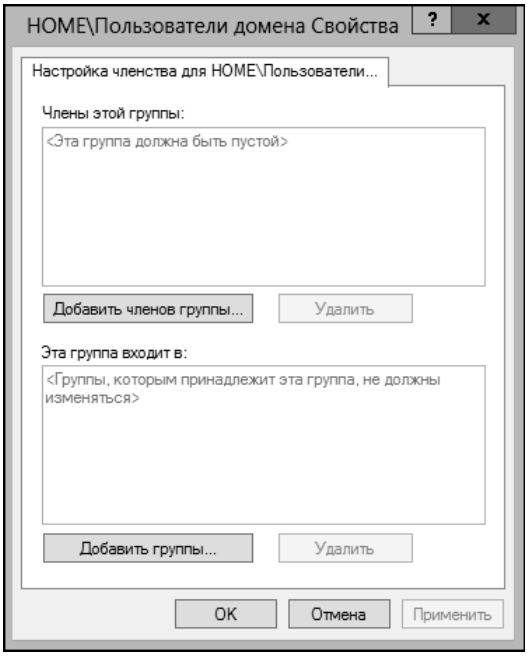


Рис. 5.4. Свойства группы

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 будут в алфавитном порядке 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.

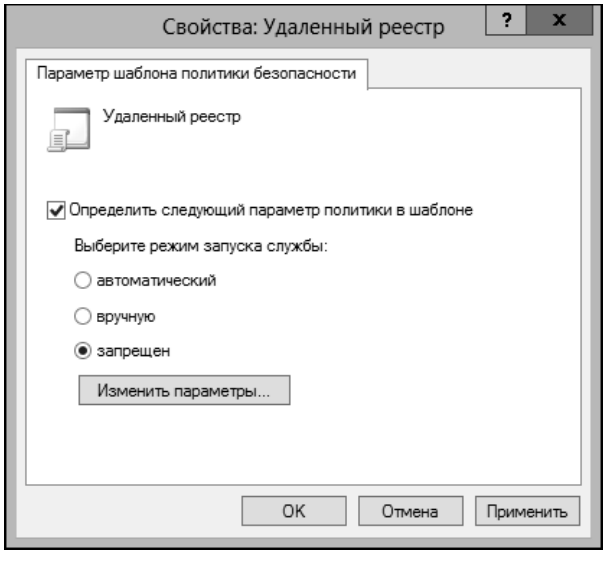


Рис. 5.5. Изменяем настройки шаблона для системных служб

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 нужно 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.
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).

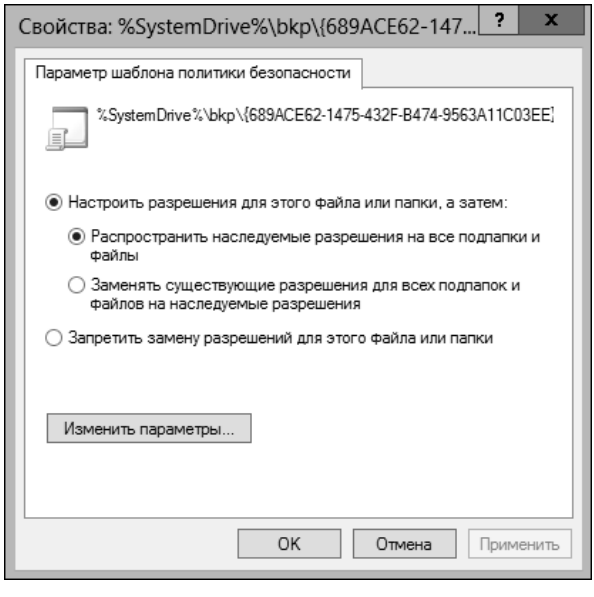


Рис. 5.6. Измените параметры шаблона для файлов и ключей реестра

3. Чтобы убедиться, что путь или ключ не заменяется, установите переключатель **Запретить замену разрешений для этого файла или папки** (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 разрешения для этого файла или папки** (Configure This Key Then), а затем одну из двух опций:
   - **Распространить наследуемые разрешения на все подпапки и файлы** (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;
   - **Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения** (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.

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. *См. главу 12* для подробных сведений.
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.

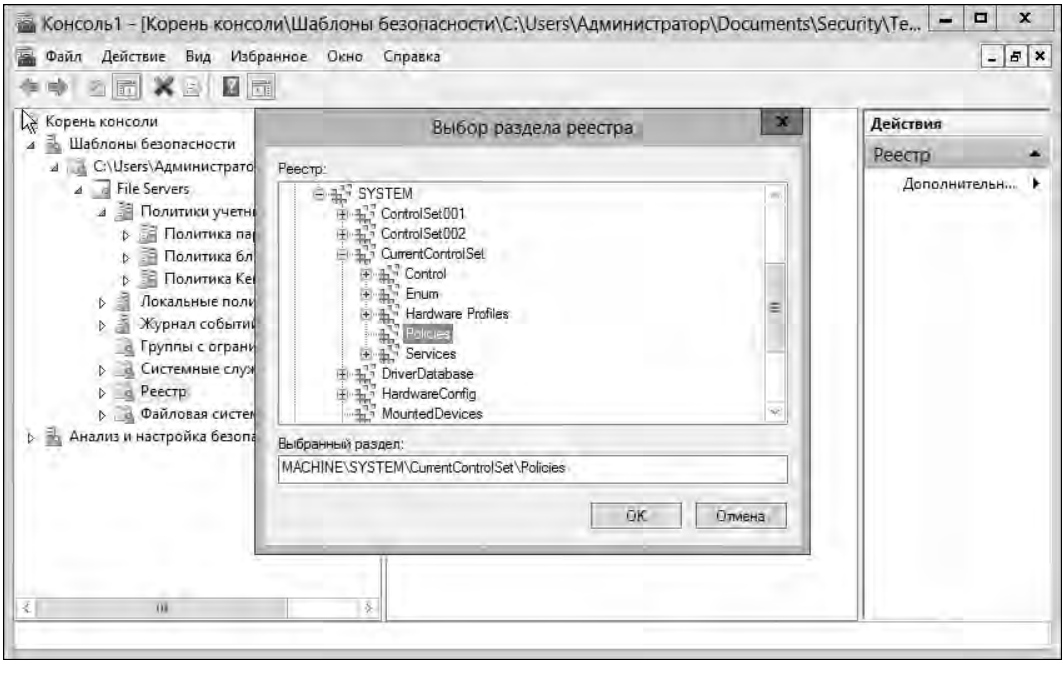


Рис. 5.7. Выберите раздел или значение реестра для его защиты

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 устанавливаются так же, как и для файлов/папок при использовании NTFS. Более детальные сведения приводятся в *главе 12*.
4. Нажмите кнопку **OK**. На экране появится окно **Добавление объекта** (Add Object). Чтобы убедиться, что разрешения раздела не заменяются, выберите переключатель **Запре-**

тить 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

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;
   - **Заменять 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.

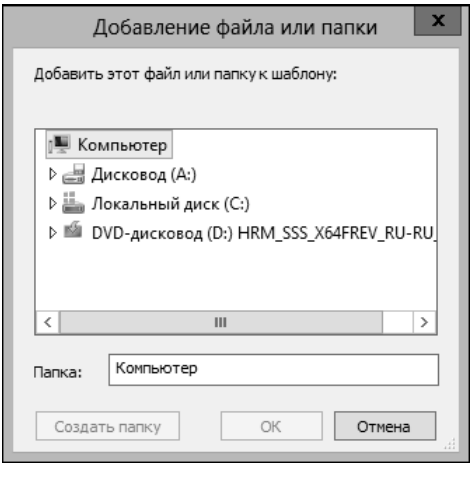


Рис. 5.8. Выберите файл или папку для защиты

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 12*.
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.
   - **Заменять 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. Применение 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, нужно 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 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).

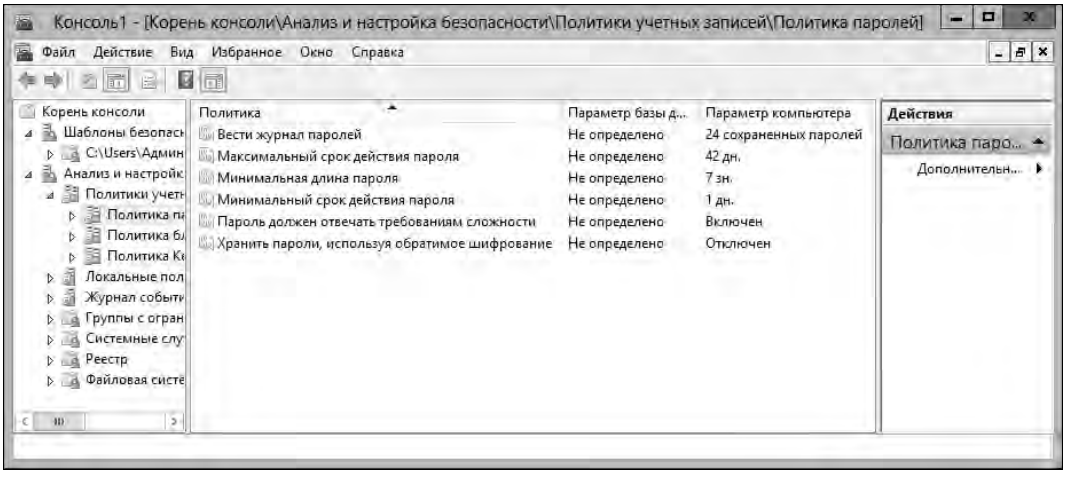


Рис. 5.9. Просмотрите разницу между настройками шаблона и компьютера

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).

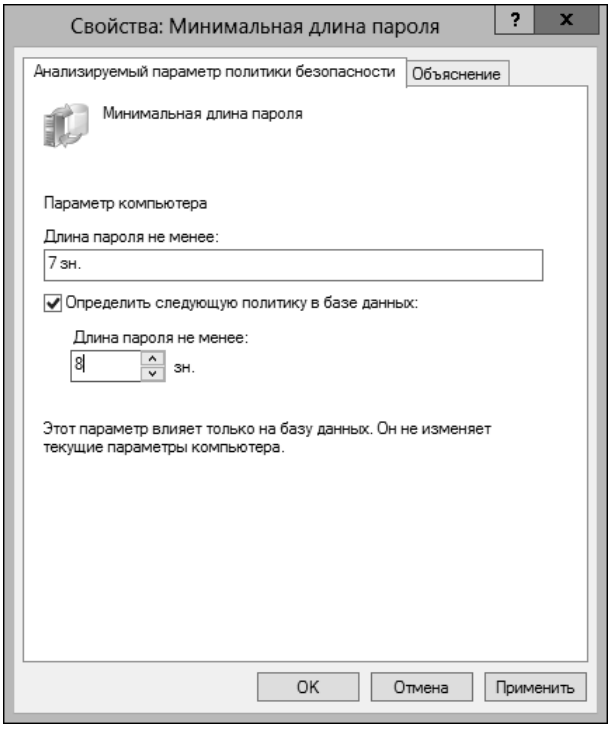


Рис. 5.10. Изменяем настройку политики в базе данных перед применением шаблона

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**.

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 графический мастер или утилита командной строки, необходимо создать шаблон отката перед применением любых настроек. *Шаблон отката* — это обратный шаблон, позволяющий удалить большинство настроек, которые применились 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 безопасности, 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 компьютеров 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 (файловые 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 графическому мастеру можно использовать 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, одинаковые 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**.

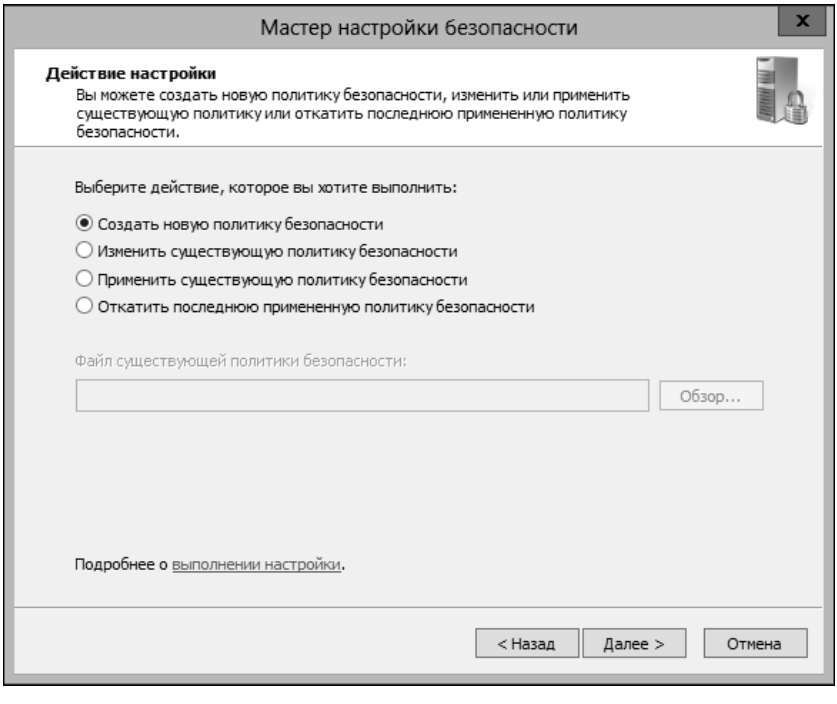


Рис. 5.11. Выберите действие настройки

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 работать. 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 кнопку **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 дан-**

ных 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 требуются какой-то включенной роли. Нажмите кнопку **Далее**.

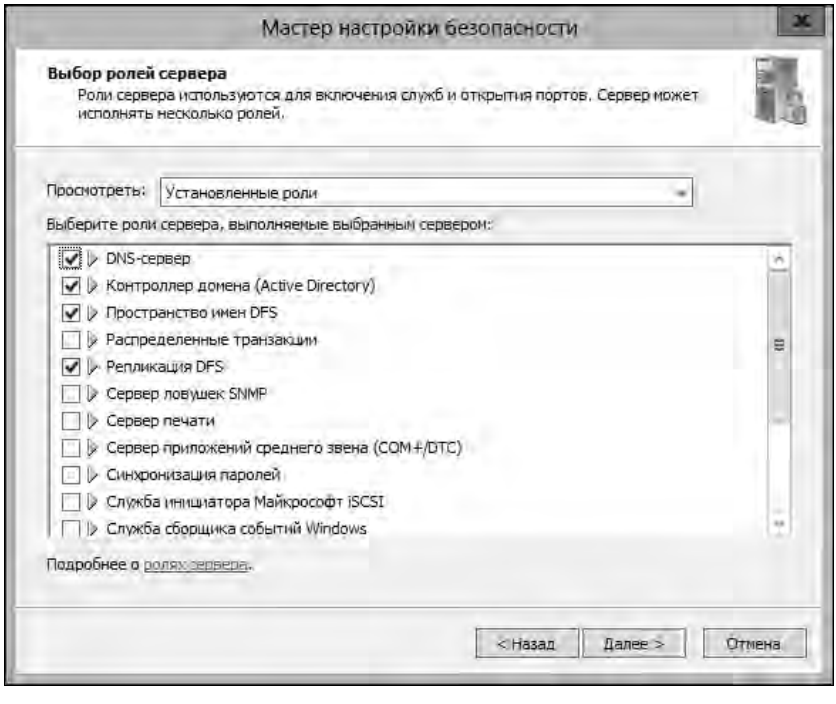


Рис. 5.12. Выберите роли, которые нужно включить

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 аутен-

тификации 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 нажмите 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.

часть II

Администрирование служб каталогов Windows Server

ГЛАВА 6

Использование Active Directory

Доменные службы Active Directory (Active Directory Domain Services, AD DS) — расширяемая и масштабируемая служба каталогов, которую можно использовать для активного управления сетевыми ресурсами. Администратору нужно четко понимать, как работает Active Directory. Данная технология усовершенствована и имеет множество функций.

Введение в Active Directory

Начиная с Windows 2000, Active Directory — сердце доменов на базе Microsoft Windows. Практически любая административная задача в той или иной мере затрагивает Active Directory. Технология Active Directory основана на стандартных интернет-протоколах и разработана для того, чтобы помочь вам определить четкую структуру вашей сети.

Active Directory и DNS

Active Directory использует систему доменных имен (Domain Name System, DNS). DNS — это стандартный интернет-сервис, объединяющий группы компьютеров в домены. Домены DNS организованы в иерархическую структуру. Иерархия домена DNS определена на основе всего Интернета, разные уровни в иерархии идентифицируют компьютеры, объединяя их в домены и домены верхнего уровня. DNS также используется для преобразования имен узлов в числовые адреса TCP/IP. С помощью DNS структура иерархии домена Active Directory может быть частью доменной иерархии Интернета или же может быть отделена от Интернета (частной).

При обращении к компьютерам в домене DNS используется *полное доменное имя* (Fully Qualified Domain Name, FQDN), например, **zeta.microsoft.com**. Здесь, **zeta** — имя отдельного компьютера, **microsoft** — домен организации, а **com** — домен верхнего уровня. Домены верхнего уровня (top-level domains, TLD) — база DNS-иерархии. TLD организованы по географическому признаку с использованием двухбуквенного кода страны (например, **ca** для Канады), по типу организации (например, **com** для коммерческих организаций), по функции (например, **mil** для министерства обороны США).

Обычные домены, например **microsoft.com**, также называются *родительскими доменами*, поскольку они являются родителями для структуры организации. Можно разделить родительские домены на поддомены, которые затем можно использовать для различных офисов, отделений или географических подразделений. Например, FQDN компьютера в офисе

Microsoft в Сиэтле может выглядеть так: **jacob.seattle.microsoft.com**. Здесь **jacob** — имя компьютера, **seattle** — поддомен, а **microsoft.com** — родительский домен. Другое название поддомена — *дочерний домен*.

DNS интегрируется в технологию Active Directory, причем так глубоко, что сначала нужно настроить DNS в своей сети, а затем уже устанавливать Active Directory. Работа с DNS описана в *главе 16*.

В случае с Windows Server 2012 процесс установки Active Directory состоит из двух частей. Процесс установки начинается в диспетчере серверов выбором команды **Добавить роли и компоненты** (Add Roles And Features), которая запустит мастер добавления ролей и компонентов (Add Roles And Features Wizard), используемый для установки роли AD DS. В результате будут установлены двоичные файлы, необходимые для роли, а процесс установки будет показан на странице **Ход установки** (Installation Progress).

> ***Практический совет***
>
> Двоичные файлы, необходимые для установки ролей и компонентов, называются *полезными данными*. В Windows Server 2012 можно не только удалить роль или компонент, но и удалить полезные данные для этого компонента или роли, используя параметр `-Remove` командлета Uninstall-WindowsFeature.
>
> Можно восстановить удаленные полезные данные, используя командлет Install-WindowsFeature. По умолчанию полезные данные восстанавливаются с помощью Windows Update. Используйте параметр `-Source` для восстановления полезной нагрузки из точки монтирования WIM. В следующем примере восстанавливаются двоичные файлы AD DS и всех необходимых подкомпонентов через Windows Update:
>
> ```
> install-windowsfeature -name ad-domain-services -includeallsubfeature
> ```

Когда установка будет завершена, нужно запустить мастер настройки доменных служб Active Directory (Active Directory Domain Services Configuration Wizard), щелкнув по соответствующей ссылке на странице **Ход установки**; этот мастер используется для настройки роли. Он заменяет файл Dcpromo.exe, который ранее использовался для настройки контроллеров домена. Мастер также запускает файл Adprep.exe для подготовки надлежащей схемы. Если ранее Adprep.exe не запускался отдельно, будет установлен первый контроллер домена на базе Windows Server 2012 в существующем домене/лесу, мастер попросит ввести соответствующие учетные данные, необходимые для запуска команды Adprep. Для подготовки леса нужно предоставить учетные данные члена одной из следующих групп: **Администраторы предприятия** (Enterprise Admins), **Администраторы схемы** (Schema Admins) или **Администраторы домена** (Domain Admins). Для подготовки домена необходимо предоставить учетные данные члена группы **Администраторы домена**. При установке первого контроллера домена только для чтения (read-only domain controller, RODC) в лесу нужно предоставить учетные данные члена группы **Администраторы предприятия**.

Если DNS еще не установлен, будет предложено его установить. Если домен еще не создан, мастер поможет создать домен и настроить Active Directory в новом домене. Мастер также поможет добавить дочерние домены в существующие структуры домена. Для проверки корректности установки домена выполните следующее:

- проверьте журнал событий Directory Service на наличие ошибок;
- убедитесь, что папка SYSVOL доступна для клиентов;
- проверьте работу разрешения имен с помощью DNS;
- проверьте репликацию изменений в Active Directory.

Примечание

В оставшейся части этой главы термины *"каталог"* и *"домены"* относятся к Active Directory и доменам Active Directory соответственно, за исключением случаев, когда автор книги хочет отделить понятие структуры Active Directory от DNS и других типов каталогов.

Помните, что при использовании диспетчера серверов для Windows Server 2012 и функционального уровня леса в Windows Server 2003 или выше все необходимые приготовления выполняются автоматически при разворачивании контроллера домена. Это означает, что мастер конфигурации (Configuration Wizard) автоматически обновляет схему Active Directory леса и домена так, что она будет совместима с Windows Server 2012 в случае необходимости.

Развертывание контроллера домена только для чтения

Когда домен и лес работают на функциональном уровне Windows Server 2003 или выше, а эмулятор первичного контроллера домена (Primary Domain Controller, PDC) работает под управлением Windows Server 2008 или выше, можно развернуть контроллеры домена только для чтения (Read-only domain controller, RODC). Любой контроллер домена под управлением Windows Server 2008 R2 или более поздней версии может быть настроен как RODC. После установки службы DNS-сервера на RODC последний может так же работать, как DNS-сервер только для чтения (read-only DNS, RODNS). В этой конфигурации верны следующие условия.

- RODC тиражирует разделы каталога приложения, которые использует DNS, включая разделы ForestDNSZones и DomainDNSZones. Клиенты могут запрашивать RODNS-сервер для разрешения имен. Однако RODNS-сервер не поддерживает прямые клиентские обновления, поскольку RODNS не регистрирует записи ресурсов ни для какой размещаемой зоны Active Directory.
- Когда клиент пытается обновить DNS-записи, сервер возвращает ссылку. Затем клиент может попытаться обновить DNS-сервер, указанный в ссылке. Посредством репликации в фоновом режиме сервер RODNS пытается получить обновленную запись от DNS-сервера, который и произвел обновление. Этот запрос репликации делается только для измененной записи DNS. Данные зоны или домена не передаются во время этого специального запроса.

Первый установленный в лесу или домене контроллер домена (под управлением Windows Server 2008 R2 или более поздней версии) не может быть контроллером домена только для чтения. Однако можно настроить последующие контроллеры домена как RODC.

Дополнительная информация

У домена и леса должна быть правильная схема, необходимая для поддержки RODC, и также они должны быть подготовлены для работы с RODC. Ранее, в некоторых случаях, это требовало подготовки схем леса и домена для Windows Server 2008 R2 с последующим обновлением схемы леса для RODC. При использовании диспетчера серверов в Windows Server 2012, Windows Server 2003 (и более поздних версиях) вся необходимая подготовка выполняется автоматически как часть развертывания контроллеров домена и контроллеров домена только для чтения.

Компоненты Active Directory для Windows Server 2008 R2

Если производится обновление до Windows Server 2012, но еще не был развернут Windows Server 2008 R2, то нужно знать о связанных компонентах Active Directory. Если использу-

ются Windows Server 2008 R2 и Windows Server 2012 и эти операционные системы развернуты на всех контроллерах домена по всем доменам в лесу Active Directory, то домены могут работать на функциональном уровне домена Windows Server 2008 R2, а лес — на функциональном уровне леса Windows Server 2008 R2. Эти операционные уровни позволяют использовать много средств Active Directory с улучшенной управляемостью и производительностью.

- **Корзина Active Directory** (Active Directory Recycle Bin) — позволяет администраторам отменять ошибочное удаление объектов Active Directory аналогично восстановлению удаленных файлов из обычной Корзины Windows. Работа с Корзиной Active Directory описана в *разд. "Корзина Active Directory" далее в этой главе*.
- **Управляемые учетные записи служб** (Managed service accounts) — представляют специальный тип доменной учетной записи пользователя для управляемых служб, которые сокращают приостановки обслуживания и устраняют другие проблемы путем автоматического управления паролями учетной записи и SPN (Service Principal Name, имя участника службы). Подробную информацию *см. в главе 8*.
- **Управляемые виртуальные учетные записи** (Managed virtual accounts) — представляют специальный тип локальной учетной записи компьютера для управляемых служб, которые обеспечивают доступ к сети с идентификацией компьютера в окружении домена. Подробную информацию *см. в главе 8*.
- **Обеспечение механизма аутентификации** (Authentication Mechanism Assurance) — улучшает процесс аутентификации, позволяя администраторам управлять доступом к ресурсам на основе входа пользователя в систему с применением метода входа на основании сертификата. Таким образом, администратор может определить, какой набор прав доступа есть у пользователя: при входе в систему с использованием смарт-карты применяется один набор прав доступа, при входе в систему без смарт-карты — другой набор прав доступа.

> ***Практический совет***
>
> Технически можно использовать управляемые учетные записи служб в смешанном окружении домена. Однако нужно вручную назначить SPN для управляемых учетных записей служб, и схема Active Directory должна быть совместима с Windows Server 2008 R2 и более поздней версией.

Другие улучшения не нуждаются в повышении функционального уровня домена или леса, но они требуют использования Windows Server 2012.

- **Оффлайн-соединение с доменом** (Offline domain join) — позволяет администраторам предварительно настраивать учетные записи компьютера в домене, чтобы подготовить операционные системы к развертыванию. Это дает возможность компьютерам присоединяться к домену без необходимости связи с контроллером домена.
- **Модуль Active Directory для Windows PowerShell** (Active Directory module for Windows PowerShell) — предоставляет командлеты Windows PowerShell для управления Active Directory. Импортировать модуль Active Directory можно с помощью команды `import-module activedirectory`, введенной в командной строке PowerShell.
- **Центр администрирования Active Directory** (Active Directory Administrative Center) — предоставляет ориентируемый на задачу интерфейс для управления Active Directory. В диспетчере серверов в меню **Средства** (Tools) выберите команду **Центр администрирования Active Directory**.

- **Веб-службы Active Directory** (Active Directory Web Services) — представляют веб-интерфейс для доменов Active Directory.

Более подробно эти компоненты описаны в *главе 7*.

Компоненты Active Directory для Windows Server 2012

Доменные службы Active Directory в ОС Windows Server 2012 имеют множество дополнительных компонентов, предоставляющих администраторам дополнительные опции для реализации и управления Active Directory. В табл. 6.1 приведены ключевые компоненты. Как минимум, эти функции требуют обновления схемы Active Directory в леса и доменах до Windows Server 2012. Также необходимо обновить домен, лес или оба функциональных уровня до режима Windows Server 2012.

Таблица 6.1. *Ключевые компоненты Active Directory для Windows Server 2012*

Компонент	Преимущества	Требования
Активация с помощью Active Directory (Active Directory-based activation)	Позволяет использовать AD для автоматической активации клиентов под управлением Windows 8 и Windows Server 2012. Любой клиент, подключенный к службе, активирован	Volume Licensing; схема Active Directory должна быть обновлена до Windows Server 2012; ключ установлен с использованием роли сервера Volume Activation или командной строки
Средства управления политикой на основе заявок (Claims-based policy controls)	Предоставляет доступ и гибкие политики аудита	Политики на основе заявок должны быть включены для политики контроллера домена по умолчанию; файловые серверы должны работать под управлением Windows Server 2012; в домене должен быть хотя бы один контроллер домена под управлением Windows Server 2012
Создание индекса с задержкой (Deferred index creation)	Позволяет задерживать создание индекса в каталоге, пока не получен UpdateSchemaNow или пока не перезагружен контроллер домена	Контроллер домена должен работать под управлением Windows Server 2012
Расширенная детальная политика паролей (Enhanced Fine-Grained Password Policy)	Позволяет администраторам использовать Центр администрирования Active Directory Windows Server 2012 для создания и управления объектами настроек пароля (password-settings objects, PSO)	Функциональный уровень домена Windows Server 2008 или выше
Расширенная Корзина (Enhanced Recycle Bin)	Позволяет администраторам восстанавливать удаленные объекты с использованием Центра администрирования Active Directory для Windows Server 2012	У доменов должна быть включена Корзина, а также необходим функциональный уровень леса Windows Server 2008 R2 или выше

Таблица 6.1 *(продолжение)*

Компонент	Преимущества	Требования
Групповые управляемые учетные записи службы (Group Managed Service Accounts)	Позволяет нескольким службам использовать одну управляемую учетную запись службы	Схема Active Directory должна быть обновлена до Windows Server 2012; в домене должен быть как минимум один контроллер домена под управлением Windows Server 2012; службы должны быть запущены на Windows Server 2012
Ограниченное делегирование Kerberos по доменам (Kerberos constrained delegation across domains)	Позволяет управляемым учетным записям службы действовать от имени пользователей в доменах и лесах	В каждом домене должен быть как минимум один контроллер домена под управлением Windows Server 2012; сервер переднего плана должен работать под управлением Windows Server 2012; сервер заднего плана должен работать под управлением Windows Server 2003 или более поздней версии
Защита Kerberos (Kerberos with Armoring)	Улучшает безопасность домена; позволяет присоединенному к домену клиенту и контроллеру домена связываться по защищенному каналу	Контроллеры домена Windows Server 2012; функциональный уровень домена Windows Server 2012; на клиентах должна быть включена политика **Require FAST**; на контроллерах домена должна быть включена политика **Поддержка динамического контроля доступа и защита Kerberos** (Support CBAC and Kerberos Armoring)
Внешнее подключение к домену (Off-premises domain join)	Позволяет подключение компьютера к домену по Интернету	Для домена должен быть включен Direct Access, а контроллеры домена должны работать под управлением Windows Server 2012
Предупреждения относительных идентификаторов (Relative ID (RID) soft ceiling and warnings)	Добавляет предупреждения, поскольку глобальное пространство RID израсходовано. Добавляет мягкий потолок в 900 млн RID, что предотвращает переопределение RID администратором	Контроллер домена с ролью RID под управлением Windows Server 2012, остальные — под управлением Windows Server 2012
Интеграция диспетчера серверов (Server Manager integration)	Позволяет выполнять все шаги, необходимые для разворачивания локальных и удаленных контроллеров домена	Windows Server 2012; функциональный уровень леса Windows Server 2003 или выше

Таблица 6.1 *(окончание)*

Компонент	Преимущества	Требования
Клонирование виртуального контроллера домена (Virtual domain controller cloning)	Позволяет безопасно развертывать виртуальные копии контроллеров домена. Также помогает поддерживать состояние контроллера домена	Контроллер домена с ролью **Эмулятор PDC** под управлением Windows Server 2012; виртуальные контроллеры домена также должны работать под управлением Windows Server 2012

Работа со структурами домена

Active Directory предоставляет логические и физические структуры для сетевых компонентов. Логические структуры помогают организовать объекты каталога и управляют сетевыми учетными записями и общими ресурсами. К логическим структурам относятся:

- *организационные подразделения* — подгруппа доменов, которая зеркально отображает бизнес-структуру или функциональную структуру предприятия;
- *домены* — группа компьютеров, которые совместно используют общую базу данных каталога;
- *деревья домена* — один или более доменов, разделяющих непрерывное пространство имен;
- *лес домена* — одно или более деревьев, которые делятся общей информацией каталога.

Физические структуры служат для упрощения сетевых коммуникаций и установки физических границ вокруг сетевых ресурсов. Физические структуры, помогающие отображать физическую структуру сети, следующие:

- *подсети* — сетевая группа с определенным диапазоном IP-адресов и маской сети;
- *сайты* — одна или более подсетей. Сайты используются для настройки доступа к каталогу и репликации.

Домены

Домен Active Directory — это просто группа компьютеров, разделяющих общую базу данных. Имена доменов Active Directory должны быть уникальными. Например, у вас не может быть двух доменов **microsoft.com**, но допустимо иметь родительский домен **microsoft.com** и дочерние домены **seattle.microsoft.com** и **ny.microsoft.com**. Если домен — это фрагмент частной сети, то имя, присвоенное новому домену, не должно конфликтовать с другими существующими доменными именами этой частной сети. Если домен — часть Интернета, то имя, присвоенное новому домену, не должно конфликтовать с другими существующими именами Интернета. Чтобы обеспечить уникальность имени в Интернете, нужно зарегистрировать родительское доменное имя перед его использованием. Домен можно зарегистрировать через любого регистратора доменных имен. Найти текущий список регистраторов можно на сайте InterNIC (**www.internic.net**).

У каждого домена есть собственная политика безопасности и доверительные отношения с другими доменами. Также домены могут охватывать несколько физических расположений. Это означает, что домен может состоять из множества сайтов, а у этих сайтов может

быть много подсетей (рис. 6.1). В базе данных каталога домена находятся объекты, определяющие учетные записи для пользователей, группы и компьютеров, а также совместно используемые ресурсы, такие как принтеры и папки.

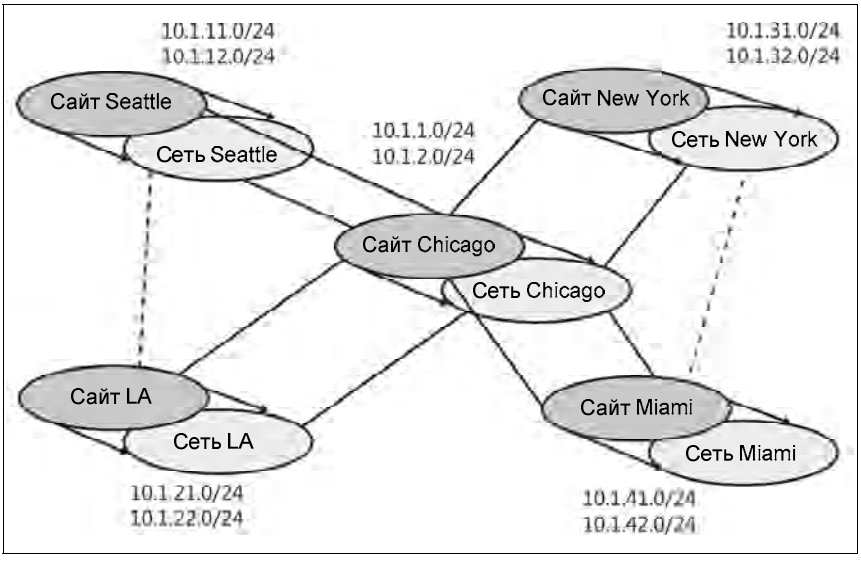


Рис. 6.1. Эта диаграмма сети изображает глобальную сеть (WAN) с несколькими сайтами и подсетями

Примечание

Учетные записи пользователя и группы рассматриваются в *главе 8*. Учетные записи компьютера и различных типов компьютеров, используемых в доменах Windows Server, рассматриваются в *разд. "Работа с доменами Active Directory" далее в этой главе*.

Функции домена ограничены и контролируются функциональным уровнем (режимом работы) домена. Доступно несколько режимов работы домена:

- **Windows Server 2003** — поддерживаются контроллеры домена, работающие под управлением Windows 2003 и более поздних версий;
- **Windows Server 2008** — поддерживаются контроллеры домена под управлением Windows 2008 и более поздних версий;
- **Windows Server 2008 R2** — поддерживаются контроллеры домена под управлением Windows 2008 R2 и Windows Server 2012;
- **Windows Server 2012** — поддерживаются контроллеры домена, работающие только под управлением Windows Server 2012.

Лес и дерево домена

У каждого домена Active Directory есть доменное имя DNS, например **microsoft.com**. Один или более доменов, разделяющих один общий каталог, называются *лесом*. Доменные имена в этом лесу могут быть последовательными или непоследовательными в иерархии имен DNS.

Когда у доменов последовательная структура имен, говорят, что они образуют *дерево* домена. На рис. 6.2 показан пример доменного дерева. Здесь у корневого домена **msnbc.com** есть

два дочерних домена: **seattle.msnbc.com** и **ny.msnbc.com**. Эти домены, в свою очередь, имеют поддомены. Все домены являются частью одного дерева, поскольку у них один и тот же корневой домен.

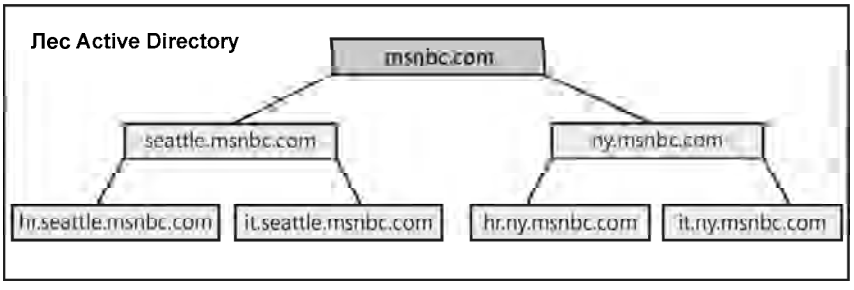


Рис. 6.2. Домены в одном дереве имеют последовательную структуру имен

Если домены в лесу имеют непоследовательную структуру имен DNS, они формируют отдельные деревья в лесу. В одном лесу может быть одно или больше доменных деревьев (рис. 6.3). В этом примере домены **msnbc.com** и **microsoft.com** являются корневыми для разных деревьев в одном лесу.

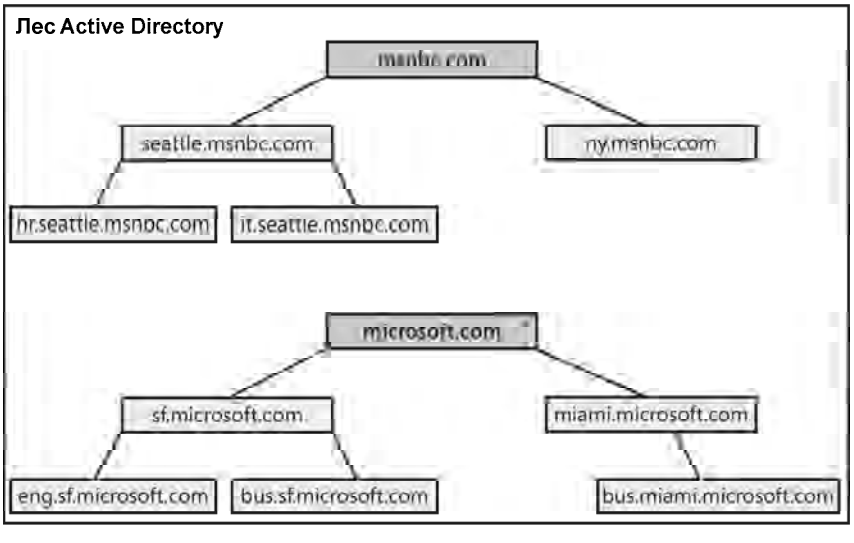


Рис. 6.3. Несколько деревьев в лесу с непоследовательными структурами имен

Получить доступ к доменным структурам можно с помощью оснастки **Active Directory — домены и доверие** (Active Directory Domains and Trust) (рис. 6.4). Данную оснастку можно вызвать в консоли управления Microsoft (Microsoft Management Console, MMC). Также можно запустить ее из меню **Средства** диспетчера серверов. В оснастке находятся отдельные записи для каждого корневого домена. На рис. 6.4 активный домен — HOME.DOMAIN.

Функции леса ограничены и контролируются функциональным уровнем леса (режим работы леса). Доступно несколько функциональных уровней леса:

- **Windows Server 2003** — поддерживаются контроллеры домена, работающие под управлением Windows 2003 и более поздних версий;

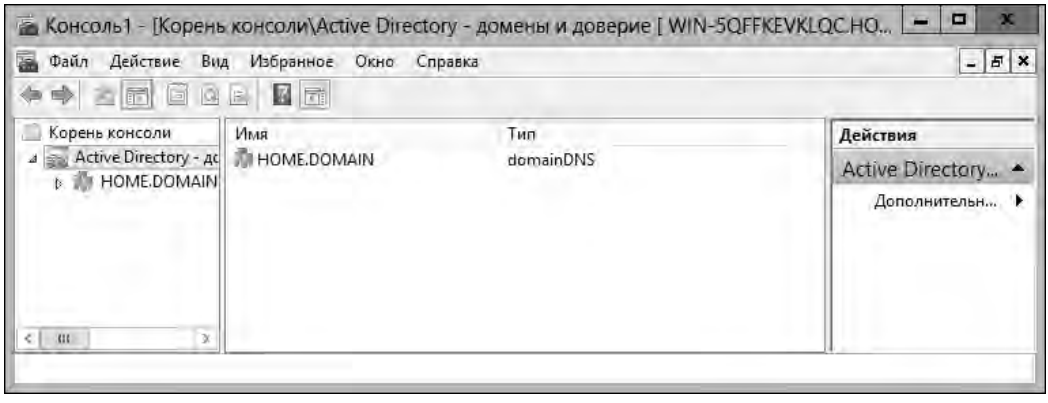


Рис. 6.4. Используйте оснастку **Active Directory — домены и доверие** для работы с доменами, деревьями и лесом

- **Windows Server 2008** — поддерживаются контроллеры домена под управлением Windows 2008 и более поздних версий;
- **Windows Server 2008 R2** — поддерживаются контроллеры домена под управлением Windows 2008 R2 и Windows Server 2012;
- **Windows Server 2012** — поддерживаются контроллеры домена, работающие только под управлением Windows Server 2012.

Когда все домены в лесу будут работать на функциональном уровне леса Windows Server 2003, будут заметны улучшения по сравнению с более ранними реализациями в эффективности глобальной репликации и репликации каталога. Поскольку значения связи реплицируются, администратор получит улучшенную репликацию между сайтами (intersite-репликацию). Администратор может деактивировать объекты класса схемы и атрибуты; использовать динамические вспомогательные классы; переименовывать домены; создавать односторонние, двухсторонние и переходные доверия леса.

Режим работы леса Windows Server 2008 предлагает последовательные усовершенствования производительности и функций функционального уровня леса Windows Server 2003. Когда все домены в лесу будут работать в этом режиме, станут заметны улучшения репликации внутри сайта (intrasite) и между сайтами (intersite) по всей организации. Также контроллеры домена могут использовать репликацию распределенной файловой системы (Distributed File System, DFS), а не службу репликации файлов (File Replication Service, FRS). Кроме того, принципалы безопасности Windows Server 2008 не создаются, пока эмулятор PDC в корневом домене леса не работает под управлением Windows Server 2008.

У функционального уровня леса Windows Server 2008 R2 есть еще несколько дополнительных функций: Корзина Active Directory, управляемые учетные записи службы и механизм аутентификации.

Несмотря на то, что Active Directory для Windows Server 2012 улучшен, большинство этих улучшений требуют использования только контроллеров домена и схемы под управлением Windows Server 2012. Основное исключение — Защита Kerberos — требует функциональный уровень домена Windows Server 2012.

Вообще говоря, нельзя понизить функциональный уровень леса после его повышения. Однако после повышения функционального уровня до Windows Server 2012 он может быть понижен Windows Server 2008 R2. Если Корзина Active Directory не включена, можно понизить функциональный уровень леса с Windows Server 2012 до Windows Server 2008 R2 или

до Windows Server 2008; либо с Windows Server 2008 R2 до Windows Server 2008. Нельзя понизить функциональный уровень домена до Windows Server 2003 или еще ниже.

Организационные подразделения

Организационные подразделения, или организационные единицы, являются подгруппами в доменах, которые часто зеркально отражают функциональную или деловую структуру организации. Также можно представлять организационные подразделения как логические контейнеры, в которые помещаются учетные записи, общие ресурсы и другие организационные подразделения. Например, можно создать организационные подразделения HumanResources, IT, Engineering и Marketing для домена **microsoft.com**. Позже можно развернуть эту схему, включив дочерние подразделения.

Объекты, помещенные в организационное подразделение, могут прибыть только из родительского домена. Например, организационное подразделение, связанное с **seattle.microsoft.com**, может содержать объекты только для этого домена. Нельзя добавить объекты из **ny.microsoft.com** в эти контейнеры, но можете создать отдельное организационное подразделение, чтобы зеркально отразить деловую структуру **seattle.microsoft.com**.

Организационные подразделения полезны в организационных объектах для отражения деловой или функциональной структуры. Но это не единственная причина использовать организационное подразделение. Есть и другие причины.

- Организационные подразделения позволяют назначить групповые политики небольшому числу ресурсов домена без применения этих политик ко всему домену. Это помогает устанавливать и управлять групповыми политиками на соответствующем уровне в предприятии.
- Организационные подразделения создают небольшие, более управляемые представления объектов каталога в домене. Это помогает более эффективно управлять ресурсами.
- Организационные подразделения позволяют делегировать полномочия и легко управлять административным доступом к доменным ресурсам. Это помогает управлять объемом полномочий администратора в домене. Можно предоставить пользователю *A* административные полномочия для одного организационного подразделения, а пользователю *B* — для всех организационных подразделений в домене.

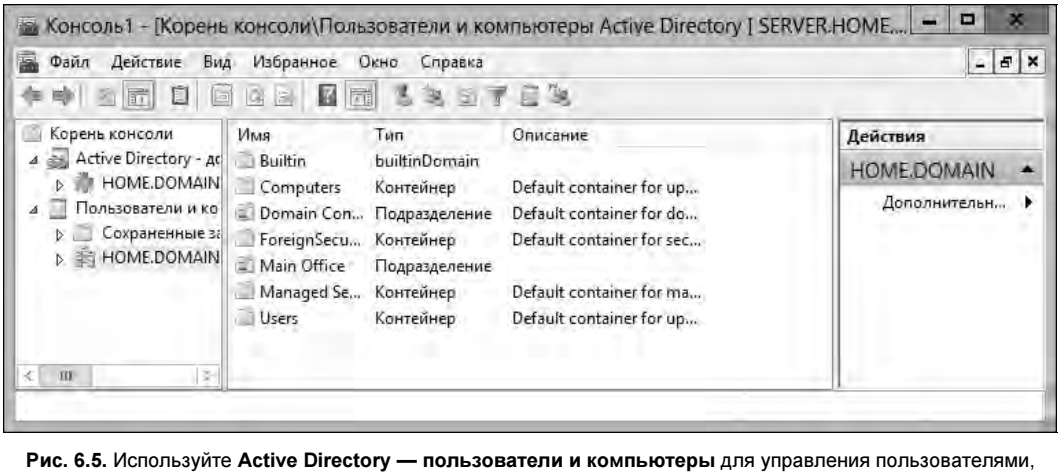


Рис. 6.5. Используйте **Active Directory — пользователи и компьютеры** для управления пользователями, группами, компьютерами и организационными подразделениями

В оснастке **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers) представлены в виде папок (рис. 6.5). Эта утилита выполнена в виде оснастки для MMC, ее также можно запустить из меню **Средства** диспетчера серверов.

Сайты и подсети

Сайт — это группа компьютеров в одной или более IP-подсети. Сайты используются для отображения физической структуры вашей сети. Отображение сайта независимо от логических структур домена, поэтому нет необходимости устанавливать связь между физической структурой сети и ее логической доменной структурой. С помощью Active Directory можно создавать множество сайтов в пределах одного домена или создать один сайт, который будет обслуживать несколько доменов. Диапазоны IP-адресов, используемые сайтом и пространством имен домена, также не связаны.

Можно подумать о подсети, как о группе сетевых адресов. В отличие от сайтов, где могут быть разные диапазоны IP-адресов, у подсетей есть только один определенный диапазон IP-адресов и сетевая маска. Имена подсетей выводятся в форме "сеть/битовая маска", например, 192.168.19.0/24. Здесь, адрес сети 192.168.19.9 и маска 255.255.255.0 комбинируются для создания имени подсети 192.168.19.0/24.

> ***Примечание***
>
> Не беспокойтесь, не нужно знать, как создаются имена подсетей. В большинстве случаев необходимо ввести адрес сети и маску сети, а Windows Server самостоятельно сгенерирует имя.

Компьютеры объединяются в сайты на основе их расположения в подсети или ряде подсетей. Если компьютеры в подсетях могут эффективно взаимодействовать друг с другом, говорят, что они хорошо соединены. Идеально, если сайты состоят из подсетей и компьютеров, которые хорошо соединены. Если подсети не являются хорошо соединенными, возможно, нужно установить несколько сайтов. Есть несколько преимуществ хорошего соединения.

- Когда клиенты входят в домен, процесс аутентификации сначала ищет контроллеры домена, которые находятся в том же сайте, что и клиент. Это означает, что сначала используются локальные контроллеры домена, если это возможно, что в итоге локализует сетевой трафик и ускоряет процесс аутентификации.
- Информация каталога тиражируется чаще в пределах сайта, чем между сайтами. Это уменьшает сетевой трафик, вызванный репликацией, а также позволяет убедиться, что локальные контроллеры домена быстро получили актуальную информацию. Также можно использовать соединения сайта, чтобы настроить, как информация каталога будет реплицироваться между сайтами. Контроллер домена, выделенный для осуществления межсайтовой репликации, называется сервером-плацдармом (bridgehead-сервером). Определяя сервер-плацдарм для обработки репликации между сайтами, администратор помещает основную нагрузку на определенный сервер, а не на любой доступный сервер сайта.

Доступ к сайтам и подсетям администратор получает через утилиту **Active Directory — сайты и службы**. Данная утилита — оснастка для MMC, и ее можно добавить к любой обновляемой консоли. Также можно запустить оснастку **Active Directory — сайты и службы** из меню **Средства** диспетчера серверов.

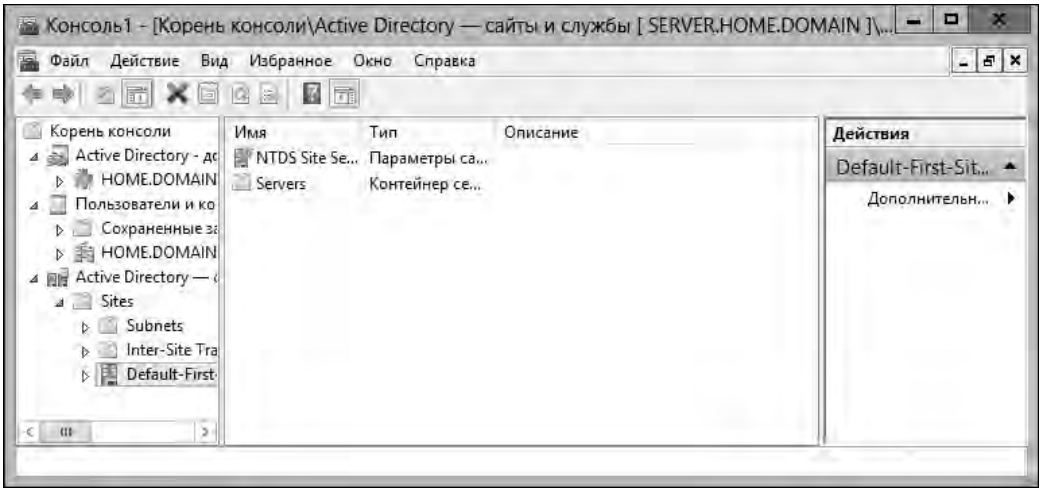


Рис. 6.6. Используйте **Active Directory — сайты и службы**, чтобы управлять сайтами и подсетями

Работа с доменами Active Directory

Хотя можно настроить и Active Directory, и DNS в одной сети Windows Server, у доменов Active Directory и DNS-доменов разное назначение. Домены Active Directory помогают управлять учетными записями, ресурсами и безопасностью. Домены DNS устанавливают доменную иерархию и преимущественно применяются для разрешения имен. Операционная система Windows Server использует DNS для преобразования символьных имен **zeta.microsoft.com** в числовые TCP/IP-адреса, например, 172.16.18.8. Дополнительная информация о DNS и о DNS-доменах приводится в *главе 16*.

Использование компьютеров с Active Directory

Пользовательские компьютеры под управлением профессиональных или бизнес-версий Windows могут полностью использовать Active Directory. Эти компьютеры получают доступ к сети как клиенты Active Directory и имеют полный доступ к функциям Active Directory. Как клиенты, эти системы могут использовать переходные доверительные отношения, которые существуют в пределах дерева или леса. Переходные доверительные отношения не устанавливаются явно. Вместо этого доверие устанавливает автоматически на основе структуры леса и набора полномочий в лесу. Эти отношения позволяют авторизованным пользователям получать доступ к ресурсам в любом домене в лесу.

Серверы предоставляют услуги другим системам и могут действовать как контроллеры домена или рядовые серверы. Контроллеры домена отличаются от рядового сервера, поскольку на нем выполняются доменные службы Active Directory (Active Directory Domain Services). Можно превратить рядовой сервер в контроллер домена, установив на него доменные службы Active Directory. Также можно понизить роль контроллера домена до рядового сервера, удалив AD DS. Для повышения или понижения роли сервера используется мастер установки доменных служб Active Directory (Active Directory Sites and Services) (Dcpromo.exe).

В домене может быть один или более контроллеров домена. Когда у домена есть несколько контроллеров домена, они автоматически реплицируют данные каталога, используя модель

репликации multi-master. Данная модель позволяет любому контроллеру домена обрабатывать изменения каталога и затем реплицировать эти изменения на другие контроллеры домена.

Поскольку используется мультимастер структуры домена, у всех контроллеров домена одинаковая ответственность. Однако администратор может назначить приоритет некоторым контроллерам домена для выполнения определенного рода задач, например, назначить какой-то сервер сервером-плацдармом, в результате он получит приоритет в репликации информации каталога на другие сайты. Кроме того, некоторые задачи лучше всего выполняются единственным сервером. Сервер, обрабатывающий этот тип задачи, называется владельцем (хозяином) операций (operation master). Есть пять ролей FSMO (Flexible Single Master Operations, ролей, выполняющихся одним сервером), которые будут рассмотрены чуть позже в этой главе.

Начиная с Windows 2000 (и более поздних версий) компьютеры, присоединяющиеся к домену, имеют учетную запись компьютера. Подобно другим ресурсам, учетные записи компьютера хранятся в Active Directory, как объекты. Используйте учетные записи компьютера, чтобы управлять доступом к сети и ее ресурсам. Компьютер получает доступ к домену с помощью своей учетной записи, которая аутентифицируется перед предоставлением компьютеру доступа к сети.

> ***Практический совет***
>
> Контроллеры домена используют глобальный каталог Active Directory для аутентификации компьютера и пользователя. Если глобальный каталог недоступен, войти в домен могут только члены группы **Администраторы домена**, поскольку информация о членстве в группе хранится в глобальном каталоге, и эта информация нужна для аутентификации. В Windows 2003 (и более поздних версиях) серверы кэшируют информацию о членстве в универсальной группе, что решает эту проблему. Более подробную информацию *см. в разд. "Структура каталога" далее в этой главе*.

Работа с функциональными уровнями домена

Для поддержки структур домена Active Directory поддерживает следующие функциональные уровни домена.

- **Режим Windows Server 2003.** Когда домен работает в режиме Windows Server 2003, каталог поддерживает контроллеры домена, работающие под управлением Windows Server 2008 R2, Windows Server 2008 и Windows Server 2003. Домен, работающий в режиме Windows Server 2003, может использовать универсальные группы, вложение группы, преобразование типов группы, простое переименование контроллера домена, обновление метки времени входа в систему и номера версий ключа Kerberos KDC.
- **Режим Windows Server 2008.** Когда домен работает в режиме Windows Server 2008, каталог поддерживает контроллеры домена, работающие под управлением Windows Server 2008 и Windows Server 2008 R2. Контроллеры домена Windows Server 2003 больше не поддерживаются. Домен, работающий в режиме Windows Server 2008, может использовать дополнительные функции Active Directory, в том числе сервис репликации DFS для расширенной репликации внутри сайта и между сайтами.
- **Режим Windows Server 2008 R2.** Когда домен работает в режиме Windows Server 2008 R2, каталог поддерживает контроллеры домена, работающие только под управлением Windows Server 2008 R2. Контроллеры домена Windows Server 2003 и Windows Server 2008 больше не поддерживаются. Домен, работающий в режиме Windows Server 2008

R2, может использовать Корзину Active Directory, управляемые учетные записи служб, механизм обеспечения безопасности и другие важные расширения Active Directory.

- **Режим Windows Server 2012.** Когда домен работает в режиме Windows Server 2012, каталог поддерживает контроллеры домена, работающие только под управлением Windows Server 2012. Контроллеры домена, работающие под управлением Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, больше не поддерживаются. Схема Active Directory для Windows Server 2012 поддерживает много расширений, но только функция Защита Kerberos требует этого режима.

Больше нельзя понизить функциональный уровень (режим работы) домена после того, как он будет повышен. Однако при повышении функционального уровня домена до Windows Server 2008 R2 или Windows Server 2012, а функционального уровня леса — Windows Server 2008 или ниже, есть возможность отката функционального уровня домена обратно на Windows Server 2008 или Windows Server 2008 R2. Нельзя откатить функциональный уровень домена обратно до Windows Server 2003 или ниже.

Использование функционального уровня Windows Server 2003

Каждый домен в вашем предприятии должен работать на функциональном уровне Windows Server 2003 или выше. Это дает уверенность в том, что компьютеры в ваших доменах могут использовать множественные улучшения в Active Directory. После того как избавитесь от структур Windows NT и обновите структуры Windows 2000 в организации, появится возможность изменить функциональный уровень на Windows Server 2003.

Перед обновлением контроллеров домена Windows 2000 необходимо подготовить домен для обновления. Для этого нужно обновить схемы леса и домена так, чтобы они были совместимы с доменами Windows Server 2003. Необходимое обновление может автоматически выполнить утилита Adprep.exe. Все, что нужно — это запустить утилиту на мастере операций схемы в лесу, а затем на мастере операций инфраструктуры для каждого домена в лесу. Как обычно, необходимо протестировать любую процедуру в лаборатории перед осуществлением ее в производственном окружении.

На инсталляционном носителе Windows Server 2003 находятся утилита Adprep и вспомогательные файлы в подпапке i386. Для обновления выполните следующие действия:

1. На хозяине операций схемы в лесу выполните команду `<cdrom>:\i386\adprep.exe /forestprep`. Необходимо использовать учетную запись администратора, являющегося членом группы **Администраторы предприятия** (Enterprise Admins), **Администраторы схемы** (Schema Admin) или **Администраторы домена** (Domain Admins) в лесу корневого домена.
2. На мастере операций инфраструктуры для каждого домена в лесу запустите `<cdrom>:\i386\adprep.exe /domainprep`. Нужно использовать учетную запись члена группы **Администраторы домена** в соответствующем домене.

> ***Примечание***
>
> Для определения, какой сервер является текущим мастером операций схемы для домена, откройте окно командной строки и введите команду `dsquery server –hasfsmo schema`. Служба каталогов вернет строку, содержащую имя сервера, например,
>
> `"CN=CORPSERVER01,CN=Servers,CN=Default-First-Site-Name,CN=Sites, CN=Configuration, DC=microsoft, DC=com."`.
>
> В данном случае мастером операций схемы является CORPSERVER1 в домене **microsoft.com**.

Примечание

Для определения, какой сервер является текущим мастером операций инфраструктуры, откройте окно командной строки и введите команду `dsquery server –hasfsmo infr`.

Практический совет

Вообще говоря, все, что можно ввести в командной строке, можно ввести в оболочке PowerShell. Это возможно, поскольку PowerShell ищет внешние команды и утилиты как часть нормальной обработки. Пока внешняя команда или утилита находятся в каталоге, указанном в переменной окружения `PATH`, PowerShell может запустить эту команду или утилиту. Однако нужно учитывать порядок выполнения PowerShell: 1) альтернативные или определенные в профиле псевдонимы; 2) встроенные или определенные в профиле функции; 3) командлеты или ключевые слова языка; 4) сценарии с расширением ps1; 5) внешние команды, утилиты, файлы. Таким образом, если у элемента, поиск которого происходит на шагах 1—4, такое же имя, как у запускаемой команды, будет выполнен этот элемент, а не ожидаемая команда.

После обновления серверов можно повысить функциональный уровень домена и леса для получения дополнительных функций Active Directory, которые предоставляются функциональным уровнем Windows Server 2003. Помните, что как только будет произведено обновление, можно использовать лишь ресурсы Windows Server 2003 и более поздних версий в домене и нельзя будет вернуться к старому режиму. Необходимо использовать режим Windows Server 2003, только если не нужны старые структуры доменов Windows NT, резервные контроллеры доменов Windows NT (BDC) или доменные структуры Windows 2000.

Использование функционального уровня Windows Server 2008

После того как будут обновлены структуры Windows 2000 и Windows Server 2003 в организации, можно изменить функциональный уровень до режима Windows Server 2008.

Перед обновлением контроллеров домена на базе Windows Server 2003 необходимо подготовить домен для Windows Server 2008. Чтобы обновить схемы леса и домена так, чтобы они были совместимы с доменами Windows Server 2008, используйте утилиту Adprep.exe. Выполните следующие инструкции:

1. На мастере операций схемы в лесу скопируйте содержимое папки Sources\Adprep с инсталляционного носителя Windows Server 2008 в локальную папку и запустите `adprep /forestprep`. Если планируете установить контроллеры домена только для чтения, запустите `adprep /rodcprep`. Также нужно использовать учетную запись администратора, который является членом группы **Администраторы предприятия**, **Администраторы схемы** или **Администраторы домена в лесу корневого домена** (Domain Admins in the forest root domain).
2. На мастере операций инфраструктуры для каждого домена в лесу скопируйте содержимое папки Sources\Adprep с установочного диска Windows Server 2008 в локальную папку, а затем выполните команду `adprep /domainprep`. Нужно использовать учетную запись члена группы **Администраторы домена** в соответствующем домене.
3. Если ранее не выполнили `adprep /domainprep /gpprep` в каждом домене, нужно вручную выполнить эту задачу.

   Диспетчер серверов для Windows Server 2012 не подготовит групповую политику. Обратите внимание на то, что групповая политика должна быть подготовлена только в первый раз, когда развертываете контроллеры домена на базе Windows Server 2003 SP1 или поздних версий. Команда `adprep /gpprep` модифицирует записи управления доступом

(Access Control Entries, ACE) для всех объектов групповой политики в каталоге SYSVOL для предоставления доступа только чтения всем контроллерам домена предприятия. Этот уровень доступа требуется для поддержки результирующей политики (Resultant Set of Policy, RSoP), для политики на базе сайта и заставляет службу репликации файлов NT (NT File Replication Service, NTFRS) снова отправить все GPO всем контроллерам домена.

Примечание

Для определения, какой сервер является текущим мастером операций схемы для домена, откройте окно командной строки и введите команду `dsquery server –hasfsmo schema`. Для определения, какой сервер является текущим мастером операций инфраструктуры, откройте окно командной строки и введите команду `dsquery server –hasfsmo infr`

После обновления всех ваших контроллеров домена до Windows Server 2008 можно повысить функциональный уровень домена и леса для получения дополнительных функций Active Directory. Если сделать это, можно будет использовать только ресурсы Windows Server 2008 (или поздних версий) и нельзя будет вернуться к прежнему режиму. Необходимо использовать режим Windows Server 2008, только когда больше нет необходимости в старых доменных структурах Windows NT, Windows NT BDC или доменных структурах Windows 2000 и Windows Server 2003.

Использование функционального уровня Windows Server 2008 R2

Системы Windows Server 2008 R2 и Windows Server 2012 работают только на 64-битном оборудовании. Поэтому необходимо устанавливать Windows Server 2008 R2 и Windows Server 2012 на новом оборудовании, а не на "железе", разработанном для более ранних версий Windows Server.

Перед обновлением контроллеров домена Windows Server 2008 необходимо подготовить домен для Windows Server 2008 R2. Чтобы сделать это, нужно использовать утилиту Adprep.exe для обновления схем леса и домена так, чтобы они были совместимы с Windows Server 2008 R2. Выполните следующие действия:

1. На мастере операций схемы в лесу скопируйте содержимое папки Sources\Adprep с установочного носителя Windows Server 2008 R2 в локальную папку и запустите команду `adprep /forestprep`. Если планируете установить контроллеры домена только для чтения, также запустите `adprep /rodcprep`. Нужно использовать учетную запись администратора, который является членом группы **Администраторы предприятия**, **Администраторы схемы** или **Администраторы домена в лесу корневого домена**.
2. На мастере операций инфраструктуры для каждого домена в лесу скопируйте содержимое папки Sources\Adprep с установочного диска Windows Server 2008 R2 в локальную папку, а затем выполните команду `adprep /domainprep`. Нужно использовать учетную запись члена группы **Администраторы домена** в соответствующем домене.

Как обычно, сначала протестируйте все в лаборатории, а затем уже в производственном окружении.

Примечание

Для определения, какой сервер является текущим мастером операций схемы для домена, откройте окно командной строки и введите команду `dsquery server –hasfsmo schema`. Для определения, какой сервер является текущим мастером операций инфраструктуры, введите команду `dsquery server –hasfsmo infr`.

После обновления всех контроллеров домена до Windows Server 2008 R2 можно повысить функциональный уровень домена и леса с целью получения дополнительных функций Active Directory. После этого можно использовать только ресурсы Windows Server 2008 R2 (или поздних версий) и нельзя вернуться к прежнему режиму. Необходимо использовать режим Windows Server 2008 R2, только когда больше нет необходимости в старых доменных структурах Windows NT, Windows NT BDC или доменных структурах Windows 2000, Windows Server 2003, Windows Server 2008.

Использование функционального уровня Windows Server 2012

Как и Windows Server 2008 R2, Windows Server 2012 работает только на 64-битном оборудовании, и вполне возможно, что придется обновить ваши аппаратные средства перед установкой Windows Server 2012. В отличие от ранних выпусков Windows Server, операции обновления домена и леса больше не нужно выполнять вручную. Вместо этого все необходимые операции будут выполнены автоматически (когда развернете контроллер домена на базе Windows Server 2012) при условии, что используете диспетчер серверов для Windows Server 2012 и функциональный уровень леса — Windows Server 2003 или выше. Это означает, что мастер настройки автоматически обновит схемы леса и домена.

При желании можно вручную выполнить подготовительные операции для Windows Server 2012. Для этого используйте утилиту Adprep.exe. Инструкции подобны описанным ранее.

После обновления всех контроллеров домена до Windows Server 2012 можно повысить функциональный уровень леса и домена для получения последних функций Active Directory. Если сделать это, можно будет использовать только ресурсы Windows Server 2012 в своем домене.

Повышение или понижение функциональности домена и леса

Домены, работающие на функциональном уровне Windows Server 2003 или выше, могут использовать универсальные группы, вложение группы, преобразование типов группы, обновление меток времени входа в систему и номера версий ключа Kerberos KDC. В этом режиме (или более высоком) администраторы могут делать следующее:

- переименовывать контроллеры домена без предварительного превращения их в рядовые серверы;
- переименовывать домены, работающие на контроллерах доменов под управлением Windows Server 2003 (или выше);
- создавать расширенные двусторонние доверия между двумя лесами;
- реструктурировать домены в доменной иерархии путем их переименования и перемещения на разные уровни;
- использовать улучшения репликации для отдельных членов группы и глобальных каталогов.

По сравнению с более ранними реализациями у леса, работающего на функциональном уровне Windows Server 2003 или более высоком, более эффективная глобальная репликация каталога и репликация внутри сайта и между сайтами, также есть возможность установки односторонних, двусторонних и переходных доверий леса.

Практический совет

Процесс обновления домена и леса может генерировать много сетевого трафика, поскольку информация реплицируется по сети. Иногда весь процесс обновления может занять 15 минут или больше. За это время можно испытать задержку в скорости отклика при взаимодействии с серверами, поэтому лучше запланировать обновление вне нормального рабочего времени. Также нужно полностью протестировать совместимость с существующими приложениями (особенно со старыми приложениями), прежде чем выполнить эту операцию.

Повысить функциональный уровень домена можно с помощью следующих действий:

1. Запустите оснастку **Active Directory — домены и доверие**. В дереве консоли щелкните правой кнопкой мыши по домену, а затем выберите команду **Изменение режима работы домена** (Raise Domain Functional Level).

   В окне **Повышение режима работы домена** (Raise Domain Functional Level) будет отображено текущее имя домена и его функциональный уровень.

2. Для изменения функциональности домена выберите новый функциональный уровень домена из предоставленного списка, а затем нажмите кнопку **Повысить** (Raise).

3. Нажмите кнопку **OK**. Новый функциональный уровень домена будет реплицирован каждому контроллеру домена. Эта операция может занять некоторое время в большой организации.

Можно повысить функциональный уровень леса с помощью следующих действий:

1. Откройте оснастку **Active Directory — домены и доверие**. В дереве консоли щелкните правой кнопкой мыши по узлу **Active Directory — домены и доверие**, а затем выберите команду **Изменение режима работы леса** (Raise Forest Functional Level).

   В окне **Повышение режима работы леса** (Raise Forest Functional Level) будет отображено имя леса и текущий режим его работы.

2. Для изменения режима работы леса выберите новый функциональный уровень леса и нажмите кнопку **Повысить**.

3. Нажмите кнопку **OK**. Новый режим работы леса будет реплицирован на каждый контроллер домена в лесу. В большой организации данная операция займет некоторое время.

Есть и другой способ повысить режим работы домена или леса — использовать Центр администрирования Active Directory (Active Directory Administrative Center). Эта утилита доступна из меню **Средства** диспетчера серверов. Для повышения уровня работы домена выполните следующие действия:

1. В Центре администрирования Active Directory по умолчанию для администрирования открыт локальный домен. Если нужно работать с другим доменом, в меню **Управление** (Manage) выберите команду **Добавить узлы перехода** (Add Navigation Nodes). В окне **Добавление узлов перехода** (Add Navigation Nodes) выберите домен и нажмите кнопку **OK**.

2. В левой панели выберите домен, с которым хотите работать. На панели **Задачи** (Tasks) выберите задачу **Повышение режима работы домена** (Raise Domain Functional Level). В одноименном окне будет отображено текущее имя домена и его функциональный уровень.

3. Для изменения функциональности домена выберите новый функциональный уровень домена из предоставленного списка, а затем нажмите кнопку **Повысить** (Raise).

4. Нажмите кнопку **OK**. Новый функциональный уровень домена будет реплицирован каждому контроллеру домена. Эта операция может занять некоторое время в большой организации.

Следующие действия позволяют повысить функциональный уровень леса:

1. В Центре администрирования Active Directory выберите домен, с которым хотите работать. На панели **Задачи** (Tasks) выберите задачу **Повышение режима работы леса** (Raise Forest Functional Level). В одноименном окне будет отображено имя леса и текущий режим его работы.
2. Для изменения режима работы леса выберите новый функциональный уровень леса и нажмите кнопку **Повысить**.
3. Нажмите кнопку **OK**. Новый режим работы леса будет реплицирован на каждый контроллер домена в лесу. В большой организации данная операция займет некоторое время.

Обычно нельзя понизить режим работы леса или домена после того, как он был повышен. Однако есть определенные исключения, как было ранее упомянуто в этой главе. Имейте в виду, что если включена Корзина Active Directory (Active Directory Recycle Bin), то нельзя будет понизить функциональный уровень леса.

Структура каталога

У Active Directory есть много компонентов, ведь он основан на многих технологиях. Данные каталога сделаны доступными для пользователей и компьютеров через хранилища данных и глобальные каталоги. Несмотря на то, что задачи Active Directory наиболее влияют на хранилище данных, глобальные каталоги одинаково важны, потому что они используются во время входа в систему и для поиска информации. Фактически, если глобальный каталог недоступен, типичные пользователи не смогут войти в домен. Единственный способ изменить это поведение заключается в локальном кэшировании состава универсальной группы. У кэширования состава универсальной группы есть преимущества и недостатки, которые мы рассмотрим чуть позже.

Администратор получает доступ и распределяет данные Active Directory с помощью протоколов доступа к каталогу и репликации. Протоколы доступа к каталогу позволяют клиентам связываться с компьютерами, на которых выполняются службы Active Directory. Репликация нужна, чтобы убедиться, что обновления данных отправлены контроллерам доменов. Несмотря на то что мультимастер репликации — основной метод тиражирования обновлений, некоторые изменения в данных должны быть обработаны только индивидуальными контроллерами домена, которые называются *хозяевами операций* (operation master). Одна из функций, которая также изменяет способ работы мультимастера репликации — Application Directory Partitions (разделы каталога приложений).

С помощью разделов каталога приложений администраторы предприятия (принадлежат к группе **Администраторы предприятия**) могут создавать разделы репликации в лесу доменов. Эти разделы — логические структуры, используемые для управления репликацией данных в лесу доменов. Например, можно создать раздел, чтобы строго управлять репликацией информации DNS в домене, предотвращая репликацию информации DNS на другие системы.

Раздел каталога приложения может появиться как дочерний элемент домена, дочерний элемент другого раздела приложения или новое дерево в лесу доменов. Копии раздела каталога приложения можно сделать доступными на любом контроллере домена Active Directory,

работающем под управлением Windows Server 2008 (или более поздних версий), в том числе серверы глобального каталога. Несмотря на то что разделы каталога приложения полезны в больших доменах и лесах, они добавляют издержки с точки зрения планирования, администрирования и обслуживания.

Хранилище данных

Хранилище данных содержит информацию об объектах, таких как учетные записи, совместно используемые ресурсы, организационные подразделения и групповые политики. Другое название хранилища данных — *каталог*, что относится к самому Active Directory. На контроллерах домена хранится файл Ntds.dit. Расположение этого файла устанавливается при установке Active Directory, он должен находиться на системном диске с файловой системой NTFS, отформатированном для использования с Windows Server 2008 или более поздними версиями. Также можно хранить данные каталога отдельно от основного хранилища данных. Так лучше делать для групповых политик, сценариев и других типов публичной информации, которая хранится на общем системном томе (SYSVOL).

Предоставление общего доступа к информации каталога называется *публикацией*. Например, можно опубликовать информацию о принтере путем предоставления к нему общего доступа по сети. Точно так же публикуется информация о папке — путем предоставления к ней общего доступа.

Контроллеры домена тиражируют большинство изменений в хранилище данных способом мультимастера. Администраторы сетей небольшого и среднего размера редко управляют репликацией хранилища данных. Репликация обрабатывается автоматически, но можно настроить ее, чтобы она соответствовала потребностям крупных организаций или организаций с особыми требованиями.

Не все данные каталога реплицируются. Вместо этого реплицируется только публичная информация, попадающая в одну из трех категорий:

- *данные домена* — содержат информацию об объектах домена: учетные записи, общие ресурсы, организационные подразделения и групповые политики;
- *конфигурационные данные* — описывают топологию каталога. Содержат список всех доменов, деревьев домена и леса, также расположений контроллеров домена и глобальных серверов каталога;
- *данные схемы* — описывают все объекты и типы данных, которые могут храниться в каталоге. Схема по умолчанию, предоставляемая с Windows Server, описывает объекты учетных записей, объекты общих ресурсов и др. Можно расширить схему по умолчанию, определяя новые объекты и атрибуты или добавляя атрибуты в существующие объекты.

Глобальные каталоги

Когда состав универсальной группы не кэшируется локально, глобальные каталоги включают сетевой вход в систему, предоставляя информацию о составе универсальной группы при инициировании процесса входа в систему. Также глобальные каталоги включают поиск по каталогу по всем доменам леса. Контроллер домена, определяемый как глобальный каталог, хранит в каталоге полную копию всех объектов для его домена и частичную копию (partial replica) для всех других доменов в лесу.

Примечание

Частичные копии используются, поскольку для входа в систему и операций поиска необходимы только определенные свойства объектов. Частичная репликация означает, что по сети будет передаваться меньший объем данных, сокращающий размер трафика.

По умолчанию первый установленный в домене контроллер назначается глобальным каталогом. Если в домене есть только один контроллер домена, то контроллер домена и глобальный каталог — один и тот же сервер. В противном случае глобальный каталог находится на специально настроенном контроллере домена. Также можно добавить глобальные каталоги в домен, чтобы улучшить время отклика при входе в систему и поиске информации. Рекомендуется иметь один глобальный каталог для сайта в пределах домена.

Контроллеры домена, размещающие глобальный каталог, должны быть хорошо соединены с контроллерами домена, действующими как владельцы инфраструктуры. Роль владельца инфраструктуры (infrastructure master) — одна из пяти операций, которую можно назначить контроллеру домена. В домене мастер инфраструктуры отвечает за обновление ссылок на объект. Хозяин инфраструктуры делает это, сравнивая ее данные с данными из глобального каталога. Если хозяин инфраструктуры находит устаревшие данные, он запрашивает обновленные данные из глобального каталога. После этого мастер инфраструктуры реплицирует изменения другим контроллерам домена. Подробно роли мастера операций рассмотрены в *разд. "Роли FSMO" далее в этой главе*.

Если в домене находится только один контроллер, можно назначить роль мастера инфраструктуры и роль глобального каталога на один и тот же сервер. Когда в домене два или больше контроллера, глобальный каталог и хозяин инфраструктуры должны располагаться на отдельных контроллерах домена. Если это не так, тогда хозяин инфраструктуры не сможет найти устаревшие данные, и больше никогда не будет реплицировать изменения. Единственное исключение — ситуация, когда все контроллеры домена содержат глобальный каталог. В этом случае нет разницы, какой из них является мастером инфраструктуры.

Одна из основных причин сконфигурировать дополнительные глобальные каталоги в домене заключается в том, чтобы убедиться в доступности каталога при входе в систему и при поиске по каталогу. Снова, если у домена есть только один глобальный каталог, который не доступен, и нет локального кэширования состава универсальных групп, обычные пользователи не смогут войти в систему, а те, которые уже вошли, не смогут произвести поиск по каталогу. В этом случае единственные пользователи, которые могут войти в домен (при недоступности глобального каталога) — члены группы **Администраторы домена**.

Поиск в глобальном каталоге очень эффективен. Каталог содержит информацию обо всех объектах во всех доменах в лесу. Это позволяет разрешать поисковые запросы в локальном домене, а не в домене другой части сети. Локальное разрешение запросов уменьшает сетевую нагрузку и в большинстве случаев гарантирует более быстрые ответы на поисковые запросы.

Совет

Если был замечен медленный вход в систему или увеличение времени отклика, можно настроить дополнительные глобальные каталоги. Но чем больше глобальных каталогов, тем больше нагрузка на сеть, поскольку больше данных будет реплицироваться по сети.

Кэширование состава универсальных групп

В крупной организации наличие глобальных каталогов в каждом офисе не очень практично. Отсутствие глобальных каталогов в каждом офисе представляет проблему лишь тогда, когда удаленный офис теряет связь с основным офисом или определенным филиалом, в кото-

ром находится глобальный каталог. Если это произойдет, то обычные пользователи не смогут войти в систему, вход будет разрешен только членам группы **Администраторы домена**. Это происходит потому, что по сети нужно отправить запросы входа в систему на сервер глобального каталога, и это невозможно без связи.

Проблему можно решить разными способами. Можно превратить один из контроллеров домена удаленного офиса в глобальный сервер каталога, выполнив процедуру, которая будет рассмотрена в *разд. "Настройка глобальных каталогов" главы 7*. Недостаток этого метода заключается в том, что на определенный сервер будет повышена нагрузка, и потребуются дополнительные ресурсы. Также придется более тщательно контролировать доступность глобального каталога.

Другой способ решения проблемы заключается в кэшировании состава универсальных групп. Любой контроллер домена может разрешить запросы входа в систему без обращения к глобальному каталогу. Это позволяет ускорить вход в систему и упрощает выключение сервера, поскольку ваш домен не полагается на единственный сервер или группу серверов для входа в систему. Также это решение уменьшает трафик репликации. Вместо периодической репликации всего глобального каталога по сети будет обновлен только состав универсальной группы в кэше. По умолчанию обновление происходит каждые 8 часов на каждом контроллере домена, что локально кэширует состав группы.

Кэширование членства в универсальной группе привязано к сайту. Помните, что сайт — это физическая структура каталога, состоящая из одной или более подсетей с определенным диапазоном IP-адресов и сетевой маской. Контроллеры домена под управлением Windows Server и глобальный каталог, с которым они связываются, должны находиться в одном и том же сайте. Если есть несколько сайтов, нужно настроить локальное кэширование в каждом сайте. Также пользователи сайта должны быть частью домена Windows, работающего в режиме Windows Server 2003 или выше. Чтобы узнать, как настроить кэширование, *см. разд. "Настройка кэширования членства в универсальных группах" главы 7*.

Репликация и Active Directory

Независимо от того, используется ли репликация FRS или DFS, в каталоге хранятся три типа информации: данные домена, данные схемы и конфигурационные данные.

Данные домена реплицируются на все контроллеры домена в пределах определенного домена. Данные схемы и конфигурационные данные реплицируются всем доменам и дереве доменов или лесу. Кроме того, в глобальные каталоги реплицируются все объекты в отдельном домене и подмножестве свойств объектов в лесу.

Это означает, что контроллеры доменов хранят и реплицируют следующее:

- информацию схемы для дерева домена или леса;
- конфигурационную информацию для всех доменов в дереве или лесу;
- все объекты каталога и свойства для соответствующих доменов.

Однако контроллеры домена, размещающие глобальный каталог, хранят и реплицируют информацию схемы для леса и конфигурационную информацию для всех доменов в лесу. Также они хранят и тиражируют (реплицируют) подмножество свойств для всех объектов каталога в лесу, который реплицируется только между серверами, содержащими глобальные каталоги и все объекты каталога и свойства для их домена:

- информацию схемы для леса;
- конфигурационную информацию для всех доменов в лесу;

- подмножество свойств между GC-узлами;
- все объекты каталога и свойства для их доменов.

Для получения лучшего понимания репликации рассмотрим следующий сценарий, в котором устанавливается новая сеть:

1. Начните с установки первого контроллера домена в домене А. Данный сервер является единственным контроллером домена, и он также является глобальным каталогом. Нет никакой репликации к другим контроллерам доменов в сети.
2. Установите второй контроллер домена в домене А. Поскольку у нас теперь есть два контроллера, начнется репликация. Чтобы убедиться, что данные реплицированы правильно, назначьте один контроллер домена мастером инфраструктуры, а другой пусть работает как глобальный каталог. Хозяин инфраструктуры наблюдает за обновлениями глобального каталога и запрашивает обновления у измененных объектов. Оба контроллера домена тиражируют данные схемы и данные конфигурации.
3. Установите третий контроллер домена в домене А. Этот сервер не является глобальным каталогом. Хозяин инфраструктуры наблюдает за обновлениями глобального каталога, запрашивает обновления у измененных объектов, а затем реплицирует эти изменения на третий контроллер домена. Три контроллера домена также реплицируют данные схемы и конфигурационные данные.
4. Установите новый домен, домен Б, и добавьте в него контроллеры домена. Глобальный каталог размещен в домене А, и домен Б начинает репликацию всех данных схемы и конфигурации, а также подмножества данных домена в каждом домене. Репликация внутри домена А продолжается, как было описано ранее. Начинается репликация данных внутри домена Б.

Active Directory и LDAP

LDAP (Lightweight Directory Access Protocol) — стандартный коммуникационный протокол для сетей TCP/IP. Протокол LDAP специально разработан для получения доступа к службам каталогов с наименьшими затратами ресурсов. Также LDAP определяет операции запроса и изменения информации каталога.

Клиенты Active Directory могут использовать LDAP для взаимодействия с компьютерами Active Directory независимо от того, вошли ли они в сеть или нет, или для поиска общих ресурсов. Также можно использовать LDAP для управления Active Directory.

LDAP — это открытый стандарт, который используют многие другие службы каталогов, что упрощает взаимодействие между каталогами и обеспечивает более четкий миграционный путь от других служб каталогов до Active Direcotry. Для улучшения функциональной совместимости также можно использовать интерфейс ADSI (Active Directory Service Interface). ADSI поддерживает стандартные интерфейсы программирования приложений (API) для LDAP, определенные в RFC 1823. ADSI может использоваться в паре с Windows Script Host для создания и управления объектов в Active Directory.

Роли FSMO

Роли хозяина операций выполняют задачи, решение которых способом мультимастера непрактично. Определено пять ролей операций и можно присвоить эти роли одному или нескольким контроллерам домена. Несмотря на то, что определенные роли могут быть при-

своены только один раз в лесу, некоторые другие роли должны быть определены один раз в каждом домене.

У каждого леса Active Directory должны быть следующие роли.

- **Владелец схемы** (Schema Master) — контролирует обновления и модификации схемы каталога. Для обновления схемы каталога нужно получить доступ к владельцу схемы. Чтобы определить, какой сервер является текущим владельцем схемы в домене, откройте окно командной строки и введите команду `dsquery server -hasfsmo schema`.
- **Владелец доменных имен** (Domain Naming Master) — контролирует добавление или удаление доменов в лесу. Для добавления или удаления доменов нужно получить доступ к владельцу доменных имен. Для определения, какой сервер является текущим хозяином доменных имен, откройте окно командной строки и введите команду `dsquery server -hasfsmo name`.

Эти роли должны быть уникальными в лесу. То есть можно назначить лишь одного владельца схемы и одного владельца доменных имен в лесу.

У каждого домена Active Directory должны быть следующие роли.

- **Владелец относительных идентификаторов** (Relative ID master) — распределяет относительные идентификаторы контроллерам домена. Независимо от того, создается ли объект пользователя, группы или компьютера, контроллеры домена присваивают этому объекту уникальный идентификатор безопасности. Идентификатор безопасности состоит из префикса идентификатора безопасности домена и уникального относительного идентификатора, назначенного владельцем относительных идентификаторов. Для определения, какой сервер является текущим владельцем относительных идентификаторов для домена, откройте окно командной строки и введите команду `dsquery server -hasfsmo rid`.
- **Эмулятор основного контроллера домена** (PDC emulator) — при использовании операции смешанного режима эмулятор PDC работает как Windows NT PDC. Его задача — аутентификация входов Windows NT, изменение паролей и репликация обновлений на BDC. Эмулятор PDC является сервером времени по умолчанию и как таковой осуществляет синхронизацию времени в домене. Чтобы определить, какой сервер является текущим эмулятором PDC, откройте окно командной строки и введите команду `dsquery server -hasfsmo pdc`.
- **Владелец инфраструктуры домена** (Infrastructure master) — обновляет ссылки объектов путем сравнения их данных каталога с глобальным каталогом. Если данные устарели, владелец инфраструктуры запрашивает обновленные данные из глобального каталога и затем реплицирует изменения на другие контроллеры домена. Чтобы определить, какой сервер является владельцем инфраструктуры, откройте окно командной строки и выполните команду `dsquery сервер -hasfsmo infr`.

Эти роли должны быть уникальными в пределах домена. Это означает, что в пределах домена можно назначить только одного владельца относительных идентификаторов, один PDC-эмулятор и одного владельца инфраструктуры.

Роли FSMO обычно назначаются автоматически, но при желании можно назначить их вручную. При установке новой сети для выполнения всех пяти FSMO-ролей назначается первый контроллер домена. Если позже будет создан дочерний домен или корневой домен в новом дереве, автоматически будет назначен первый контроллер домена нового домена для выполнения FSMO-ролей. В новом лесу контроллер домена назначается для выполнения всех FSMO-ролей. Если новый домен находится в том же лесу, назначаются следующие

роли: владелец относительных ID, PDC-эмулятор и владелец инфраструктуры. Роли хозяина схемы и хозяина доменных имен остаются в первом домене леса.

Когда в домене только один контроллер домена, то этот компьютер обрабатывает все FSMO-роли. Если вы работаете с единственным сайтом, назначение ролей FSMO по умолчанию является вполне приемлемым. Когда же добавите новые контроллеры домена и новые домены, возможно, понадобится распределить FSMO-роли на другие контроллеры домена.

Когда в домене есть два или больше контроллера, можно настроить два владельца операций. Здесь один контроллер домена можно сделать владельцем операций, а второй сервер сделать резервным. Резервный владелец операций будет использоваться, когда что-то случится с основным сервером. Убедитесь, что контроллеры домена — прямые партнеры по репликации и хорошо соединены.

Когда доменная структура вырастет, можно разделить роли между различными контроллерами домена. Это повысит скорость отклика владельцев операций. Обратите внимание на текущие обязанности контроллера домена, который планируется использовать.

Рекомендации

Две роли, которые не нужно разделять — это владелец схемы и владелец доменных имен. Всегда назначайте эти роли одному и тому же серверу. Для более эффективной работы нужно назначить роли владельца относительных ID и PDC-эмулятора также одному и тому же серверу. Но в случае необходимости можно разделить эти роли. Например, в большой сети, где пиковые нагрузки вызывают проблемы производительности, вы, возможно, захотите поместить роли хозяина RID и PDC-эмулятора на разные контроллеры доменов. Кроме того, обычно не нужно помещать роль владельца инфраструктуры на контроллер домена, на котором находится глобальный каталог. *См. разд. "Глобальные каталоги" ранее в этой главе*.

Корзина Active Directory

Когда ваш лес Active Directory работает в режиме Windows Server 2008 R2 или выше, можно использовать Корзину Active Directory (Active Directory Recycle Bin). Корзина Active Directory добавляет легкую в использовании функцию восстановления для объектов Active Directory. При включении этой функции все атрибуты удаленного объекта сохраняются, позволяя восстановить объект в том же состоянии, что и до удаления. Также можно восстановить объекты из Корзины без инициирования аутентичного восстановления (authoritative restore). Это существенно отличается от ранее доступного метода, который использовал авторитетное восстановление для восстановления удаленных объектов из контейнера Deleted Objects. Ранее, при удалении объекта большая часть нессылочных атрибутов очищалась, а все ссылочные атрибуты удалялись. В результате даже если получалось восстановить удаленный объект, то нельзя было восстановить его состояние.

Подготовка схемы для Корзины

Перед включением Корзины следует обновить схему Active Directory с необходимыми Корзине атрибутами. Для этого подготовьте лес и домен для режима Windows Server 2008 R2. После этого схема будет обновлена и каждый объект в лесу будет обновлен с атрибутами Корзины. Этот процесс необратим, как только он будет запущен.

После подготовки Active Directory необходимо обновить все контроллеры домена в вашем лесу до Windows Server 2008 R2 (или выше), а затем повысить режим домена и леса до

Windows Server 2008 R2 или выше. Дополнительно можно обновить схему Active Directory в вашем лесу и доменах для Windows Server 2012 для включения расширенной Корзины.

После всех этих операций можно включить Корзину и получить к ней доступ. Как только Корзина будет включена, ее нельзя будет отключить. Теперь при удалении объекта Active Directory он будет переведен в состояние *"логически удален"* и перемещен в контейнер **Deleted Objects** (рис. 6.7). Также изменится его имя. Удаленный объект остается в контейнере **Deleted Objects** определенный период времени, который по умолчанию равен 180 дней.

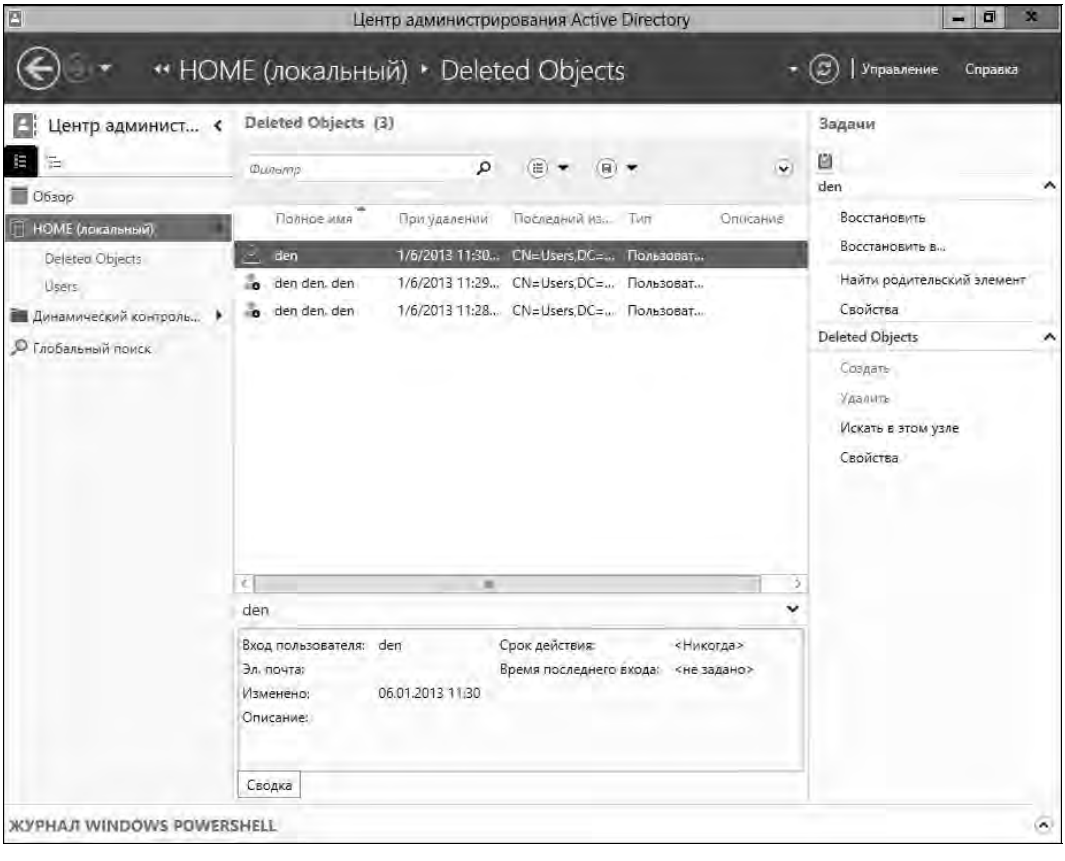


Рис. 6.7. Удаленные объекты остаются в контейнере **Deleted Objects** определенный период времени

Восстановление удаленных объектов

Если было принято решение не использовать Корзину, восстановить удаленные объекты из контейнера **Deleted Objects** можно все еще с использованием авторитетного восстановления и других методов, которые далее будут рассмотрены в этом разделе. Процедура осталась неизменной еще со времен предыдущих версий Windows Server[1]. Однако кое-что изменилось: теперь объекты восстанавливаются в их предыдущие состояния со всеми ссылоч-

[1] В дополнение к этой главе предлагаю ознакомиться с материалом по адресу: **http://www.exams.com.ua/articles/administration/windows/3011.htm**. — *Прим. пер.*

ными и нессылочными атрибутами. Для осуществления авторитетного восстановления контроллер домена должен быть переведен в режим восстановления (Directory Services Restore Mode, DSRM).

Вместо того чтобы использовать авторитетное восстановление и вывести контроллер домена из эксплуатации, можно восстановить удаленные объекты с помощью утилиты Ldp.exe или командлетов Active Directory для Windows PowerShell. Если схема Active Directory была обновлена в своем лесу и доменах до Windows Server 2012, можно также включить расширенную Корзину, позволяющую восстановить удаленные объекты с использованием Центра администрирования Active Directory.

Помните, что Active Directory блокирует доступ к объекту сразу же после удаления. Но после удаления и до блокирования проходит немного времени, в течение которого Active Directory обрабатывает ссылочную таблицу объекта для обслуживания ссылочной целостности значений ссылочных атрибутов. Затем Active Directory запрещает доступ к удаленному объекту.

Использование Ldp.exe для базового восстановления

Для просмотра контейнера **Deleted Objects** и восстановления удаленных объектов можно использовать утилиту Ldp.exe:

1. Введите команду `Ldp.exe` в поле поиска приложений и нажмите клавишу <Enter>.
2. В меню **Параметры** (Options) выберите команду **Элементы управления** (Controls). В одноименном окне из списка **Предопределенная загрузка** (Load Predefined) выберите вариант **Return Deleted Objects**, а затем нажмите кнопку **OK**.
3. В меню **Подключение** (Connection) выберите команду **Привязка** (Bind), привяжитесь к серверу, содержащему лес корневого домена. Выберите тип привязки и нажмите кнопку **OK**.
4. В меню **Вид** (View) выберите команду **Дерево** (Tree). В окне **Дерево** (Tree View) используйте список **Базовое расширяемое имя (DN)** (BaseDN) для выбора соответствующему лесу корневого домена, например, `DC=Cpandl,DC=Com`, а затем нажмите кнопку **OK**.
5. В консоли дерева дважды щелкните на контейнере `CN=Deleted Objects`.
6. Найдите нужный объект Active Directory, затем щелкните на нем правой кнопкой мыши и выберите команду **Изменить** (Modify).
7. В поле **Изменить запись Атрибут** (Edit Entry Attribute) введите `isDeleted`, в поле **Значения** (Values) ничего вводить не нужно.
8. В области **Операция** (Operation) выберите операцию **Удалить** (Delete), а затем нажмите кнопку **Ввод** (Enter).
9. Теперь в поле **Атрибут** (Edit Entry Attribute) введите `distinguishedName`. В поле **Значения** (Values) введите исходное имя этого объекта Active Directory.
10. В области **Операция** выберите операцию **Заменить** (Replace). Включите режим **Расширенный** (Extended) и нажмите кнопку **Ввод** (Enter), а затем — **Выполнить** (Run).

Использование Windows PowerShell для базового и расширенного восстановления

Командлеты Active Directory для Windows PowerShell позволяют восстановить удаленные объекты с использованием скриптов или путем ввода команд в приглашении PowerShell.

Команда Get-ADObject используется для получения объекта или объектов, которые нужно восстановить. Эти объекты следует передать командлету Restore-ADObject, который используется для восстановления выбранных объектов в базе данных каталога.

> ***Примечание***
>
> Модуль Active Directory не импортируется в Windows PowerShell по умолчанию. Импортировать этот модуль можно с помощью команды `import-module activedirectory`, введенной в приглашении PowerShell. Более подробная информация приведена в *разд. "Центр администрирования Active Directory и Windows PowerShell" главы 7*.

Чтобы использовать командлеты Active Directory для восстановления, нужно открыть приглашение PowerShell с правами администратора, для этого щелкните правой кнопкой мыши по записи Windows PowerShell и выберите команду **Запуск от имени администратора** (Run As Administrator). Базовый синтаксис восстановления объекта следующий:

```
Get-ADObject -Filter {ObjectId} -IncludeDeletedObjects | Restore-ADObject
```

Здесь `ObjectID` — значение фильтра, позволяющее идентифицировать восстанавливаемый объект. Например, можно восстановить удаленную учетную запись пользователя по отображаемому имени или имени учетной записи SAM, как показано в следующих примерах:

```
Get-ADObject -Filter {DisplayName -eq "Rich Tuppy"}
-IncludeDeletedObjects | Restore-ADObject


Get-ADObject -Filter {SamAccountName -eq "richt"}
-IncludeDeletedObjects | Restore-ADObject
```

Заметьте, что вложенные объекты должны быть восстановлены с наивысшего уровня удаленной иерархии в живой родительский контейнер. Например, если случайно удалили организационное подразделение и все его учетные записи, необходимо ее восстановить перед восстановлением связанных учетных записей.

Базовый синтаксис для восстановления объектов контейнера, таких как организационное подразделение, следующий:

```
Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=ContainerID)" -IncludeDeletedObjects |
Restore-ADObject
```

Здесь *`ContainerID`* — значение фильтра, идентифицирующее объект контейнера, который нужно восстановить. Например, можно восстановить организационное подразделение Corporate Services так:

```
Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=Corporate_Services)"
-IncludeDeletedObjects | Restore-ADObject
```

Если организационное подразделение содержит учетные записи и их также нужно восстановить, используйте ранее рассмотренную технику. Базовый синтаксис требует установки поисковой основы и ассоциирования учетных записей с их последним известным родителем, как показано здесь:

```
Get-ADObject -SearchBase "CN=Deleted Objects,ForestRootDN" -Filter {lastKnownParent
-eq "ContainerCN,ForestRootDN"} -IncludeDeletedObjects | Restore-ADObject
```

Здесь *`ForestRootDN`* — имя леса корневого домена, например, `DC=Cpandl,DC=Com`, а *`ContainerDN`* — это общее имя контейнера, например, `OU=Corporate_Services` или `CN=Users`.

Следующий пример восстанавливает все учетные записи, которые были удалены из организационного подразделения Corporate Services:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=Cpandl,DC=com" -Filter
{lastKnownParent -eq "OU=Corporate_Services,DC=Cpandl,DC=com"}
-IncludeDeletedObjects | Restore-ADObject
```

Использование расширенной Корзины для восстановления

Расширенная Корзина существенно упрощает восстановление удаленных объектов. Как только будет обновлена схема Active Directory в ваших лесах и доменах до Windows Server 2012, можно включить расширенную Корзину с помощью следующих действий:

1. В Центре администрирования Active Directory по умолчанию для администрирования открывается локальный домен. Если нужно работать с другим доменом, выберите команду меню **Управление | Добавление узлов перехода** (Manage | Add Navigation Nodes). В окне **Добавление узлов перехода** (Add Navigation Nodes) выберите домен и нажмите кнопку **OK**.
2. На левой панели выберите домен. На панели **Задачи** выберите задачу **Включить корзину** (Enable Recycle Bin) и нажмите кнопку **OK** в окне подтверждения.
3. Active Directory начнет реплицировать изменения всем контроллерам домена в лесу. Как только изменения будут реплицированы, расширенная Корзина станет доступной для использования. Если выбрать **Обновить** (Refresh) в Центре администрирования Active Directory, будет отображен контейнер **Deleted Object**, он используется для расширенной Корзины.

Помните, что действие расширенной Корзины распространяется на весь лес. При включении этой опции на одном из доменов леса Active Directory реплицирует изменения на все контроллеры домена всех доменов леса.

Расширенная Корзина позволяет восстанавливать объекты намного проще. В Центре администрирования Active Directory домены, использующие расширенную Корзину, обладают контейнером **Deleted Objects**. В этом контейнере находится список удаленных объектов. Как упомянуто ранее, удаленные объекты остаются в Корзине 180 дней (по умолчанию).

Для каждого удаленного объекта выводится его имя, дата удаления, последний известный родитель и тип. После выбора объекта можно использовать команды панели **Задачи** для работы с ним. Чтобы восстановить объект, выберите команду **Восстановить** (Restore). Она восстанавливает объект в исходный контейнер. Например, если объект удален из контейнера **Users**, он будет восстановлен в этот контейнер.

Команда **Восстановить в** (Restore To) восстанавливает объект в альтернативный контейнер в пределах исходного домена или в другой домен в пределах текущего леса. Укажите альтернативный контейнер в окне **Восстановить в** (Restore To). Например, если объект был удален из контейнера **Users** домена **tech.cpandl.com**, можно восстановить его в организационном подразделении Dev домена **eng.cpandl.com**.

ГЛАВА 7

Базовое администрирование Active Directory

Базовое администрирование Active Directory фокусируется на ключевых задачах доменных служб Active Directory: создание учетной записи компьютера или присоединение компьютера к домену. В этой главе будут рассмотрены средства, которые используются для управления Active Directory, а также методы для управления компьютерами, контроллерами доменов и организационными подразделениями.

Средства управления Active Directory

Администраторам доступно несколько наборов утилит, использующихся для управления Active Directory, в том числе графические утилиты администрирования, утилиты командной строки, утилиты поддержки и командлеты Microsoft Windows PowerShell.

Утилиты администрирования Active Directory

Утилиты администрирования Active Directory предоставляются в виде оснасток для консоли **Управление компьютером** (Microsoft Management Console, MMC). Для управления Active Directory используются следующие основные утилиты:

- **Центр администрирования Active Directory** (Active Directory Administrative Center) — для осуществления задач управления;
- **Active Directory — домены и доверие** (Active Directory Domains and Trusts) — для работы с доменами, деревьями доменов и лесами доменов;
- **Модель Active Directory для Windows PowerShell** (Active Directory Module for Windows PowerShell) — для управления Active Directory при работе с Windows PowerShell;
- **Active Directory — сайты и службы** (Active Directory Sites and Services) — для управления сайтами и подсетями;
- **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers) — для управления пользователями, группами, компьютерами и организационными подразделениями;
- **Управление групповой политики** (Group Policy Management) — для управления способом использования групповой политики в организации. Предоставляет доступ к RSoP для моделирования и журналирования.

Внимание!

Брандмауэр Windows может влиять на администрирование с помощью некоторых MMC-оснасток. Если брандмауэр Windows включен на удаленном компьютере и отображается сообщение об ошибке об отсутствии соответствующих прав, о том, что сетевой путь не найден или доступ запрещен, нужно настроить исключение на удаленном компьютере для TCP-порта 445. Для решения этой проблемы необходимо включить политику **Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования** (Windows Firewall: Allow Remote Administration Exception) в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена** (Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile). Либо в командной строке можно ввести команду `netsh firewall set portopening tcp 445 smb enable`. Подробно см. статью Microsoft Knowledge Base Article 840634 (**support.microsoft.com/default.aspx?scid=kb;en-us;840634**).

Запустить эти средства администрирования Active Directory можно из меню **Средства** (Tools) диспетчера серверов или добавить их в любую консоль MMC. Если используется другой компьютер с доступом в домен Windows Server, эти утилиты будут недоступны, пока не будут установлены. Для этого можно использовать мастер добавления ролей и компонентов (Add Roles And Features Wizard) (нужно добавить компонент **Средства удаленного администрирования сервера** (Remote Server Administration Tools for AD DS)).

Утилиты Active Directory для командной строки

Есть несколько утилит, позволяющих администрировать Active Directory из командной строки.

- **Adprep** — позволяет вручную подготовить лес или домен Windows для установки контроллеров домена Windows. Для подготовки леса или домена используйте команды `adprep /forestprep` и `adprep /domainprep` соответственно. Если планируется установка RODC, необходимо запустить команду `adprep /rodcprep` для леса.

  Практический совет

  Как было сказано в *главе 6*, диспетчер серверов для Windows Server 2012 автоматически подготавливает лес и домены. Однако необходимо использовать учетную запись с соответствующими правами. Чтобы выполнение команды было успешным для леса, нужно использовать учетную запись администратора, которая является членом группы **Администраторы предприятия** (Enterprise Admins), **Администраторы схемы** (Schema Admins) или **Администраторы домена в лесу корневого домена** (Domain Admins in the forest root domain). Чтобы выполнение команды было успешным для домена, необходимо использовать учетную запись из группы **Администраторы домена** (Domain Admins). Можно запустить утилиту Adprep на любом сервере под управлением 64-битной версии Windows Server 2008 или более поздней версии. Сервер нуждается в сетевом соединении с владельцем схемы для леса и владельцем инфраструктуры домена, в который нужно добавить контроллер домена. Если эти типы операций находятся на сервере Windows Server 2003, сервер, на котором выполняется утилита Adprep, должен быть присоединен к домену, и при этом невозможно использовать смарт-карты.

- **Dsadd** — добавляет компьютеры, контакты, группы, организационные подразделения и пользователей в Active Directory. Введите команду `dsadd` *`objectname`* `/?` в командной строке для получения справки об использовании той или иной команды, например, `dsadd computer /?`.
- **Dsget** — отображает свойства компьютеров, контактов, групп, организационных подразделений, пользователей, сайтов, подсетей и серверов, зарегистрированных в Active

Directory. Введите команду `dsget objectname /?` в командной строке для получения справки о команде, например, `dsget subnet /?`.

- **Dsmod** — модицифирует свойства компьютеров, контактов, групп, организационных подразделений, пользователей, сайтов, подсетей и серверов, зарегистрированных в Active Directory. Введите команду `dsmode objectname /?` в командной строке для получения справки о команде, например, `dsmode server /?`.
- **Dsmove** — перемещает один объект в новое расположение в пределах доменов или переименовывает объект без его перемещения. Введите команду `dsmove /?` в командной строке для получения справки об использовании этой команды.
- **Dsquery** — использует поисковый критерий для обнаружения компьютеров, контактов, групп, организационных подразделений, пользователей, сайтов, подсетей и серверов, зарегистрированных в Active Directory. Введите команду `dsquery /?` в командной строке для получения справки об использовании этой команды.
- **Dsrm** — удаляет объекты из Active Directory. Для получения справки введите команду `dsrm /?`.
- **Ntdsutil** — позволяет пользователю просматривать информацию о сайте, домене, сервере. Управляет ролями FSMO, осуществляет обслуживание базы данных Active Directory. Введите команду `ntdsutil /?` в командной строке для получения информации по использованию команды.

Программа Adprep находится на установочном носителе Windows Server 2012 в папке \support\adprep. Остальные утилиты станут доступны после установки компонента **Средства удаленного администрирования сервера** (Remote Server Management Tools for AD DS).

Утилиты поддержки Active Directory

С компонентом **Средства удаленного администрирования сервера** устанавливается множество утилит поддержки Active Directory. В табл. 7.1 представлен список наиболее полезных утилит поддержки для настройки, управления и решения проблем Active Directory.

Таблица 7.1. *Обзор утилит поддержки Active Directory*

Утилита поддержки	Имя исполнимого файла	Описание
Редактирование ADSI (ADSI Edit)	Adsiedit.msc	Открывает и редактирует Active Directory Services Interface для контейнеров домена, схемы и конфигурации
Active Directory Administration Tool	Ldp.exe	Осуществляет операции LDAP на Active Directory
Утилита отображения разрешений (список ACL) объекта доменных служб AD DS (Directory Services Access Control Lists Utility)	Dsacls.exe	Управляет списками контроля доступом (ACL) для объектов в Active Directory
Управление пространствами имен, серверами и клиентами DFS (Distributed File System Utility)	Dfsutil.exe	Управляет распределенной файловой системой (DFS) и отображает информацию DFS

Таблица 7.1 *(окончание)*

Утилита поддержки	Имя исполнимого файла	Описание
DNS Server Troubleshooting Tool	Dnscmd.exe	Управляет свойствами DNS-серверов, зонами и записями ресурсов
Replication Diagnostics Tool	Repadmin.exe	Управляет и контролирует репликацию с использованием командной строки
Windows Domain Manager	Netdom	Позволяет управлять доменами и доверительными отношениями из командной строки

Использование оснастки *Active Directory — пользователи и компьютеры*

Active Directory — пользователи и компьютеры (Active Directory Users And Computers) — это одна из основных утилит администратора, которая используется для управления Active Directory. С ее помощью можно управлять всеми задачами, связанными с пользователем, группой и компьютером, а также организационными утилитами.

Запустить утилиту **Active Directory — пользователи и компьютеры** можно из меню **Средства** (Tools) диспетчера сервера (командой **Пользователи и компьютеры Active Directory**). Также можно добавить оснастку **Active Directory — пользователи и компьютеры** в любую обновляемую консоль. По умолчанию оснастка **Active Directory — пользователи и компьютеры** работает с доменом, к которому в данный момент подключен администратор. Администратор может получить доступ к объектам компьютера и пользователя в этом домене с помощью дерева консоли (рис. 7.1). Если невозможно найти контроллер домена или если нужный домен не отображается, необходимо подключиться к контроллеру домена в текущем домене или в другом домене. Другая высокоуровневая задача, которую можно выполнить с помощью этой утилиты, — это просмотр расширенных опций или поиск объектов.

В оснастке **Active Directory — пользователи и компьютеры** отображается стандартный набор папок:

- **Builtin** — список встроенных пользователей и групп;
- **Computers** — контейнер по умолчанию для учетных записей компьютера;
- **Domain Controllers** — контейнер по умолчанию для контроллеров домена;
- **ForeignSecurityPrincipals** — содержит информацию по объектам из доверенного внешнего домена. Обычно эти объекты создаются, когда объекты из внешнего домена добавлены в группу текущего домена;
- **Managed Service Accounts** — контейнер по умолчанию для управляемых учетных записей служб;
- **Microsoft Exchange Security Groups** — контейнер по умолчанию для групп, используемых Microsoft Exchange Server. Эта папка доступна, только если в вашем окружении запущен Exchange Server;

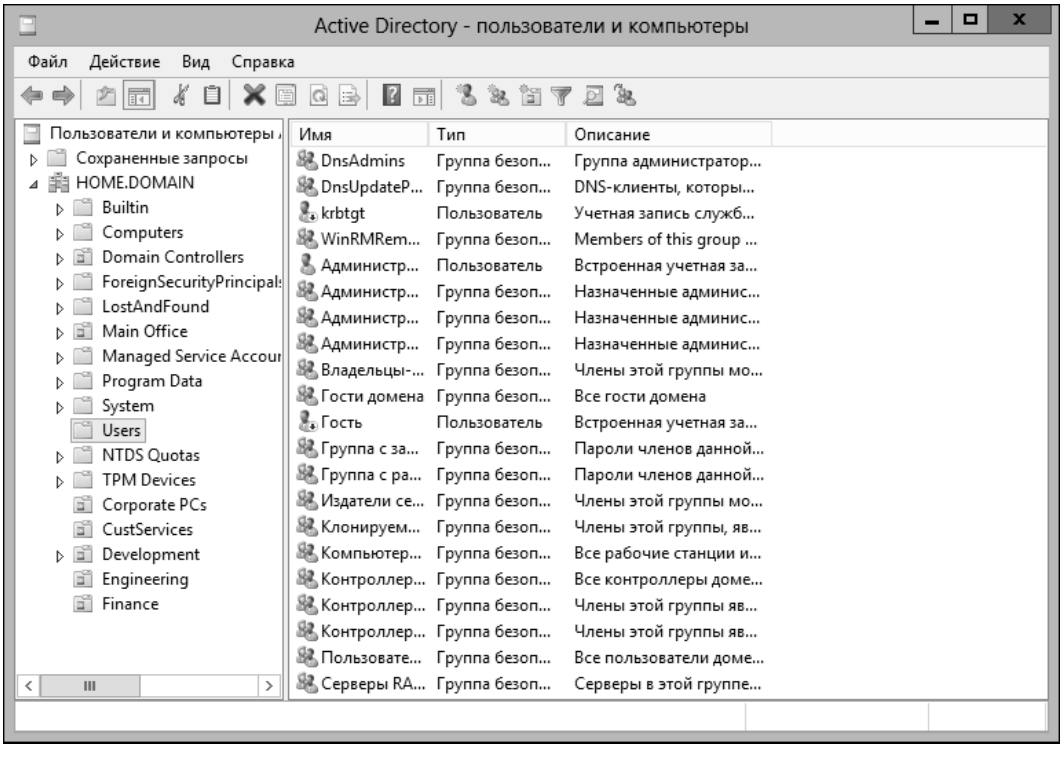


Рис. 7.1. При работе с оснасткой **Active Directory — пользователи и компьютеры** можно получить доступ к объектам компьютера и пользователей с помощью дерева консоли

- **Сохраненные запросы** — содержит сохраненные поисковые критерии, так чтобы можно было быстро осуществить ранее произведенные запросы по Active Directory;
- **Users** — контейнер по умолчанию для пользователей.

Оснастка **Active Directory — пользователи и компьютеры** обладает расширенными параметрами, которые по умолчанию не отображаются. Для получения доступа к этим опциям в меню **Вид** (View) выберите команду **Дополнительные компоненты** (Advanced Features). После этого будут доступны следующие дополнительные папки:

- **LostAndFound** — содержит объекты, которые потеряли родителя. Такие объекты можно удалить или восстановить;
- **NTDS Quotas** — содержит данные квотирования службы каталога;
- **Program Data** — содержит сохраненные в Active Directory данные для приложений Microsoft;
- **System** — содержит встроенные системные параметры;
- **TPM Devices** — выводит устройства с сохраненной в Active Directory информацией владельца TPM (Trusted Platform Module).

При желании можно добавить папки для организационных подразделений. На рис. 7.1 администратором созданы организационные подразделения Corporate PCs, CustServices, Development, Engineering и Finance.

По умолчанию оснастка подсоединяется к локальному домену и к первому контроллеру домена, который ответит на запрос. Можно работать с любым доменом леса, при условии, что есть соответствующие права доступа. Для смены домена выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой мыши на элементе **Пользователи и компьютеры Active Directory** (Active Directory Users And Computers) и выберите команду **Сменить домен** (Change Domain).
2. В окне **Смена домена** (Change Domain) будет отображено имя текущего домена. Введите новое имя домена или нажмите кнопку **Обзор**, выберите домен в окне **Обзор доменов** (Browse For Domain) и затем нажмите кнопку **OK**.
3. Если всегда нужно использовать этот домен при работе с **Active Directory — пользователи и компьютеры**, выберите опцию **Сохранить этот параметр домена для этой консоли** (Save This Domain Setting For The Current Console) и нажмите кнопку **OK**. В противном случае просто нажмите кнопку **OK**.

Если оснастка **Active Directory — пользователи и компьютеры** не отображает доступные объекты, значит, она не подключена к домену или нельзя найти контроллер домена. Необходимо подключиться к контроллеру домена для получения доступа к объектам пользователя, группы и компьютера. Для подключения к контроллеру домена выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой мыши на элементе **Пользователи и компьютеры Active** и выберите команду **Сменить контроллер домена** (Change Domain Controller). В окне **Смена сервера каталогов** (Change Directory Server) будет показано название текущего домена и контроллера домена.
2. Список **Заменить на** (Change To) содержит перечень доступных контроллеров домена в текущем домене. По умолчанию выбрано значение **Любой доступный для записи контроллер домена** (Any Writable Domain Controller). Если выбрать эту опцию, будет установлено подключение к контроллеру домена, который первым ответит на запрос. В противном случае укажите определенный контроллер домена, к которому нужно подключиться.
3. Если всегда нужно использовать этот контроллер домена при работе с **Active Directory — пользователи и компьютеры**, установите флажок **Сохранить настройку текущей консоли** (Save This Setting For The Current Console), а затем нажмите кнопку **OK**. В противном случае просто нажмите кнопку **OK**.

> ***Примечание***
>
> Окно **Смена сервера каталогов** также показывает сайт, с которым связан контроллер домена, тип контроллера домена, версию и состояние. Если тип контроллера домена — GC, то это глобальный каталог.

Можно подключиться к определенному контроллеру домена для решения проблем. Например, если подозреваете, что репликация не работает как нужно, необходимо проверить объекты на определенном контроллере домена. После подключения сможете найти несоответствия в недавно обновленных объектах.

В оснастке **Active Directory — пользователи и компьютеры** есть встроенная функция поиска, которую можно использовать для нахождения учетных записей, совместно используемых ресурсов и других объектов каталога. Можно легко произвести поиск по текущему домену, определенному домену или всему каталогу.

Рассмотрим, как произвести поиск по объектам каталога:

1. В дереве консоли щелкните правой кнопкой мыши по текущему домену или другому контейнеру, в котором нужно произвести поиск, а затем выберите команду **Найти** (Find). Будет открыто окно **Поиск** (Find), подобное изображенному на рис. 7.2.
2. В списке **Найти** (Find) выберите то, что нужно найти:
   - **Пользов., контакты и группы** (Users, Contacts, And Groups) — поиск учетных записей пользователей и групп, а также контактов, сохраненный в каталоге;
   - **Компьютеры** (Computers) — поиск учетных записей компьютеров по типу, имени и владельцу;
   - **Принтеры** (Printers) — поиск принтеров по имени, модели и функциям;
   - **Общие папки** (Shared Folders) — поиск общих папок по имени или ключевым словам;
   - **Организационные подразделения** (Organizational Units) — поиск организационных подразделений по имени;
   - **Пользовательский поиск** (Custom Search) — расширенный поиск или LDAP-запрос;
   - **Общие запросы** (Common Queries) — быстрый поиск по именам учетных записей, описаниям учетных записей, отключенным учетным записям, паролям и дням с момента последнего входа в систему.

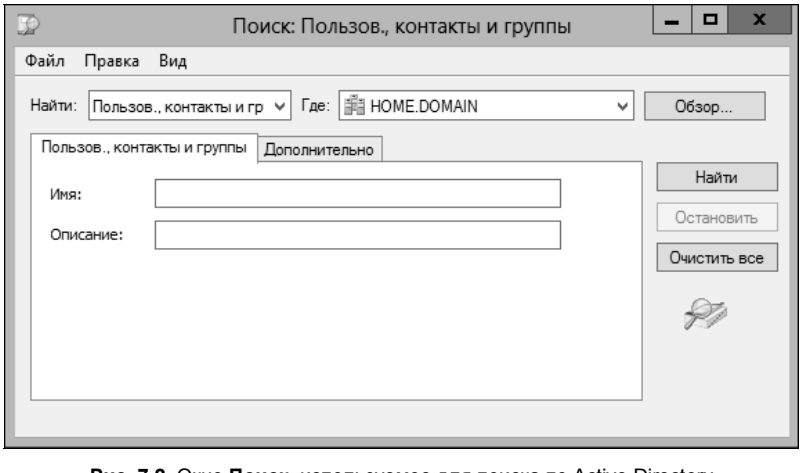


Рис. 7.2. Окно **Поиск**, используемое для поиска по Active Directory

3. Раскрывающийся список **Где** (In) позволяет выбрать расположение поиска. Если выбрать контейнер, например **Компьютеры**, именно он и будет выбран по умолчанию. Для поиска по остальным объектам каталога выберите вариант **В Active Directory** (Entire Directory).
4. Введите параметры поиска, а затем нажмите кнопку **Найти** (Find). В результатах поиска будут отображены любые совпадения (рис. 7.3). Дважды щелкните на объекте, чтобы просмотреть или изменить его свойства. Щелкните правой кнопкой мыши по объекту, чтобы открыть меню, содержащее команды управления объектом.

Примечание

Тип поиска определяет, какие текстовые поля и вкладки будут доступны в окне **Поиск**. В большинстве случаев нужно найти просто имя объекта, которое вводится в поле **Имя** (Name), но также доступны и другие параметры поиска. Например, для принтеров можно найти цветные принтеры, также можно найти принтеры, поддерживающие двустороннюю печать, и т. д.

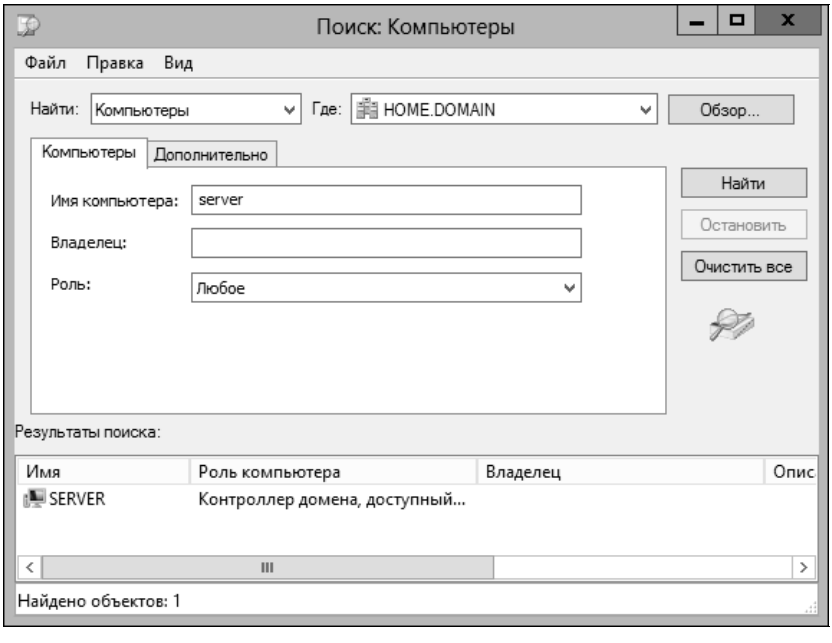


Рис. 7.3. Результаты поиска

Центр администрирования Active Directory и Windows PowerShell

Центр администрирования Active Directory (Active Directory Administrative Center) предоставляет ориентированный на задачу интерфейс для управления Active Directory (рис. 7.4). Для запуска этой утилиты выберите соответствующую команду из меню **Средства** диспетчера серверов. Эту утилиту можно использовать для выполнения множества задач, в том числе:

- подключения к одному или нескольким доменам;
- создания и управления учетными записями пользователей, групп и организационными подразделениями;
- создания и управления объектов параметров паролей;
- повышения режима работы леса и домена;
- восстановления удаленных объектов из Корзины Active Directory.

Утилита Центр администрирования Active Directory по умолчанию устанавливается в Windows Server 2012, а на клиентских компьютерах эта программа доступна после установки компонента **Средства удаленного администрирования сервера** (Remote Server

Administration Tools, RSAT). Эта утилита использует Windows PowerShell для осуществления административных задач и основана на Microsoft .NET Framework. Оба этих компонента должны быть установлены и правильно настроены, иначе нельзя будет использовать Центр администрирования Active Directory.

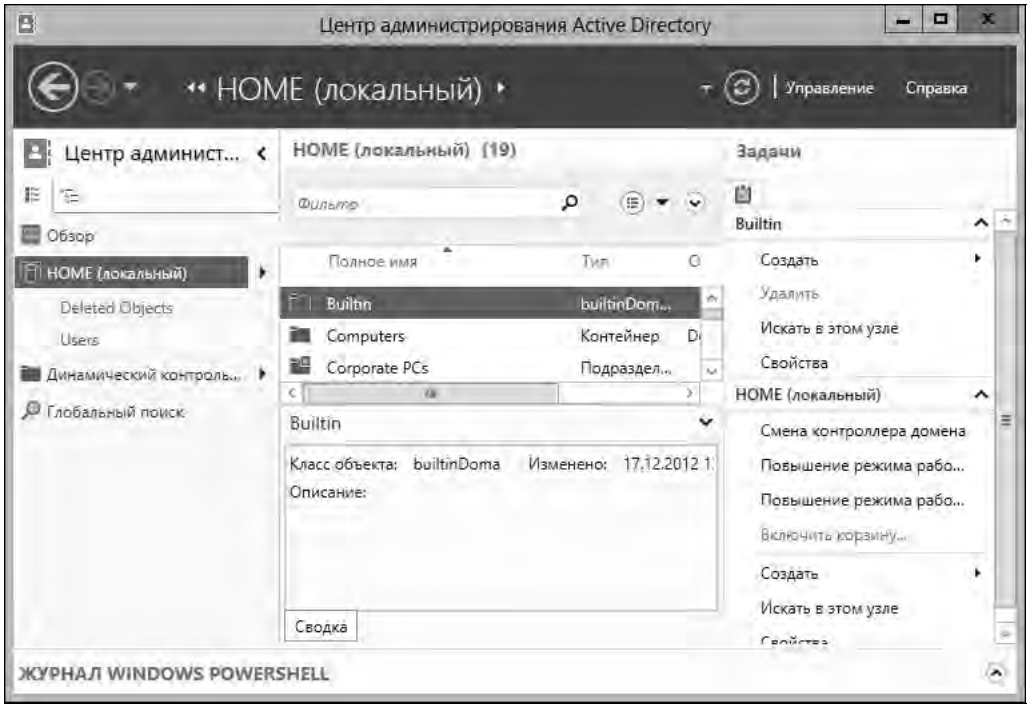


Рис. 7.4. Ориентированный на задачу интерфейс управления Active Directory

В Центре администрирования Active Directory по умолчанию для администрирования открыт локальный домен. Если нужно работать с другим доменом, в меню **Управление** (Manage) выберите команду **Добавить узлы перехода** (Add Navigation Nodes). В окне **Добавление узлов перехода** (Add Navigation Nodes) выберите домен, с которым нужно работать, и нажмите кнопку **OK**. После этого выберите домен, щелкнув по нему на левой панели.

По умолчанию утилита подключается к первому контроллеру домена, ответившему на запрос. Для решения проблем с репликацией необходимо подключиться к определенному контроллеру домена. После этого можно исследовать объекты контроллера и найти несоответствия в недавно обновленных объектах. Чтобы соединиться с определенным контроллером домена, щелкните правой кнопкой мыши по имени домена на панели слева и выберите команду **Смена контроллера домена** (Change Domain Controller).

В окне **Смена контроллера домена** (Change Domain Controller) будет отображено название текущего домена и контроллера домена (рис. 7.5). Выберите контроллер домена, который нужно использовать, и нажмите кнопку **Изменить** (Change).

Подобно утилите **Active Directory — пользователи и компьютеры**, Центр администрирования Active Directory имеет встроенные функции, которые можно использовать для поиска объектов каталога. Основной поисковый фильтр, находящийся на левой панели, можно использовать для выбора контейнера каталога.

Поисковый фильтр поможет быстро найти объекты уровня контейнера в пределах домена или дочернего организационного подразделения внутри выбранного организационного подразделения. После выбора узла домена на панели слева можно использовать фильтр, чтобы быстро найти организационное подразделение высокого уровня или встроенные контейнеры, которые начинаются с введенных в фильтр букв. Например, можно выбрать узел домена на панели слева, а в поле **Фильтр** (Filter) ввести `sa`, чтобы найти все высокоуровневые организационные подразделения, название которых начинается с букв "sa", например Sales. Поиск не включает дочерние организационные подразделения или подконтейнеры, результаты поиска не будут содержать организационные подразделения SalesVT или SalesCA, поскольку они являются дочерними организационными подразделениями для Sales.

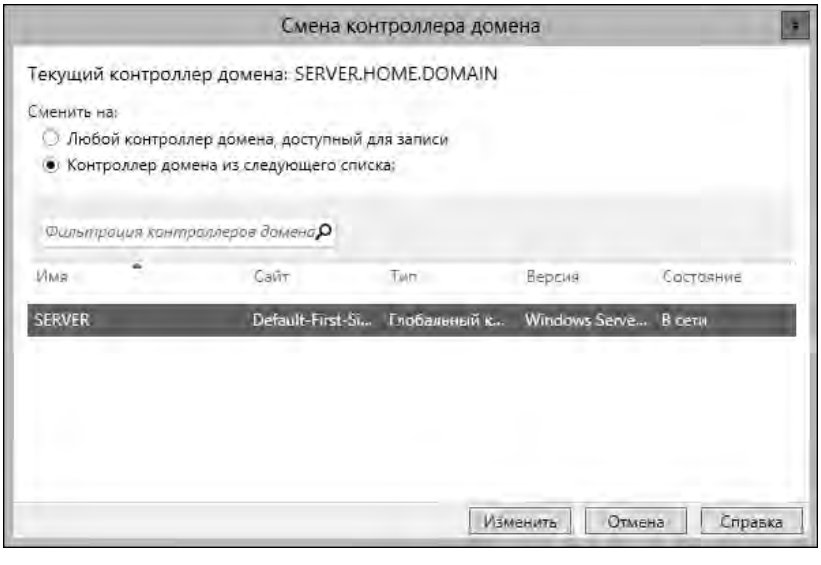


Рис. 7.5. Изменение контроллера домена

После выбора определенного контейнера можно произвести поиск по этому контейнеру, используя технику фильтров. Если выбрать узел **Глобальный поиск** (Global Catalog Search), можно будет найти имена всех объектов уровня контейнера, например, пользователей, группы, компьютеры и т. д. в выбранном в данный момент узле контейнера.

При глобальном поиске можно изменить связанный узел контейнера, щелкнув правой кнопкой мыши на списке **Область** (Scope) и выбрав узел, который будет использоваться. Выберите опцию **Поиск в глобальном каталоге** (Global Catalog Search) для поиска нестандартных объектов вроде схем атрибутов, схем классов и т. д.

Практический совет

Фильтр основан на начальных символах любой части имени объекта. Для групп это означает имя группы и имя учетной записи группы SAM (Security Accounts Manager). Для пользователей это означает имя, фамилию, полное имя, универсальный принципал (UPN), имя учетной записи группы SAM.

Дополнительно Центр администрирования Active Directory использует веб-сервисы, предоставляемые веб-службами Active Directory (Active Directory Web Services, ADWS). По крайней мере, веб-службы должны быть установлены хотя бы на одном контроллере в каж-

дом домене. По умолчанию соединения делаются через TCP-порт 9389, поэтому должны быть настроены исключения для этого порта.

Также можно работать с Active Directory, используя модуль Active Directory для Windows PowerShell. Модуль автоматически импортируется при выборе соответствующей команды из меню **Средства** диспетчера серверов. В противном случае модуль по умолчанию не будет добавлен в Windows PowerShell, и нужно его импортировать перед началом работы с командлетами Active Directory.

Для импортирования модуля Active Directory в командной строке Windows PowerShell введите команду `Import-Module ActiveDirectory`. Как только модуль будет импортирован, его можно использовать в текущей запущенной инстанции Windows PowerShell. При следующем запуске Windows PowerShell необходимо импортировать этот модуль снова, если нужно использовать его функции. Альтернативно можно выбрать команду **Модуль Active Directory для Windows PowerShell** (Active Directory Module For Windows PowerShell) в меню **Средства** диспетчера серверов для импорта модуля при запуске Windows PowerShell.

В командной строке Windows PowerShell можно вывести список доступных командлетов с помощью команды `get-command`. Используйте команду Get-Help для получения подробной информации об использовании командлетов. Если ввести команду `get-help *-*`, будет отображен список всех командлетов, в том числе описание каждого командлета. Для получения справки по определенному командлету введите команду `get-help` *`имя_командлета`*. Доступно несколько десятков командлетов Active Directory, их список можно получить с помощью команды `get-help *-ad*` в командной строке Windows PowerShell.

> ***Примечание***
>
> В Windows Server 2012 модуль ActiveDirectory для Windows PowerShell устанавливается по умолчанию, на клиентских компьютерах он станет доступным после установки средств удаленного администрирования сервера (RSAT). Windows PowerShell основывается на .NET Framework и Windows RemoteManagement (WinRM) для осуществления административных задач.

Управление учетными записями компьютера

Учетные записи компьютеров хранятся в Active Directory в виде объектов. Учетные записи используются для контроля доступа к сети и ее ресурсам. Администратор может добавить учетные записи компьютера в стандартные контейнеры, отображенные в оснастке **Active Directory — пользователи и компьютеры**. Лучше всего использовать папки **Computers**, **Domain Controllers**, а также любые созданные организационные подразделения.

Создание учетных записей компьютера на рабочей станции или сервере

Самый простой способ создать учетную запись компьютера — это войти в систему компьютера, который нужно настроить, а затем присоединиться к домену, как будет описано далее в этой главе. После этого необходимая учетная запись компьютера будет автоматически создана и помещена в папку **Computers** или в **Domain Controllers** (в случае необходимости). Также можно создать учетную запись компьютера с помощью оснастки **Active Directory — пользователи и компьютеры** или Центра администрирования Active Directory перед установкой компьютера.

Создание учетной записи компьютера в Центре администрирования Active Directory

Используя Центр администрирования Active Directory, можно создать стандартную учетную запись компьютера, добавить учетную запись в виде члена определенной группы и установить свойства менеджера компьютера. Чтобы сделать это, выполните следующие действия:

1. В Центре администрирования Active Directory щелкните правой кнопкой мыши на контейнере, в который нужно поместить учетную запись компьютера, далее выберите команду **Создать | Компьютер** (New | Computer). Это откроет окно **Создать Компьютер** (Create Computer), показанное на рис. 7.6.

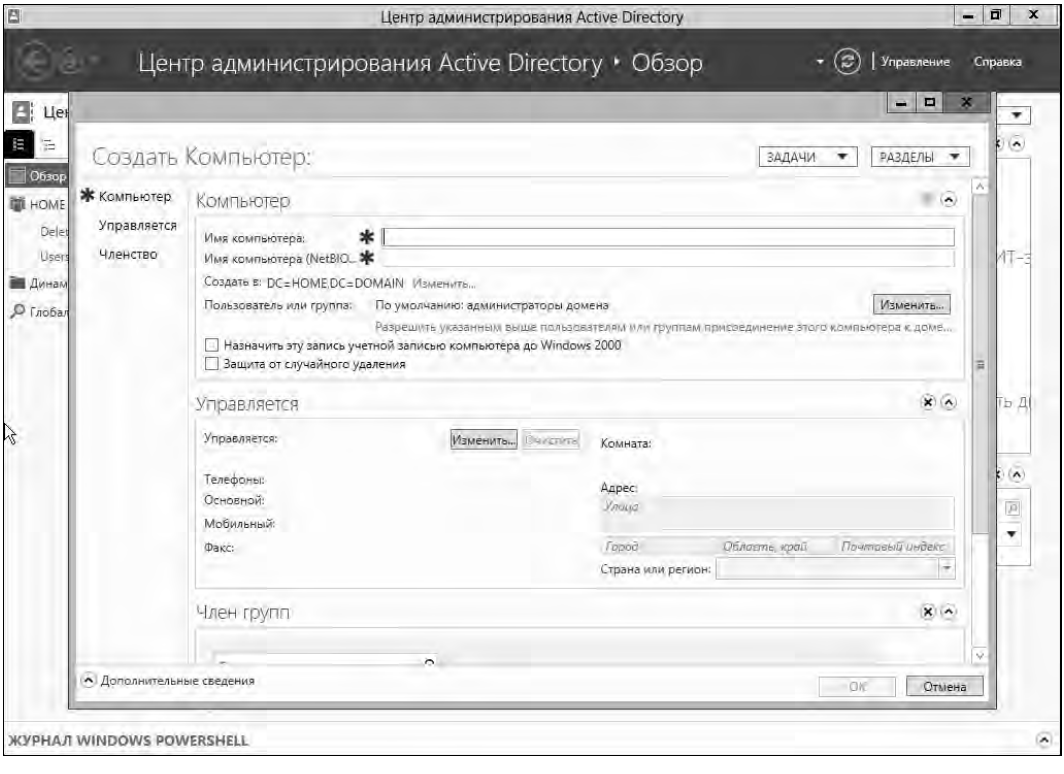


Рис. 7.6. Создание нового компьютера и установка его свойств

2. Введите имя компьютера.
3. По умолчанию только члены группы **Администраторы домена** могут присоединить этот компьютер к домену. Чтобы разрешить другому пользователю или группе присоединять компьютер к домену, нажмите кнопку **Изменить** (Change) и выберите учетную запись пользователя или группы в окне **Выбор: "Пользователь" или "Группа"** (Select User Or Group).

> ***Примечание***
>
> Можно выбрать любого существующего пользователя или группу. Это позволит делегировать полномочия, чтобы подсоединить эту учетную запись компьютера к домену.

4. Если эта учетная запись будет использоваться с приложениями, разработанными для старых операционных систем, установите флажок **Назначить эту запись учетной записью компьютера до Windows 2000** (Assign This Computer Account As A Pre-Windows 2000 Computer).
5. Дополнительно можно отметить флажок **Защита от случайного удаления** (Protect From Accidental Deletion), чтобы пометить эту учетную запись как защищенную в Active Directory. Защищенные учетные записи могут быть удалены, только если сбросить флаг защиты перед удалением учетной записи.
6. Назначить принципал безопасности в качестве менеджера компьютера можно, нажав кнопку **Изменить** (Edit) в области **Управляется** (Managed By), затем нужно выбрать пользователя или группу в окне **Выбор: "Пользователь" или "Группа"**. Кого назначить менеджером компьютера, зависит от корпоративной политики, это может быть основной пользователь компьютера, директор филиала в определенном офисе или специалист из группы поддержки.
7. Учетная запись будет автоматически добавлена в соответствующую группу компьютера по умолчанию. Обычно это группа **Domain Computers**. Но можно добавить компьютер в другую группу, нажав кнопку **Добавить** (Add) в области **Член групп** (Member Of). Затем появится окно **Выбор: "Группы"** (Member Of), чтобы определить группы, к которым должна принадлежать учетная запись компьютера.
8. Нажмите кнопку **OK** для создания учетной записи компьютера.

Создание учетной записи компьютера с помощью оснастки *Active Directory — пользователи и компьютеры*

Можно создать два типа учетных записей компьютера: стандартную учетную запись компьютера и управляемую учетную запись компьютера. Управляемые учетные записи компьютера доступны после установки в домене службы развертывания Windows (Windows Deployment Services, WDS).

Используя оснастку **Active Directory — пользователи и компьютеры**, можно создать стандартную учетную запись так:

1. В дереве консоли **Active Directory — пользователи и компьютеры** щелкните правой кнопкой мыши по контейнеру, в который нужно поместить учетную запись компьютера, затем выберите команду меню **Создать | Компьютер**. Будет отображено окно **Новый объект — Компьютер** (New Object — Computer Wizard), изображенное на рис. 7.7.
2. Введите имя компьютера.
3. По умолчанию только члены группы **Администраторы домена** могут присоединить этот компьютер к домену. Чтобы разрешить другому пользователю или группе присоединять компьютер к домену, нажмите кнопку **Изменить**, а затем выберите учетную запись пользователя или группы в окне **Выбор: "Пользователь" или "Группа"**.

   Примечание

   Можно выбрать любую существующую учетную запись пользователя или группы, чтобы делегировать полномочия и подсоединить эту учетную запись компьютера к домену.

4. Если эта учетная запись будет использоваться со старыми операционными системами, отметьте флажок **Назначить учетной записи статус пред-Windows 2000 компьютера** (Assign This Computer Account As A Pre-Windows 2000 Computer).

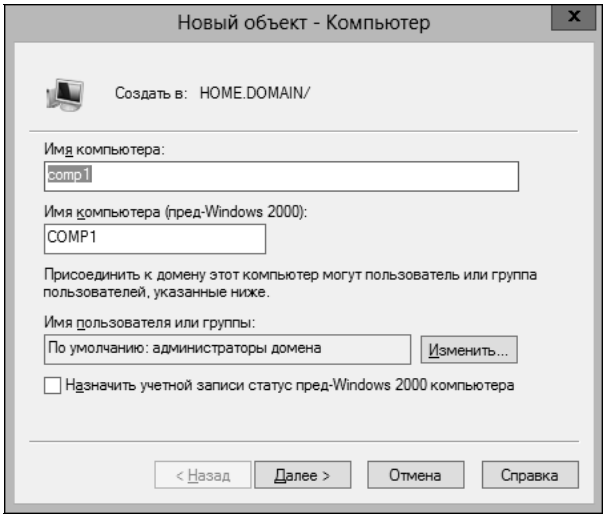


Рис. 7.7. Создайте новую учетную запись компьютера в окне **Новый объект — Компьютер**

5. Если службы развертывания Windows не установлены, нажмите кнопку **OK**, чтобы создать учетную запись компьютера. В противном случае нажмите кнопку **Далее** дважды, а затем — кнопку **Готово**.

При работе со службами развертывания Windows управляемые учетные записи компьютера используются для предварительной подготовки учетных записей компьютера для автоматической установки компьютера. Используя оснастку **Active Directory — пользователи и компьютеры**, можно создать управляемые учетные записи компьютера:

1. Повторите шаги 1—4 предыдущей процедуры. Нажмите кнопку **Далее** для отображения страницы **Управляемый** (Managed).
2. Выберите параметр **Это управляемый компьютер** (This Is A Managed Computer), а затем введите глобальный уникальный идентификатор компьютера/универсальный уникальный идентификатор (GUID/UUID). Нажмите кнопку **Далее**.
3. На следующей странице (**Хост-сервер** (Host Server)) будет возможность определить, какой хост-сервер использовать или разрешить любому доступному хост-серверу участвовать в удаленной установке. Для выбора хост-сервера установите переключатель **Следующий сервер удаленной установки** (The Following Remote Installation Server) и нажмите кнопку **Найти** (Find). В окне **Поиск** (Find) нажмите кнопку **Найти** (Find Now) для отображения списка всех серверов удаленной установки в организации. Выберите хост-сервер, который нужно использовать, а затем нажмите кнопку **OK**, чтобы закрыть окно поиска.
4. Нажмите кнопку **Далее**, а затем — кнопку **Готово**.

Практический совет

Можно найти GUID/UUID в BIOS или на корпусе компьютера. Если Windows PowerShell установлен, для получения GUID/UUID используется WMI-класс Win32_ComputerSystemProduct. Следующий пример возвращает UUID[1] компьютера:

```
get-wmiobject -class win32_computersystemproduct | fl uuid
```

[1] Приведенная команда возвращает идентификатор в виде xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. В окне **Хост-сервер** нужно ввести идентификатор без дефисов. — *Прим. пер.*

Следующий пример возвращает UUID удаленного компьютера:

```
get-wmiobject -class win32_computersystemproduct -computername engpc24 |
format-list pscomputername, uuid
```

После создания стандартной или управляемой учетной записи в оснастке **Active Directory — пользователи и компьютеры** нужно пометить учетную запись как защищенную. Защищенные учетные записи не могут быть удалены до тех пор, пока предварительно не будет сброшен флаг защиты.

Для защиты учетной записи компьютера выполните следующие действия:

1. Убедитесь, что в меню **Вид** (View) оснастки **Active Directory — пользователи и компьютеры** включен режим **Дополнительные компоненты** (Advanced Features).
2. Дважды щелкните на учетной записи компьютера, чтобы открыть окно **Свойства**.
3. На вкладке **Объект** (Object) установите флажок **Защитить объект от случайного удаления** (Protect Object From Accidental Deletion), а затем нажмите кнопку **OK**.

Просмотр и редактирование свойств учетной записи компьютера

Используя оснастку **Active Directory — пользователи и компьютеры** или Центр администрирования Active Directory, можно просматривать и редактировать учетные записи компьютера:

1. В дереве консоли разверните узел домена.
2. Выберите контейнер или организационное подразделение, где находится учетная запись компьютера.
3. Дважды щелкните на учетной записи, чтобы открыть окно **Свойства**, позволяющее просматривать и редактировать параметры учетной записи.

В оснастке **Active Directory — пользователи и компьютеры** дополнительные вкладки и параметры станут доступны, только если выбрана опция **Дополнительные компоненты** (Advanced Features) в меню **Вид** (View). В Центре администрирования Active Directory большинство опций доступно на вкладках панели **Расширения** (Extensions).

Удаление, отключение и включение учетных записей компьютера

Если учетная запись компьютера больше не нужна, ее можно удалить из Active Directory. Вместо удаления можно временно отключить учетную запись и включить ее позже, когда она снова понадобится.

Чтобы удалить, отключить или снова включить учетную запись компьютера, выполните следующие действия:

1. Запустите оснастку **Active Directory — пользователи и компьютеры** или Центр администрирования Active Directory. В дереве консоли выберите контейнер, в котором размещена учетная запись компьютера.
2. Щелкните правой кнопкой мыши по учетной записи компьютера и затем выберите одну из следующих команд:
   - **Удалить** (Delete) — удаление учетной записи. Нажмите кнопку **Да** (Yes) для подтверждения удаления;

- **Отключить** (Disable Account) — временное отключение учетной записи. Затем нажмите кнопку **Да** для подтверждения действия. Красный кружочек с крестиком внутри свидетельствует о том, что учетная запись отключена;
- **Включить** (Enable Account) — включает учетную запись, после чего ее можно снова использовать.

Если учетная запись защищена, нужно сбросить флаг защиты перед ее удалением. Дважды щелкните на учетной записи компьютера для отображения окна **Свойства**, затем выключите параметр **Защитить объект от случайного удаления** и нажмите кнопку **OK**. При использовании оснастки **Active Directory — пользователи и компьютеры** этот параметр находится на вкладке **Объект** окна **Свойства**. При использовании Центра администрирования Active Directory этот параметр находится на панели **Компьютер** (Computer).

> ***Совет***
>
> Если учетная запись на данный момент используется, ее нельзя отключить. Сначала нужно завершить работу компьютера (к которому относится учетная запись) или отключить сессию компьютера в папке **Сессия** (Sessions) утилиты **Управление компьютером** (Computer Management).

Сброс заблокированных учетных записей

Учетные записи компьютера имеют пароли, точно так же как и учетные записи пользователей. В отличие от учетных записей пользователей, пароли учетных записей компьютера управляются и обслуживаются автоматически. Для этого автоматического управления в домене хранится пароль учетной записи компьютера, который меняется каждые 30 дней (по умолчанию), а также пароль безопасного канала для установки безопасной связи с контроллерами домена. Пароль безопасного канала также обновляется каждые 30 дней. Оба пароля должны синхронизироваться. Если эти пароли не будут синхронизированы, то компьютер не сможет войти в домен, а для службы Netlogon будет зарегистрировано сообщение об ошибке аутентификации с идентификатором 3210 или 5722.

Если это произошло, необходимо сбросить пароль учетной записи компьютера. Один из способов сделать это — щелкнуть правой кнопкой мыши на учетной записи компьютера в окне **Active Directory — пользователи и компьютеры** и выбрать команду **Переустановить учетную запись** (Reset Account). После этого нужно удалить компьютер из домена (сделав его членом рабочей группы или другого домена), а затем снова подключить компьютер к домену.

> ***Практический совет***
>
> Есть несколько способов сбросить учетную запись компьютера. В Центре администрирования Active Directory щелкните правой кнопкой мыши по учетной записи компьютера и выберите команду **Переустановить учетную запись** (Reset Account). В командной строке можно использовать команду `dsmod *computer* -reset`. В Windows PowerShell можно использовать командлет Reset-ComputerMachinePassword или Set-ADAccountPassword с опцией `-Reset` для сброса пароля учетной записи. Следующая команда запускает командлет Reset-ComputerMachinePassword на удаленном компьютере:
>
> ```
> Invoke-Command -ComputerName EngPC84 -ScriptBlock
> {Reset-ComputerMachinePassword}
> ```
>
> Все эти команды требуют дополнительных действий в виде удаления компьютера из домена (путем помещения компьютера в другой домен или рабочую группу) и повторного присоединения компьютера к домену. Дополнительные действия могут потребоваться, поскольку пароли должны быть синхронизированы между локальным компьютером и доменом.

Несколько утилит используется для сброса пароля компьютера и синхронизации изменений в домене. На компьютерах, где установлен Windows PowerShell, можно использовать командлет Test-ComputerSecureChannel для тестирования безопасного соединения между компьютером и доменом. Зарегистрируйтесь локально на компьютере, откройте командную строку Windows PowerShell и введите команду:

```
test-computersecurechannel
```

Параметр `-Server` служит для тестирования канала с определенным контроллером домена. Если команда возвращает `False`, есть проблема соединения, и нужно использовать опцию `-Repair` для сброса пароля учетной записи компьютера и записи этого изменения в соответствующий объект компьютера на контроллере домена. Изменение пароля будет реплицировано другим контроллерам домена.

Другая утилита для сброса пароля компьютера и синхронизации изменений называется Netdom (работает в командной строке). Для получения более подробной информации см. статью Microsoft Knowledge Base Article 325850 (**support.microsoft.com/default.aspx?scid=kb;en-us;325850**).

Команда `netdom verify` используется для тестирования безопасного соединения между локальным компьютером и доменом. Команда `netdom resetpwd` служит для сброса пароля учетной записи локального компьютера и записи этих изменений в соответствующий объект компьютера на контроллере домена, что позволяет убедиться в изменении пароля на других контроллерах домена.

Для рядового сервера можно сбросить пароль учетной записи компьютера с помощью следующих действий:

1. Зарегистрируйтесь локально на компьютере. В командной строке введите команду `netdom resetpwd /s:`*`ServerName`* `/ud:`*`domain\UserName`* `/pd:*`, где *`ServerName`* — имя контроллера домена, который будет использоваться для установки пароля; *`domain\UserName`* — учетная запись администратора с правом изменения пароля, `*` — означает, что Netdom должен сначала запросить пароль учетной записи.
2. Введите пароль, когда программа его запросит. Netdom изменит пароль учетной записи компьютера локально и на контроллере домена. Контроллер домена распространит изменение пароля на другие контроллеры домена в домене.
3. Перезапустите компьютер.

Для контроллеров домена необходимо выполнить дополнительные действия. После *локальной* регистрации в системе нужно остановить службу **Центр распространения ключей Kerberos** (Kerberos Key Distribution Center) и установить тип запуска **Вручную** (Manual). После перезапуска компьютера проверьте, что пароль успешно сброшен, после этого можно перезапустить службу **Центр распространения ключей Kerberos** и установить тип запуска обратно на **Автоматически** (Automatic).

Перемещение учетных записей компьютера

Обычно учетные записи компьютера помещаются в контейнеры **Computers** или **Domain Controllers** либо в контейнеры пользовательских организационных подразделений. Переместить учетную запись в другой компьютер можно так: выберите компьютер в оснастке **Active Directory — пользователи и компьютеры**, а затем переместите его в другое место. В Центре администрирования Active Directory переместить пользователей нельзя.

Можно также использовать следующий метод для перемещения учетной записи компьютера при любом активном инструменте:

1. В дереве консоли выберите контейнер, в котором расположена учетная запись компьютера.
2. Щелкните правой кнопкой мыши и выберите команду **Переместить** (Move). Будет отображено одноименное окно (рис. 7.8).

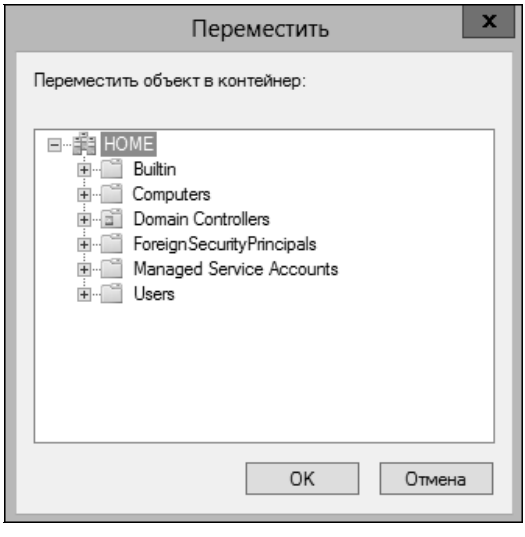


Рис. 7.8. Используйте окно **Переместить** для перемещения компьютера в разные контейнеры

3. Выберите контейнер, в который нужно переместить компьютер. Перейдите в подконтейнер или дочернее организационное подразделение. Нажмите кнопку **OK**.

Управление компьютерами

Утилита **Управление компьютером** (Computer Management) применяется для управления компьютерами, что ясно из ее названия. Независимо от используемой утилиты, **Active Directory — пользователи и компьютеры** или Центр администрирования Active Directory, можно открыть оснастку **Управление компьютером** и подсоединиться к определенному компьютеру, щелкнув правой кнопкой мыши по записи компьютера и выбрав команду **Управление** (Manage) из контекстного меню. Утилита **Управление компьютером** запустится и автоматически подключится к выбранному компьютеру.

Присоединение компьютера к домену или рабочей группе

Компьютер, присоединенный к домену или рабочей группе, может войти и получить доступ к сети. Для начала убедитесь, что сетевые компоненты надлежащим образом установлены на вашем компьютере. Они должны быть установлены во время инсталляции операционной системы. Также обратитесь к *главе 14*, в которой описана настройка соединений TCP/IP. Настройки TCP/IP должны быть корректными и разрешать связь между настраиваемым компьютером и контроллером домена. Если DHCP, WINS и DNS надлежащим образом на-

строены, рабочим станциям не нужно присваивать статический IP-адрес. Единственное, что требуется для присоединения компьютера к домену — имя компьютера и имя домена.

> ***Практический совет***
>
> Операционная система Windows Server 2012 автоматически предоставляет право **Добавление рабочих станций к домену** (Add Workstations To The Domain) неявной группе **Прошедшие проверку** (Authenticated Users). Это означает, что любой пользователь, который регистрируется в домене и проходит аутентификацию, может добавить рабочие станции в домен без необходимых полномочий администратора. Однако, из соображений безопасности, количество рабочих станций, которые аутентифицированный пользователь может добавить в домен, ограничено десятью. Если пользователь превысит этот предел, он получит сообщение об ошибке.
>
> Можно использовать утилиту Ldp.exe из утилит поддержки Windows Server 2012 для перезаписи лимита по умолчанию, установив атрибут ms-DS-MachineAccountQuota, но это плохая идея с точки зрения безопасности. Лучший и более надежный метод — создать необходимую учетную запись компьютера в определенном организационном подразделении или предоставить пользователю расширенные полномочия **Создание объектов: account** (Create Account Objects) для контейнера **Computers**. Можно также предоставить определенным пользователям полномочия **Удаление объектов: account** (Delete Account Objects) для контейнера **Computers**, что позволит назначенным пользователям удалять учетные записи из домена.

Во время установки операционной системы, вероятнее всего, уже было настроено сетевое соединение или же ранее компьютер был соединен с доменом или рабочей группой. Если это так, можно соединить компьютер с новым доменом или рабочей группой. Для этого в Windows Vista и более поздних версиях, а также в Windows Server 2008 *см. разд. "Вкладка Имя компьютера" главы 2.* Системы Windows 2000 Professional, Windows 2000 Server и Windows XP Professional и Windows Server 2003 настраиваются почти так же. Основное отличие — при щелчке по элементу **Система** в Панели управления диалоговое окно **Свойства системы** открывается сразу же.

Если имя не удалось изменить, будет отображено соответствующее сообщение, информирующее об этом, или сообщение о том, что учетная запись уже существует. Данная проблема может возникнуть при попытке изменить имя компьютера, который уже подключен к домену, либо если этот компьютер имеет активную сессию в этом домене. Можно закрыть приложение, подключенное к домену, например Проводник, получающий доступ к общей папке в сети. После этого можно повторить процесс изменения имени компьютера.

Если есть другие проблемы при соединении с доменом, убедитесь, что у настраиваемого компьютера правильная конфигурация сети. На компьютере должны быть установлены сетевые службы и в свойствах TCP/IP должен быть указан правильный DNS-сервер *(см. главу 14)*.

У всех аутентифицированных пользователей есть полномочия **Добавление рабочих станций к домену** (Add Workstations To The Domain), и по умолчанию пользователи могут создавать до 10 учетных записей компьютера при присоединении компьютера к домену. Пользователи, у которых есть полномочия **Создание объектов: account** (Create Account Objects), для контейнера **Computers** могут создать неограниченное количество учетных записей компьютера в домене. Однако у учетных записей компьютера, созданных аутентифицированными пользователями, владельцем является член группы **Администраторы домена**, а у учетных записей, созданных пользователями с правами **Создание объектов: account**, в качестве владельца устанавливается пользователь, создавший эту учетную запись. Если предоставить полномочие **Создание объектов: account**, можно также предоставить полномочие **Удаление объектов: account**, чтобы пользователи могли удалить учетные записи компьютера из домена.

Предоставить привилегии **Создание объектов: account**, **Удаление объектов: account** (или обе эти привилегии) для контейнера **Computers** можно с помощью следующих действий:

1. Откройте оснастку **Active Directory — пользователи и компьютеры** или Центр администрирования Active Directory. В оснастке **Active Directory — пользователи и компьютеры** убедитесь, что в меню **Вид** активирована команда **Дополнительные параметры**.
2. Щелкните правой кнопкой мыши по контейнеру **Computers** и выберите команду **Свойства**.
3. На вкладке **Безопасность** (Security) нажмите кнопку **Дополнительно** (Advanced). В диалоговом окне **Дополнительные параметры безопасности для "Computers"** (Advanced Security Settings For Computers) нажмите кнопку **Добавить**, чтобы открыть окно **Элемент разрешения для "Computers"** (Permission Entry For Computers).
4. Щелкните по ссылке **Выберите субъект** (Select A Principal). В окне **Выбор: "Пользователь", "Компьютер", "Учетная запись служба" или "Группа"** (Select User, Computer, Service Account, Or Group) выберите пользователя или группу, которым нужно предоставить полномочия, и нажмите кнопку **OK**. Задайте привилегии и снова нажмите кнопку **OK**.

Использование автономной регистрации в домене

Компьютеры под управлением Windows 7 и Windows 8 поддерживают автономную регистрацию в домене (offline domain join), так же как и серверы под управлением Windows Server 2008 R2 и более поздних версий. В этих версиях Windows есть утилита Djoin.exe. Любой член группы **Администраторы домена** может осуществить автономную регистрацию в домене (как и любой другой пользователь с надлежащими правами).

Основные действия для осуществления автономной регистрации в домене:

1. Создайте учетную запись компьютера в Active Directory и начните репликацию совместно используемых секретов[1] компьютера, который должен присоединиться к домену.
2. Запишите в текстовый файл соответствующую информацию состояния, необходимую для присоединения компьютера к домену, и сделайте информацию состояния доступной компьютеру.
3. После включения компьютера Windows прочитает данные настройки, и компьютер будет присоединен к домену.

> ***Примечание***
>
> Компьютеры клиентов должны быть подключены к корпоративной сети для подсоединения к домену или получения настроек домена. Благодаря новой функции удаленного подключения к домену Windows Server 2012 предоставляет возможность для компьютеров под управлением Windows 8 присоединяться к домену и получать настройки домена удаленно из Интернета.

Чтобы настроить метаданные учетной записи компьютера, нужно запустить утилиту Djoin.exe в командной строке с правами администратора. Метаданные учетной записи компьютера будут записаны в текстовый файл. После настройки компьютера можно снова запустить Djoin.exe, чтобы запросить метаданные учетной записи компьютера и добавить их

[1] См. **http://technet.microsoft.com/ru-ru/library/cc740124(v=ws.10).aspx**. — *Прим. пер.*

в каталог Windows целевого компьютера. Альтернативно можно сохранить метаданные учетной записи компьютера в файл Unattend.xml, а затем указать этот файл во время необслуживаемой установки операционной системы.

Для подготовки текстового файла с метаданными выполните следующие действия:

1. Используя учетную запись с правами присоединения компьютера к домену, войдите в систему компьютера, являющегося членом домена.
2. Используйте Djoin.exe для создания текстового файла с метаданными учетной записи компьютера. Чтобы сделать это, в командной строке с правами администратора введите команду `djoin /provision /domain` *`DomainName`* `/machine` *`MachineName`* `/savefile FileName`, где *`DomainName`* — имя домена, к которому нужно присоединиться; *`MachineName`* — имя компьютера; *`FileName`* — имя текстового файла, в который будут записаны метаданные. Например: `djoin /provision /domain cpandl /machine HrComputer15 /savefile Hrcomputer15.txt`.

   > ***Совет***
   >
   > По умолчанию учетные записи компьютера создаются в контейнере **Computers**. Если нужно использовать другой контейнер, добавьте параметр `/Machineou` и укажите контейнер, который нужно использовать. Если объект компьютера уже создан, все еще можно сгенерировать метаданные с помощью параметра `/reuse`. Если контроллер домена еще не работает под управлением Windows Server 2008 R2 или Windows Server 2012, добавьте параметр `/downlevel`.

3. На новом компьютере используйте команду Djoin.exe для импортирования текстового файла. Откройте командную строку с правами администратора и введите команду `djoin /requestODJ /loadfile` *`FileName`* `/windowspath %SystemRoot% /localosCaution`, где *`FileName`* — имя файла с метаданными. Например: `djoin /requestODJ /loadfile HrComputer15.txt /windowspath %SystemRoot% /localos`.
4. Убедитесь, что новый компьютер подключен к сети, и затем перезагрузите его. Во время запуска компьютер будет присоединен к домену.

Можно использовать файл Unattend.xml для подготовки компьютера путем создания раздела в этом файле и затем добавления содержимого текстового файла с метаданными в элемент `AccountData`, как показано в этом примере:

```
<Component>
 <Component name=Microsoft-Windows-UnattendedJoin>
 <Identification>
  <Provisioning>
   <AccountData> Insert metadata here! </AccountData>
  </Provisioning>
 </Identification>
</Component>
```

После создания файла Unattend.xml запустите новый компьютер в безопасном режиме или запустите среду предустановки Windows (Windows Preinstallation Environment), а затем запустите команду Setup с файлом ответа, как показано в следующем примере:

```
setup /unattend: FullPathToAnswerFile
```

Здесь *`FullPathToAnswerFile`* — полный путь к файлу Unattend.xml.

Управление контроллерами домена, ролями и каталогами

Контроллеры домена осуществляют много важных задач в доменах Active Directory. Многие из этих задач обсуждались в *главе 6*.

Установка и понижение роли контроллера домена

Контроллер домена устанавливается путем настройки доменных служб Active Directory на сервере. Позже, если не нужно, чтобы сервер выполнял задачи контроллера, можно понизить роль сервера. Тогда он снова станет работать как рядовой сервер. Перед установкой или понижением роли сервера нужно учитывать влияние этой операции на сеть *(см. также разд. "Структура каталогов" главы 6)*.

При установке контроллера домена, возможно, понадобится передать хозяина роли и заново настроить структуру глобального каталога. Кроме того, перед установкой доменных служб Active Directory в сети нужно развернуть DNS-сервер. При создании доменных служб AD DNS-делегация автоматически создается во время процесса установки, и этот процесс требует использования учетных данных с полномочиями обновления родительских DNS-зон.

Чтобы добавить первый контроллер домена под управлением Windows Server 2012 в существующую инфраструктуру Active Directory, мастер установки Active Directory автоматически запускает Adprep.exe для леса и домена. Подготовка леса и домена включает обновление схемы Active Directory (если нужно), создание новых объектов и контейнеров (если нужно) и модификацию дескрипторов безопасности и списков управления доступом. Для подготовки леса учетная запись должна быть членом группы **Администраторы схемы**, **Администраторы предприятия** и **Администраторы домена** для домена, в котором размещена мастер-схема и который по умолчанию является корневым доменом леса. Для подготовки домена используется учетная запись, которая может регистрироваться на владельце инфраструктуры и является членом группы **Администраторы домена**. Для подготовки RODC нужно использовать учетную запись, которая является членом группы **Администраторы предприятия**.

Перед понижением роли контроллера домена нужно переместить все его ключевые обязанности на другие контроллеры домена. Это означает отключение глобального каталога сервера и передача любых FSMO-операций, если необходимо. Также нужно удалить любые разделы каталога приложений, находящиеся на сервере.

> ***Практический совет***
>
> Заметьте, что на Windows Server 2012 все задачи установки и настройки AD DS выполняются через диспетчер серверов. Больше не нужно запускать мастер установки и отдельные задачи в командной строке. Также нет необходимости вручную подготавливать Active Directory для Windows Server 2012.
>
> Обратите внимание, что в Windows Server 2003 и выше больше не нужно понижать в роли контроллер домена, если необходимо переименовать его. Можно переименовать контроллер домена в любое время. С этим есть одна проблема — сервер станет недоступным пользователям на время процесса переименования, и нужно принудительно обновить каталог для повторной установки коммуникаций с сервером. Нельзя, однако, переместить контроллер домена в другой домен. Нужно понизить в роли контроллер домена, обновить настройки домена для сервера и его учетную запись компьютера, а затем сделать его контроллером домена в другом домене.

Для установки контроллера домена выполните следующие действия:

1. Локальный сервер автоматически добавляется для управления в диспетчере серверов. Если нужно установить AD DS на другой сервер, необходимо добавить его для управления, используя команду **Добавление серверов** (Add Servers). Использование диспетчера серверов для удаленного управления требует конфигурации, рассмотренной в *главе 2*, и минимальный набор полномочий. Обычно, нужно иметь полномочия группы **Администраторы домена** или другие явные полномочия для добавления сервера и удаленного управления им. Для установки нового леса Active Directory надо зарегистрироваться, используя локальную учетную запись компьютера **Администратор**. Для установки нового дочернего домена или нового дерева домена нужно зарегистрироваться в качестве члена группы **Администраторы предприятия**.
2. В диспетчере серверов в меню **Управление** выберите команду **Добавить роли и компоненты** (Add Roles And Features). Будет запущен мастер добавления ролей и компонентов (Add Roles And Features Wizard). Если мастер отобразит страницу **Перед началом работы** (Before You Begin), прочитайте приветствие и нажмите кнопку **Далее**.
3. На странице **Выбор типа установки** (Select Installation Type) выберите **Установка ролей или компонентов** (Role-Based Or Feature-Based Installation) и затем нажмите кнопку **Далее**.
4. На странице **Выбор целевого сервера** (Select Destination Server) показан пул серверов, добавленных вами для управления. Выберите сервер, который нужно настроить, и нажмите кнопку **Далее**.
5. На странице **Выбор ролей сервера** (Select Server Roles) установите флажок **Доменные службы Active Directory** (Active Directory Domain Services) и нажмите кнопку **Далее** дважды. Затем нажмите кнопку **Установить** (Install). Запустится мастер установки доменных служб Active Directory (Active Directory Domain Services Installation Wizard).
6. Когда задача первоначальной установки будет завершена, нужно щелкнуть по ссылке **Повысить роль этого сервера до уровня контроллера домена** (Promote This Server To A Domain Controller) для запуска мастера настройки доменных служб Active Directory (Active Directory Domain Services Configuration Wizard). Если окно мастера добавления ролей и компонентов было закрыто, нужно щелкнуть на значке **Уведомления** (Notification), а затем выбрать команду **Повысить роль этого сервера до уровня контроллера домена** (Promote This Server To A Domain Controller).

   ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

   Если установка не увенчалась успехом, запомните ошибку и внесите соответственные коррективы перед перезапуском этой процедуры. Обычно ошибки установки связаны с полномочиями, необходимыми для подготовки леса или домена для первого использования Windows Server. В этом случае выйдите из системы и войдите снова с надлежащими правами.

7. Если компьютер в данный момент является рядовым сервером, мастер позволит выполнить все действия, необходимые для установки Active Directory, в том числе автоматическую подготовку схемы каталога в лесу или домене для Windows Server 2012. Нужно указать, является ли этот сервер контроллером домена для нового домена или дополнительным контроллером домена для уже существующего домена. Чтобы проверить, что контроллер домена правильно установлен, проверьте журнал событий службы каталогов (Directory Services) на наличие ошибок, убедитесь, что папка SYSVOL доступна, удостоверьтесь, что работает разрешение имен через DNS, и проверьте репликацию изменений Active Directory.

Для понижения роли контроллера домена выполните следующие действия:

1. В консоли **Диспетчер серверов** (Server Manager) в меню **Управление** выберите команду **Удалить роли и компоненты** (Remove Roles And Features), в результате будет запущен мастер удаления ролей и компонентов (Remove Roles And Features Wizard). Если мастер отобразит страницу **Перед началом работы**, прочитайте приветствие и нажмите кнопку **Далее**.
2. На странице **Выбор целевого сервера** показан пул серверов, добавленных для управления. Выберите сервер, который нужно настроить, и нажмите кнопку **Далее**.
3. На странице **Выбор ролей сервера** сбросьте флажок **Доменные службы Active Directory**, указав тем самым, что нужно удалить эту роль.
4. Появится новое окно. В нем установите флажок **Удалить средства управления** (Remove Management Tools), чтобы средства управления AD DS были удалены, нажмите кнопку **Удалить компоненты** (Remove Features). После этого нажмите кнопку **Продолжить** (Continue). Затем нажмите кнопку **Далее** дважды.
5. На странице **Учетные данные** (Credentials) обратите внимание на вашу текущую учетную запись. Если нужно, предоставьте другие учетные данные с правами, необходимыми для удаления контроллера домена. Нажмите кнопку **Далее**.
6. Если будет отображена страница **Предупреждения** (Warnings), отметьте флажок **Продолжить удаление** (Proceed With Removal), а затем нажмите кнопку **Далее**.
7. Введите новый пароль и его подтверждение для вашей локальной учетной записи **Администратор**. Пароли должны совпадать. Нажмите кнопку **Далее**.
8. На странице **Подтверждение удаления компонентов** (Confirm Removal Selections) есть возможность установить флажок **Автоматический перезапуск конечного сервера, если требуется** (Restart The Destination Server Automatically If Required). Поскольку для полного удаления необходим запуск сервера, можно выбрать эту опцию, а затем подтвердить ее, нажав кнопку **Да**. Когда будете готовы продолжить, нажмите **Удалить** (Remove).

Осторожно!

Понижение роли сервера корректно передает любые роли, обрабатываемые сервером. Однако, если предыдущие попытки понизить роль контроллера домена не увенчались успехом, повторите эту процедуру и установите флажок **Принудительно удалить этот контроллер домена** (Force The Removal Of This Domain Controller). FSMO-роли контроллера домена можно оставить в некорректном состоянии, пока они не будут повторно назначены администратором. Данные домена также можно оставить в неопределенном состоянии.

Практический совет

Альтернативная техника установки контроллеров домена — использовать резервные носители. Данная возможность была представлена в Windows Server 2003. Для установки контроллера из резервного носителя создайте резервную копию системных данных контроллера домена и восстановите ее на другом сервере под управлением Windows Server 2003 и выше. При создании контроллера домена из резервного носителя не нужно реплицировать всю базу данных каталога по сети на новый контроллер домена. Это может реально сэкономить день при ограниченной пропускной способности или если база данных содержит тысячи записей.

Просмотр и передача ролей домена

Оснастка **Active Directory — пользователи и компьютеры** также используется для просмотра или изменения FSMO-ролей. На уровне домена можно работать с ролями для владельцев относительных ID, владельцев эмулятора первичного контроллера домена и владельцев инфраструктуры.

> ***Примечание***
>
> FSMO-роли описаны в *главе 6*. Для установки роли владельца доменных имен можно использовать утилиту **Active Directory — домены и доверие** (Active Directory Domains And Trusts) и утилиту **Схема Active Directory** (Active Directory Schema) для изменения роли владельца схемы. Самый быстрый способ определить текущие FSMO для всех ролей — это ввести команду `netdom query fsmo` в командной строке.

Для просмотра текущих FSMO-ролей выполните следующие действия:

1. В оснастке **Active Directory — пользователи и компьютеры** щелкните правой кнопкой мыши по элементу **Пользователи и компьютеры Active Directory** в дереве консоли. Из контекстного меню выберите команду **Все задачи | Хозяева операций** (All Tasks | Operations Masters). Будет открыто окно **Хозяева операций** (Operations Masters), изображенное на рис. 7.9.
2. В окне **Хозяева операций** (Operations Masters) есть три вкладки. Вкладка **RID** показывает текущее положение владельца относительных идентификаторов, на вкладке **PDC** отображено местоположение текущего владельца эмулятора PDC, а вкладка **Инфраструктура** (Infrastructure) демонстрирует положение текущего мастера инфраструктуры.

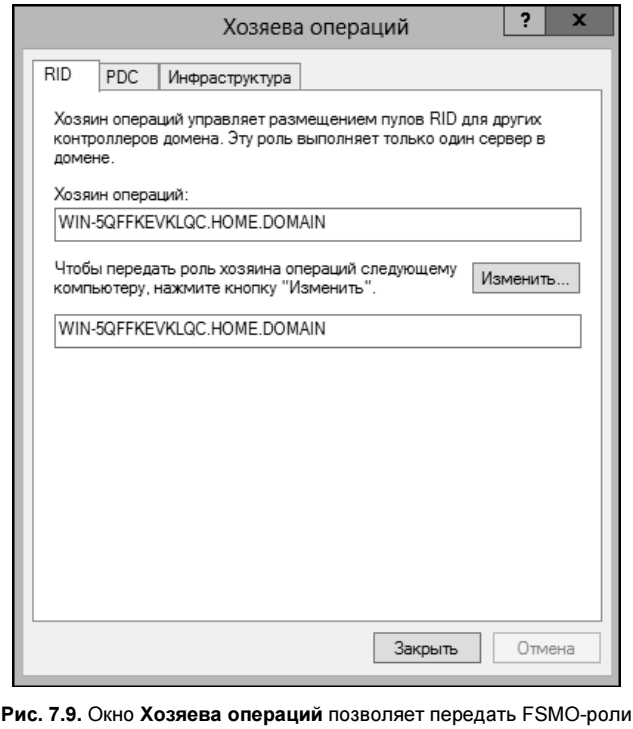


Рис. 7.9. Окно **Хозяева операций** позволяет передать FSMO-роли или посмотреть их текущее назначение

Передать текущие операции другим серверам можно так:

1. Запустите оснастку **Active Directory — пользователи и компьютеры**. В дереве консоли щелкните правой кнопкой мыши на узле **Пользователи и компьютеры Active Directory**, а затем выберите команду **Сменить контроллер домена** (Change Domain Controller).
2. В окне **Смена сервера каталогов** (Change Directory Server) выберите опцию **Этот контроллер домена или экземпляр AD LDS** (This Domain Controller Or AD LDS Instance), затем выберите контроллер домена, на который нужно перенести FSMO-роли, и нажмите кнопку **OK**.
3. В дереве консоли щелкните правой кнопкой мыши на узле **Пользователи и компьютеры Active Directory**. В контекстном меню выберите команду **Все задачи | Хозяева операций**.
4. В окне **Хозяева операций** перейдите на вкладку **RID**, **PDC** или **Инфраструктура** (в зависимости от типа роли, которую нужно перенести).
5. Нажмите кнопку **Изменить** для передачи роли ранее выбранному контроллеру домена. Нажмите кнопку **OK**.

Просмотр и передача роли *Владелец доменных имен*

Для просмотра или изменения местоположения владельца доменных имен в лесу можно использовать оснастку **Active Directory — домены и доверие** (Active Directory Domains And Trusts). В этой оснастке корневой уровень дерева консоли показывает выбранный в данный момент домен.

> ***Совет***
>
> Если нужно подключиться к другому домену, подключитесь к контроллеру домена, как было описано ранее в этой главе. Разница только в том, что теперь нужно использовать оснастку **Active Directory — домены и доверие**.

Для передачи роли владельца доменных имен выполните следующие действия:

1. Запустите оснастку **Active Directory — домены и доверие**. В дереве консоли щелкните правой кнопкой мыши на узле **Active Directory — домены и доверие**, а затем выберите команду **Сменить контроллер домена Active Directory** (Change Active Directory Domain Controller).
2. В окне **Смена сервера каталогов** (Change Directory Server) выберите опцию **Этот контроллер домена или экземпляр AD LDS** (This Domain Controller Or AD LDS Instance), а затем выберите контроллер домена, которому нужно передать роль владельца доменных имен. Нажмите кнопку **OK**.
3. В дереве консоли щелкните правой кнопкой мыши по узлу **Active Directory — домены и доверие**, а затем выберите команду **Хозяин операции** (Operations Master). Будет открыто одноименное окно.
4. В окне появится сервер, играющий роль *хозяина именования доменов*. Нажмите кнопку **Изменить** для передачи роли ранее выбранному контроллеру домена.
5. Нажмите кнопку **Закрыть**.

Просмотр и передача роли хозяина схемы

Оснастка **Схема Active Directory** (Active Directory Schema) используется для просмотра или изменения расположения хозяина схемы. Для регистрации этой оснастки откройте командную строку с правами администратора и введите команду `regsvr32 schmmgmt.dll`. Затем можно передать роль хозяина схемы так:

1. Откройте оснастку **Схема Active Directory** в консоли **Управление компьютером**.
2. В дереве консоли щелкните правой кнопкой мыши по узлу **Схема Active Directory** и выберите команду **Сменить контроллер домена Active Directory**.
3. Выберите опцию **Любой доступный для записи контроллер домена** (Any Writable Domain Controller) для разрешения Active Directory автоматически выбирать нового хозяина схемы или установите переключатель **Этот контроллер домена или экземпляр AD LDS** (This Domain Controller Or AD LDS) для выбора нового хозяина схемы.
4. Нажмите кнопку **OK**. В дереве консоли щелкните правой кнопкой мыши по узлу **Схема Active Directory** и выберите команду **Хозяин операций**.
5. Нажмите кнопку **Сменить** (Change) в окне **Смена хозяина схемы** (Change Schema Master). Нажмите кнопку **OK**, а затем — кнопку **Закрыть**.

Передача ролей с использованием командной строки

Другой способ передачи ролей — использовать команду Netdom для вывода текущих владельцев ролей FSMO, а затем использовать утилиту Ntdsutil.exe для передачи ролей. Ntdsutil.exe — утилита командной строки для управления Active Directory. Для передачи ролей в командной строке нужно выполнить следующие действия:

1. Получите список владельцев ролей FSMO с помощью команды `netdom query fsmo` в командной строке.
2. Рекомендуется (но не требуется) войти в консоль сервера, который нужно назначить новым хозяином операций. Можно войти в консоль локально или использовать удаленный рабочий стол.
3. Откройте приглашение командной строки. Один из способов сделать это — нажать клавишу <Windows> и ввести команду `cmd.exe`, а затем нажать клавишу <Enter>.
4. В приглашении введите команду `ntdsutil`. Будет запущено средство Directory Services Management Tool.
5. В приглашении **ntdsutil** введите `roles`. Это переведет утилиту в режим **fsmo maintenance**.
6. В командной строке управления FSMO введите `connections`. В приглашении **server connections** введите `connect to server` и полное доменное имя контроллера домена, которому надо назначить FSMO-роль, например, `connect to server engdc01.technology.adatum.com`. После успешной установки соединения введите `quit` для выхода из приглашения **server connections**. В приглашении **fsmo maintenance** сначала введите `transfer`, а затем идентификатор роли, которую нужно передать:
   - `pdc` — роль эмулятора PDC;
   - `rid master` — роль хозяина RID;
   - `schema master` — роль хозяина схемы;
   - `domain naming master` — роль хозяина доменных имен.

7. Введите `quit` для выхода из режима **fsmo maintenance**, а затем еще раз `quit` для выхода из утилиты Ntdsutil.

Захват ролей с использованием командной строки

Иногда может возникнуть ситуация, когда нельзя корректно передать роли сервера. Например, у контроллера домена, работающего в качестве хозяина RID, может отказать диск, что в итоге сделает недоступным весь сервер. Если невозможно восстановить рабочее состояние сервера, нужно захватить роль RID и присвоить ее другому контроллеру домена.

> ***Примечание***
>
> Захват роли сервера возможен, только когда контроллер домена, управляющий ролью, недоступен. Когда исходный сервер станет доступен, он распознает изменение и примет его.

Прежде чем произвести захват роли, убедитесь в актуальности контроллера домена, которому нужно передать роль, относительно предыдущего владельца роли. Active Directory отслеживает изменения репликации, используя порядковые номера обновления (update sequence numbers, USN). Поскольку репликация занимает некоторое время, не все контроллеры домена обязательно будут актуальны. Если сравнить USN контроллеров домена, можно определить, является ли контроллер домена самым актуальным относительно предыдущего владельца роли. Если контроллер домена актуален, можно безопасно передать роль. Если же это не так, можно дождаться репликации, а затем уже передать роль контроллеру домена.

В Windows Server 2012 есть несколько инструментов для работы с репликацией Active Directory. Одним из инструментов, которым можно воспользоваться, является Repadmin.

Отобразить состояние последней репликации для контроллера домена можно командой `repadmin /showrepl`. Синтаксис таков:

```
repadmin /showrepl DomainControllerName NamingContext
```

Здесь *`DomainControllerName`* — полное доменное имя контроллера домена, а *`NamingContext`* — имя домена, в котором находится сервер.

В следующем примере используется раздел по умолчанию для Server252 в домене Cpandl.com:

```
repadmin /showrepl server252.cpandl.com dc=cpandl,dc=com
```

> ***Примечание***
>
> PowerShell обрабатывает команды не так, как командная строка. Обычно можно ввести команды в приглашении PowerShell так же, как и в командной строке. Однако здесь PowerShell будет ошибочно считать `dc=cpandl,dc=com` двумя разными параметрами. Чтобы указать, что это один параметр, используйте кавычки: `"dc=cpandl,dc=com"`.

Чтобы отобразить наивысший порядковый номер для указанного контекста имен по каждому партнеру репликации определенного контроллера домена, введите следующее в командной строке:

```
repadmin /showutdvec DomainControllerName NamingContext
```

В этом примере отображается наивысший номер для раздела конфигурации по умолчанию на Server252 в домене Cpandl.com так:

```
repadmin /showutdvec server252.cpandl.com dc=cpandl,dc=com
```

Вывод команды покажет наивысший USN на партнерах репликации для раздела конфигурации по умолчанию:

```
Default-First-Site-Name\SERVER252 @ USN 45164 @ Time 2014-03-30 11:35:24
Default-First-Site-Name\SERVER147 @ USN 45414 @ Time 2014-03-30 11:42:16
```

Если Server252 был предыдущим хозяином роли и контроллер домена, которому нужно назначить роль, имеет USN, больший или равный USN сервера Server252, значит, контроллер домена актуален. Если же USN контроллера домена, которому нужно назначить роль, меньше USN исходного хозяина роли, значит, контроллер домена неактуален и нужно подождать, прежде чем можно будет захватить роль. Также можно использовать команду `repadmin /syncall` для принудительной репликации самого актуального контроллера домена (относительно предыдущего владельца роли) со всеми его партнерами репликации.

В PowerShell можно использовать следующие командлеты управления репликацией для просмотра и решения проблем репликации Active Directory:

- Get-ADReplicationAttributeMetadata — получает метаданные репликации для атрибутов указанного уникального имени (Distinquished Name, DN);
- Get-ADReplicationFailure — получает информацию о сбое репликации для указанного сервера, сайта, домена или леса (если применимо);
- Get-ADReplicationPartnetMetadada — получает метаданные репликации для указанного сервера, сайта, домена или леса;
- Get-ADReplicationQueueOperation — получает операции ожидания в очереди сервера репликации;
- Get-ADReplicationUpToDatenessVectorTable — получает наивысший USN для определенного сервера, сайта, домена или леса;
- Sync-ADObject — выполняет репликацию указанного объекта каталога.

Используйте командлет Get-ADReplicationPartnerMetadata для получения информации о входящей репликации сервера. Синтаксис следующий:

```
Get-ADReplicationPartnerMetadata -Target Object [-Scope Server|Site|Domain|Forest]
[-Partition Domain|Schema|Configuration|*]
```

Здесь параметр `-Target` задает имя сервера, сайта, домена или леса. Параметр `-Scope` требуется при работе с объектами, отличными от серверов. Установка раздела (`-Partition`) нужна, когда необходимо работать не с разделами по умолчанию.

В следующем примере исследуется раздел по умолчанию на CorpServer98:

```
get-adreplicationpartnermetadata -target corpserver98
```

Для исследования разделов всего сервера применяется следующий синтаксис:

```
get-adreplicationpartnermetadata -target corpserver98 -partition *
```

Подобно команде `repadmin /showutdvec`, командлет Get-ADReplicationUpToDatenessVectorTable отображает наивысшие порядковые номера для реплицируемых разделов и может помочь решить проблемы репликации. Базовый синтаксис:

```
Get-ADReplicationUpToDatenessVectorTable -Target Object [-Scope
Server|Site|Domain|Forest] [-Partition Domain|Schema|Configuration|*]
```

В этом примере отображается наивысший порядковый номер для раздела по умолчанию (раздел конфигурации домена) на CorpServer98:

```
get-adreplicationuptodatenessvectortable -target corpserver98
```

Вывод покажет наивысший USN на партнерах репликации для раздела конфигурации по умолчанию:

```
LastReplicationSuccess : 3/30/2014 1:45:57 PM
Partition       : DC=cpandl,DC=com
PartitionGuid   : c39cfdbd-e1a1-4c4c-9355-85d7ea05c10a
Partner         : CN=NTDS Settings,CN=CORPSERVER172,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cpandl,DC=com
PartnerInvocationId  : fb32931c-e319-473a-8069-d781f980057b
Server          : CorpServer98.cpandl.com
UsnFilter       : 82656
LastReplicationSuccess : 3/30/2014 1:48:44 PM
Partition       : DC=cpandl,DC=com
PartitionGuid   : c39cfdbd-e1a1-4c4c-9355-85d7ea05c10a
Partner         : CN=NTDS Settings,CN=CORPSERVER98,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cpandl,DC=com
PartnerInvocationId  : d8bf2da2-b08d-4d36-bc53-1b7f62643437
Server          : CorpServer98.cpandl.com
UsnFilter       : 12593
```

Интерпретировать вывод нужно так же, как и вывод команды `repadmin /showutdvec`. Если подозреваете проблему, можно использовать командлет Get-ADReplicationFailure для исследования проблем репликации. Основной синтаксис таков:

```
Get-ADReplicationFailure -Target Object [-Scope Server|Site|Domain|Forest]
```

Зная это, можно отобразить информацию обо всех сбоях репликации в домене Cpandl.com с помощью команды:

```
get-adreplicationfailure -Target "cpandl.com" -Scope Domain
```

Для отображения информации для определенного сайта используется команда:

```
get-adreplicationfailure -Target "NewYork-FirstSite" -Scope Site
```

Отображение информации для определенного сервера:

```
get-adreplicationfailure -Target CorpServer172
```

Следующие действия используются для захвата роли:

1. Введите `netdom query fsmo` в командной строке для получения списка текущих владельцев ролей FSMO.
2. Убедитесь, что текущий контроллер домена с ролью, которую нужно захватить, находится в состоянии оффлайн. Если сервер может вернуться в состояние онлайн, не выполняйте эту процедуру за исключением случая, когда необходимо полностью переустановить этот сервер.
3. Рекомендуется зайти с консоли сервера, который нужно назначить в качестве нового хозяина операций. Зайти в консоль можно локально или с использованием удаленного рабочего стола.
4. Откройте окно командной строки.
5. В приглашении командной строки введите `ntdsutil`. Будет запущено средство Directory Services Management Tool.
6. В приглашении **ntdsutil** введите `roles`. Это переведет утилиту в режим **fsmo maintenance**.

7. В приглашении **fsmo maintenance** введите `connections`. В приглашении **server connections** введите `connect to server` и полное доменное имя контроллера домена, которому нужно назначить роль FSMO, например, `connect to server engdc01.technology.adatum.com`
8. После успешной установки соединения введите `quit` для выхода из приглашения **server connections**. В приглашении **fsmo maintenance** сначала введите `seize`, а затем идентификатор роли, которую необходимо захватить. Идентификаторы следующие:
   - `pdc` — роль эмулятора PDC;
   - `rid master` — роль хозяина RID;
   - `schema master` — роль хозяина схемы;
   - `domain naming master` — роль хозяина доменных имен.
9. Введите `quit` для выхода из режима **fsmo maintenance** и затем еще раз `quit` для выхода из утилиты Ntdsutil.

Настройка глобальных каталогов

Роль глобальных каталогов очень важна в сети. Эта роль обсуждалась в *разд. "Структура каталога" главы 6*. Настройка дополнительных глобальных каталогов осуществляется путем включения размещения глобального каталога на контроллере домене. В дополнении если есть два или более глобальных каталогов в пределах сайта, то можно прекратить размещение глобального каталога на каком-то контроллере домена. Это можно сделать путем отключения глобального каталога на контроллере домена.

Включить или отключить глобальный каталог можно с помощью следующих действий:

1. В оснастке **Active Directory — сайты и службы** (Active Directory Sites and Services) разверните сайт, с которым нужно работать.
2. Разверните папку **Servers** сайта и затем выберите сервер, на котором необходимо разместить глобальный каталог.
3. На центральной панели щелкните правой кнопкой мыши по имени **NTDS Settings** и затем выберите команду **Свойства**.
4. Для включения размещения глобального каталога установите флажок **Глобальный каталог** (Global Catalog) на вкладке **Общие** (General).
5. Для отключения размещения глобального каталога сбросьте флажок **Глобальный каталог** на вкладке **Общие**.

> ***Осторожно!***
>
> Не включайте или выключайте глобальные каталоги без надлежащего планирования и анализа влияния на сеть. В крупном производственном окружении назначение контроллера домена глобальным каталогом может стать причиной репликации огромного количества данных по сети.

Настройка кэширования членства в универсальных группах

Кэширование членства в универсальных группах устраняет зависимость от доступности сервера глобального каталога во время входа в систему. При активации этой опции в домене, работающем в режиме Windows Server 2003 или выше, любой контроллер домена может

разрешить запросы входа локально, без обращения к серверу глобального каталога. В *главе 6* указывалось, что у этого способа есть преимущества и недостатки.

Включить или выключить кэширование состава универсальных групп можно так:

1. В оснастке **Active Directory — сайты и службы** разверните сайт, с которым нужно работать.
2. На центральной панели щелкните правой кнопкой мыши по имени **NTDS Site Settings** и выберите команду **Свойства**.
3. Для включения кэширования членства в универсальных группах установите флажок **Разрешить кэширование членства в универсальных группах** (Enable Universal Group Membership Caching) на вкладке **Параметры сайта** (Site Settings). Затем из списка **Обновлять кэш из** (Refresh Cache From) выберите сайт, членство в универсальных группах которого нужно кэшировать. Выбранный сайт должен иметь рабочий сервер глобального каталога.
4. Чтобы выключить кэширование, сбросьте флажок **Разрешить кэширование членства** в универсальных группах на вкладке **Параметры сайта**.
5. Нажмите кнопку **OK**.

Управление организационными подразделениями

Как было показано в *главе 6*, организационные подразделения (единицы) помогают организовать объекты, применить групповую политику к ограниченному числу объектов и т. д. В этом разделе будет показано, как создавать и управлять организационными подразделениями.

Создание организационных подразделений

Обычно организационные подразделения создаются для отображения деловой или функциональной структуры организации. Также можно создавать подразделения из административных соображений, например, если нужно предоставить права делегирования пользователям или администраторам. Можно создать организационные подразделения как подгруппы домена или как дочерние подразделения в пределах существующего организационного подразделения.

Для создания организационного подразделения выполните следующие действия:

1. В оснастке **Active Directory — пользователи и компьютеры** или Центре администрирования Active Directory щелкните правой кнопкой мыши на узле домена или существующем организационном подразделении, в зависимости от того, куда нужно добавить новое организационное подразделение. Из контекстного меню выберите команду **Создать | Подразделение** (New | Organizational Unit).
2. Введите имя организационного подразделения и нажмите кнопку **OK**.
3. Теперь можно переместить учетные записи и общие ресурсы в организационное подразделение *(см. разд. "Перемещение учетных записей компьютеров" ранее в этой главе)*.

Просмотр и редактирование свойств организационных подразделений

Для просмотра и редактирования свойства организационного подразделения выполните действия:

1. Откройте оснастку **Active Directory — пользователи и компьютеры** или Центр администрирования Active Directory.
2. Щелкните правой кнопкой мыши на организационном подразделении, с которым нужно работать, а затем выберите команду **Свойства**. Это отобразит окно **Свойства**, позволяющее просмотреть и отредактировать свойства.

Переименование и удаление организационных подразделений

Переименовать или удалить организационное подразделение можно так:

1. В оснастке **Active Directory — пользователи и компьютеры** щелкните правой кнопкой мыши на организационном подразделении, которое нужно переименовать или удалить.
2. Для удаления подразделения выберите команду **Удалить** (Delete), затем подтвердите удаление, нажав кнопку **Да**.
3. Для переименования подразделения выберите команду **Переименовать** (Rename), затем введите новое название подразделения и нажмите клавишу <Enter>.

В Центре администрирования Active Directory аналогичным образом можно удалить подразделение, но для переименования нужно открыть его окно **Свойства**, ввести новое имя и нажать кнопку **OK**.

Перемещение организационных подразделений

Администратор может переместить организационное подразделение в любое другое место в пределах домена в любое время. В оснастке **Active Directory — пользователи и компьютеры** просто выберите подразделение и переместите его в нужное местоположение.

В оснастке **Active Directory — пользователи и компьютеры** и в Центре администрирования Active Directory организационное подразделение можно переместить также с помощью следующих действий:

1. Щелкните правой кнопкой мыши на папке подразделения, которое нужно переместить, и выберите команду **Переместить** (Move).
2. В окне **Переместить** (Move) разверните домен и затем выберите контейнер, в который нужно переместить организационное подразделение. Нажмите кнопку **OK**.

Управление сайтами

Мастер установки доменных служб Active Directory создает сайт по умолчанию и ссылку на сайт по умолчанию, когда устанавливаются доменные службы Active Directory на первом контроллере домена в сайте. Сайт по умолчанию называется Default-First-Site-Name, а ссылка по умолчанию — DEFAULTIPSITELINK. Можно удалить сайт по умолчанию и ссылку на сайт в случае необходимости. После этого нужно создать сайт и ссылку вручную.

Настройка сайта — это процесс, состоящий из следующих этапов:

- создание сайта;
- создание одной или более подсетей и ассоциирование их с сайтом;
- ассоциирование контроллера домена с сайтом;
- связь сайта с другими сайтами с использованием связей сайта и, если необходимо, создание мостов связей.

Все эти задачи будут рассмотрены далее.

Создание сайтов

Любой администратор, являющийся членом группы **Администраторы домена** или **Администраторы предприятия**, может создавать сайты. Создать сайт можно с помощью следующих действий:

1. В оснастке **Active Directory — сайты и службы** щелкните правой кнопкой мыши на контейнере **Sites** в корне консоли, а затем выберите команду **Создать сайт** (New Site).
2. В окне **Новый объект — Сайт** (New Object — Site), показанном на рис. 7.10, введите имя сайта, например Chicago-First-Site. Имена сайтов не должны содержать пробелы и другие специальные символы, кроме дефиса.

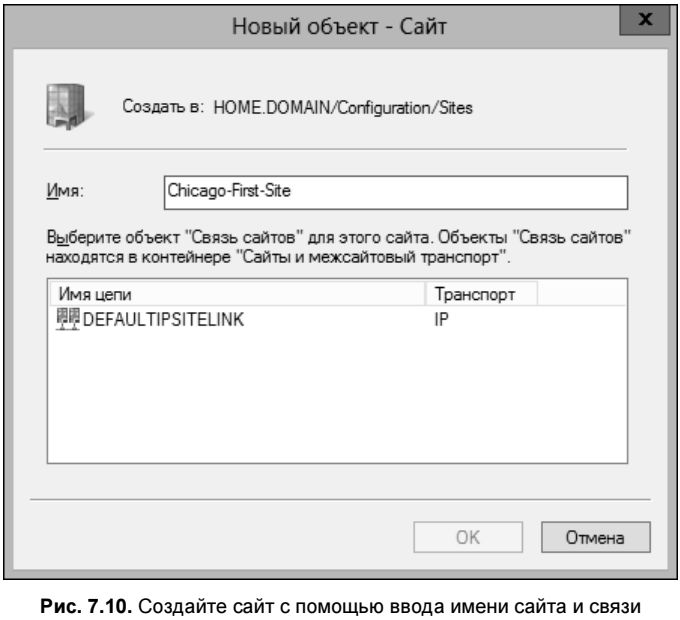


Рис. 7.10. Создайте сайт с помощью ввода имени сайта и связи

3. Щелкните на связи сайта, которая будет использоваться, чтобы соединить этот сайт с другими сайтами. Если связь сайта, с которой нужно работать, не существует, выберите связь сайта по умолчанию, а позже можно будет изменить настройки связи сайта.
4. Нажмите кнопку **OK**. Будет отображена подсказка с описанием действий, которые нужно выполнить для завершения конфигурации сайта. Нажмите кнопку **OK** снова.
5. Для завершения настройки сайта необходимо завершить оставшиеся задачи конфигурации.

Совет

Можно переименовать сайт в любое время. Для этого в оснастке **Active Directory — сайты и службы** щелкните правой кнопкой мыши на сайте и выберите команду **Переименовать**. Введите новое имя сайта и нажмите клавишу <Enter>.

Создание подсетей

Каждый определенный вами сайт должен быть связан с подсетью, описывающей сегменты сети, принадлежащие сайту. Любой компьютер с IP-адресом, принадлежащим к сегменту сети, который связан с сайтом, находится в этом сайте. Хотя с одним сайтом может быть связано несколько подсетей, подсеть может быть связана только с одним сайтом.

Для создания подсети и ее связи с сайтом выполните следующие действия:

1. В оснастке **Active Directory — сайты и службы** щелкните правой кнопкой мыши на контейнере **Subnets** в консоли дерева и выберите команду **Создать подсеть** (New Subnet). Появится окно **Новый объект — Подсеть** (New Object — Subnet), показанное на рис. 7.11.

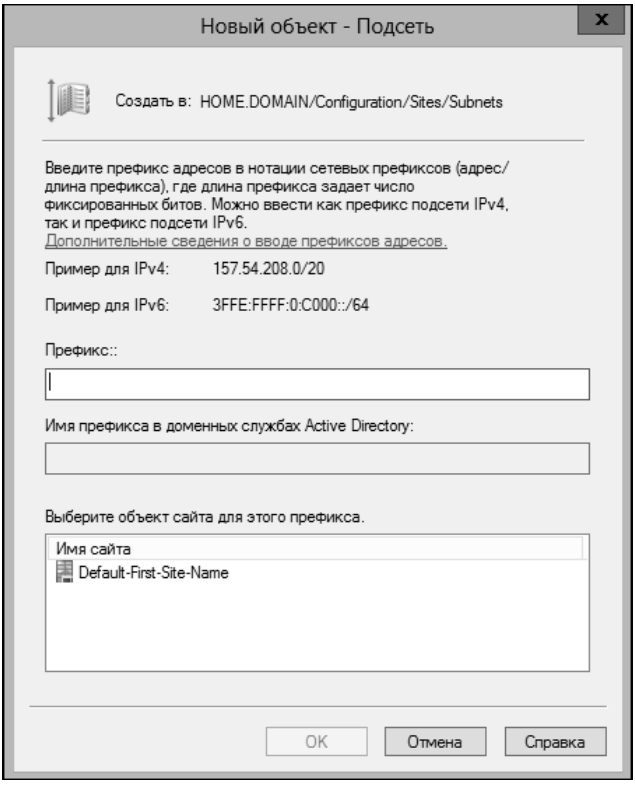


Рис. 7.11. Создайте подсеть путем ввода префикса сети и выбора соответствующего сайта

2. В поле **Префикс** (Prefix) введите IPv4/IPv6-адрес сети с использованием нотации сетевого префикса. В этой нотации введите ID сети и прямой слеш, а потом укажите, сколько битов будет использоваться для ID сети. Например, если IP сети равен 192.168.27.0 и

первые 24 бита определяют ID сети, нужно ввести 192.168.27.0/24 в качестве нотации префикса сети.

3. Выберите сайт, с которым необходимо связать сеть, а затем нажмите кнопку **OK**.

> ***Совет***
> Можно изменить связанный сайт в любое время. В оснастке **Active Directory — сайты и службы** дважды щелкните на подсети в папке **Subnets** и затем на вкладке **Общие** выберите другой сайт из списка **Сайт** (Site).

Связь контроллеров домена с сайтом

У каждого сайта должен быть как минимум один контроллер домена, связанный с ним. Добавляя второй контроллер домена в сайт, администратор обеспечивает отказоустойчивость и избыточность. Если, по крайней мере, один контроллер домена в сайте — также сервер глобального каталога, можно убедиться, что трафик поиска в каталоге и трафик аутентификации изолированы в сайте.

Можно добавить контроллер домена в сайты автоматически или вручную. При связывании подсети с сайтом любой новый контроллер домена, который будет установлен в сайте, автоматически будет помещен в сайт, если IP-адрес контроллера домена находится в допустимом для подсети диапазоне IP-адресов. Существующие контроллеры домена автоматически не могут быть связаны с сайтами. Нужно связать их с сайтом вручную путем помещения объекта контроллера домена в сайт.

Перед перемещением контроллера домена из одного сайта в другой нужно определить, в каком сайте находится контроллер домена в данный момент. Самый простой способ сделать это — ввести следующую команду в командной строке:

```
dsquery server -s DomainControllerName | dsget server -site
```

Здесь *DomainControllerName* — полное доменное имя контроллера домена, например:

```
dsquery server -s server241.cpandl.com | dsget server -site
```

Вывод этой команды — это имя сайта, в котором находится интересующий вас контроллер домена.

Для перемещения контроллера домена из одного сайта в другой выполните эти действия:

1. В оснастке **Active Directory — сайты и службы** любой контроллер домена, связанный с сайтом, отображен в узле **Servers** сайта. Выберите сайт, с которым в данный момент связан контроллер домена.
2. Щелкните правой кнопкой мыши по контроллеру домена и выберите команду **Переместить**. В окне **Переместить** (Move Server) выберите сайт, который должен содержать сервер, и нажмите кнопку **OK**.

> ***Примечание***
> Не перемещайте контроллер домена, если он находится в подсети, не связанной с сайтом. После изменения ассоциации подсети и сайта нужно переместить контроллеры домена в затронутых подсетях в надлежащие контейнеры сайта.

Настройка связей сайта

Сайты — это группы IP-подсетей, которые соединены надежными линиями с высокой скоростью передачи информации. Обычно все подсети одной локальной сети — часть одного и

того же сайта. Сети с несколькими сайтами соединяются связями сайта. Связи сайта — это логические соединения между двумя и больше сайтами. У каждой связи сайта есть расписание репликации, интервал репликации, стоимость связи и транспорт репликации.

Поскольку связи сайта используются по ссылкам глобальной сети, доступность пропускной способности очень важна. По умолчанию связи сайта настроены на репликацию данных 24 часа в день, 7 дней в неделю с интервалом в 180 минут. Если пропускная способность ограничена, необходимо изменить расписание, чтобы предоставить приоритет пользовательскому трафику в часы пик.

Когда есть несколько связей между сайтами, нужно рассмотреть относительный приоритет каждой связи. Можно назначить приоритет на основании доступности и надежности соединения. По умолчанию стоимость связи устанавливается в 100. Если к сайту есть несколько маршрутов, сначала используется "самый дешевый" маршрут (с самой низкой стоимостью). Поэтому пути с наиболее широкой пропускной способностью между сайтами должны быть настроены как "самые дешевые".

Можно настроить связи сайта с использованием протоколов RPC over IP или Simple Mail Transfer Protocol (SMTP) в качестве транспортных протоколов. В случае с IP в качестве транспортного протокола, контроллер домена устанавливает соединение RPC over IP с одним партнером репликации за один раз и синхронно тиражирует изменения Active Directory. Поскольку RPC over IP — синхронный протокол, оба партнера репликации должны быть доступны на время установки соединения. Необходимо использовать RPC over IP, если есть надежные, выделенные соединения между сайтами.

При использовании SMTP в качестве транспортного протокола, контроллеры домена конвертируют весь трафик репликации в сообщения электронной почты, которые отправляются между сайтами асинхронно. Поскольку репликация SMTP асинхронна, оба партнера репликации не должны быть доступны на момент установки соединения, а транзакции репликации будут сохранены, пока целевой сервер недоступен. Используйте SMTP, если связи ненадежны или не всегда доступны.

> ***Примечание***
>
> Если планируется использование SMTP, нужно настроить центр сертификации (certificate authority, CA). Сертификаты из центра сертификации используются для цифровой подписи и шифрования SMTP-сообщений, передаваемых между сайтами. В случае с IP, центр сертификации по умолчанию не требуется.

Можно создать связь между двумя или больше сайтами так:

1. В оснастке **Active Directory — сайты и службы** разверните контейнер **Sites**, а затем — контейнер **Inter-Site Transports**.
2. Щелкните по контейнеру транспортного протокола, который планируется использовать (IP или SMTP), а затем выберите команду **Создать связь с сайтом** (New Site Link).
3. В окне **Новый объект — Связь сайтов** (New Object — Site Link) введите имя связи сайта (рис. 7.12), например ChicagoSeattleLink. Имя связи не может содержать пробелы или специальные символы, кроме дефиса.
4. В списке **Сайты не в этой связи сайтов** (Sites Not In This Site Link) выберите первый сайт, который должен быть включен в связь, и нажмите кнопку **Добавить** (Add) для добавления сайта в список **Сайты в этой связи сайтов** (Sites In This Site Link). Повторите этот процесс для каждого сайта, который нужно добавить в связь. В связи должно быть как минимум два сайта. Нажмите кнопку **OK**.

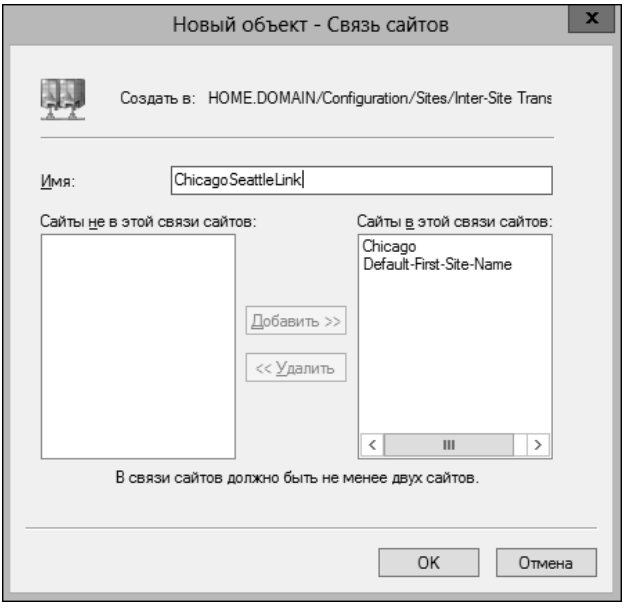


Рис. 7.12. Создайте связь сайтов путем ввода имени связи и выбора сайтов

После создания связи нужно настроить ее свойства. Это позволит указать стоимость связи, расписание репликации и интервал репликации. Для настройки свойств связи выполните следующие действия:

1. В оснастке **Active Directory — сайты и службы** щелкните правой кнопкой мыши по связи сайта и выберите команду **Свойства**.
2. В окне **Свойства** вкладка **Общие** (General) будет открыта по умолчанию. В поле **Стоимость** (Cost) введите относительную стоимость соединения. По умолчанию стоимость равна 100.
3. Поле **Реплицировать каждые** (Replicate Every) позволяет установить интервал репликации. По умолчанию интервал равен 180 минутам.
4. Расписание по умолчанию — 24 часа в день, 7 дней в неделю. Для установки другого расписания нажмите кнопку **Изменить расписание** (Change Schedule) и установите новое расписание в окне **Расписание для** (Schedule For). Нажмите кнопку **OK**.

Можно изменить связи сайта в любое время с помощью следующих действий:

1. В оснастке **Active Directory — сайты и службы** щелкните правой кнопкой мыши по связи сайта и выберите команду **Свойства**.
2. В окне **Свойства** вкладка **Общие** будет открыта по умолчанию. В списке **Сайты не в этой связи сайтов** выберите первый сайт, который нужно включить в ссылку, а затем нажмите кнопку **Добавить** для добавления сайта в список **Сайты в этой связи сайтов**. Повторите этот процесс для каждого сайта, который нужно добавить в связь.
3. В списке **Сайты в этой связи сайтов** выберите сайт, который нужно исключить из связи, а затем нажмите кнопку **Удалить** (Remove) для переноса сайта в список **Сайты не в этой связи сайтов**. Повторите этот процесс для каждого сайта, который нужно удалить из связи. Нажмите кнопку **OK**.

Создание мостов связей сайта

Все связи сайта по умолчанию транзитивные. Это означает, что когда больше двух сайтов связаны для репликации и используют один и тот же тип транспорта, все связи сайта автоматически соединены мостом, позволяя связям быть транзитивными (переходными) между сайтами. Из-за транзитивности любые два контроллера домена могут соединиться по любой последовательности связей. Например, контроллер домена сайта *A* может соединиться с контроллером домена сайта *C* через сайт *B*.

Путь связей, который контроллеры домена выбирают для соединения через сайты, в основном определяется конечной стоимостью моста связи сайта. Стоимость моста связи сайта — сумма всех связей, включенных в мост. Обычно используется путь с самой низкой стоимостью.

Зная стоимость связей и мостов связей, можно вычислить эффект сбоя связи и определить пути, которые будут использоваться, если соединение будет потеряно. Например, контроллер домена в сайте *A* обычно соединяется с контроллером домена в сайте *C* через сайт *B*. Однако, если соединение к сайту *B* будет потеряно, два контроллера домена для установки соединения должны выбрать альтернативный путь (если он доступен), например, проходящий через сайты *D* и *E*.

Топология межсайтовой репликации оптимизирована максимум для трех прыжков (по умолчанию). В больших конфигурациях такие параметры могут привести к непредсказуемым последствиям, например, когда один и тот же трафик репликации будет проходить через одну связь несколько раз. В этом случае нужно отключить автоматическое образование моста связи сайта и вручную настроить мосты связи. В противном случае обычно не требуется отключение автоматического создания моста связи сайта.

В пределах леса Active Directory можно включить или отключить транзитивность связи сайта отдельно для каждого транспортного протокола. Это означает, что все связи сайта, которые используют определенный транспортный протокол, могут либо использовать транзитивность, либо не использовать. Можно настроить транзитивность для транспортного протокола с помощью следующих действий:

1. В оснастке **Active Directory — сайты и службы** разверните контейнер **Sites**, а затем — контейнер **Inter-Site Transports**.
2. Щелкните по контейнеру транспортного протокола, который нужно использовать (IP или SMTP), а затем выберите команду **Свойства**.
3. Для включения транзитивности связи сайта выберите опцию **Установить мост для всех связей сайтов** (Bridge All Site Links) и нажмите кнопку **OK**. Когда транзитивность связи сайта будет включена, будут проигнорированы любые мосты связи сайта, которые были созданы для определенного транспортного протокола.
4. Для отключения транзитивности связи сайта сбросьте флажок **Установить мост для всех связей сайтов** и нажмите кнопку **OK**. Когда транзитивность связи сайта выключена, нужно настроить мосты связей сайтов вручную для определенного протокола.

Как только транзитивные связи отключены, можно вручную создать мосты связей сайтов между двумя или больше сайтами так:

1. В оснастке **Active Directory — сайты и службы** разверните контейнер **Sites**, а затем — контейнер **Inter-Site Transports**.
2. Щелкните по контейнеру транспортного протокола правой кнопкой мыши, который планируете использовать (IP или SMTP), а затем выберите команду **Создать мост связей сайтов** (New Site Link Bridge).

3. В окне **Новый объект — Мост связей сайтов** (New Object — Site Link Bridge) введите имя моста связей сайтов. Имя не должно содержать пробелов и других специальных символов, кроме дефиса.
4. В списке **Связи сайтов, не входящие в данный мост** (Site Links Not In This Site Link Bridge) выберите связь, которая должна быть включена в мост, и нажмите кнопку **Добавить** для добавления связи в список **Связи сайтов, входящие в данный мост** (Site Links In This Site Link Bridge). Повторите этот процесс для каждой связи сайта, которую нужно добавить в мост. Мост должен содержать как минимум две связи сайтов. Нажмите кнопку **OK**.

Изменить связи, входящие в состав моста, можно в любое время так:

1. В оснастке **Active Directory — сайты и службы** щелкните правой кнопкой мыши на контейнере моста и выберите команду **Свойства**.
2. В окне **Свойства** по умолчанию будет открыта вкладка **Общие**. В списке **Связи сайтов, не входящие в данный мост** выберите связь, которая должна быть включена в мост, и нажмите кнопку **Добавить** для добавления связи в список **Связи сайтов, входящие в данный мост**. Повторите этот процесс для каждой связи сайта, которую нужно добавить в мост.
3. Из списка **Связи сайтов, входящие в данный мост** выберите связи, которые нужно исключить из моста, и нажмите кнопку **Удалить** (Remove) для перемещения связей в список **Связи сайтов, не входящие в данный мост**. Повторите этот процесс для каждой связи сайта, которую нужно удалить из моста. Нажмите кнопку **OK**.

Обслуживание Active Directory

Чтобы убедиться в правильной работе Active Directory, нужно периодически производить мониторинг и обслуживание. В этом помогут несколько утилит, которые мы рассмотрим в данном разделе.

Использование утилиты *Редактирование ADSI*

Для решения проблем с Active Directory применяется утилита администрирования **Редактирование ADSI** (ADSI Edit). Ее можно использовать для управления определениями классов объектов и их атрибутами в схеме, а также для работы с другими контекстами именования, включая контекст именования по умолчанию, контекст именования **Конфигурация** (Configuration) и контекст именования RootDSE. Если нужно создать пользовательский набор атрибутов для пользователей и групп, используйте утилиту **Редактирование ADSI**, которую можно запустить одноименной командой из меню **Средства** в диспетчере серверов.

Использовать оснастку **Редактирование ADSI** (ADSI Edit) для подключения к контексту имен можно так:

1. Щелкните правой кнопкой мыши на узле **Редактирование ADSI** в дереве консоли и выберите команду **Подключение к** (Connect To). Будет отображено окно **Параметры подключения** (Connection Settings), показанное на рис. 7.13.
2. В окне **Параметры подключения** по умолчанию установлен переключатель **Выберите известный контекст именования** (Select A Well Known Naming Context). Выберите контекст именования, с которым нужно работать.

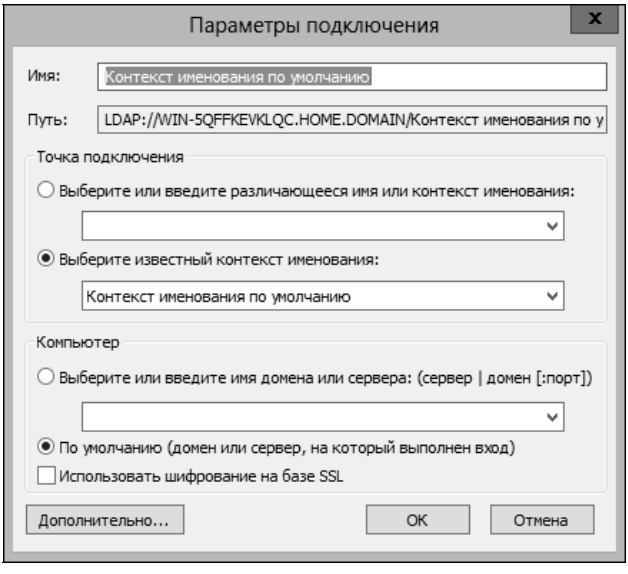


Рис. 7.13. Подключитесь к контексту именования

3. Когда нажмете кнопку **OK**, будет установлено подключение к любому доступному контроллеру домена в вашем домене. Для подключения к другому домену или серверу установите переключатель **Выберите или введите имя домена или сервера** (Select Or Type A Domain Or Server) и затем выберите или введите сервер или домен, с которым нужно работать, дополнительно можно ввести номер порта для соединения, например FileServer252.cpandl.com:389. Порт 389 — это порт LDAP по умолчанию.

После того как выбраны контекст именования, домен и сервер, можно работать с контекстом именования. При подключении к разным контекстам именования есть различные узлы

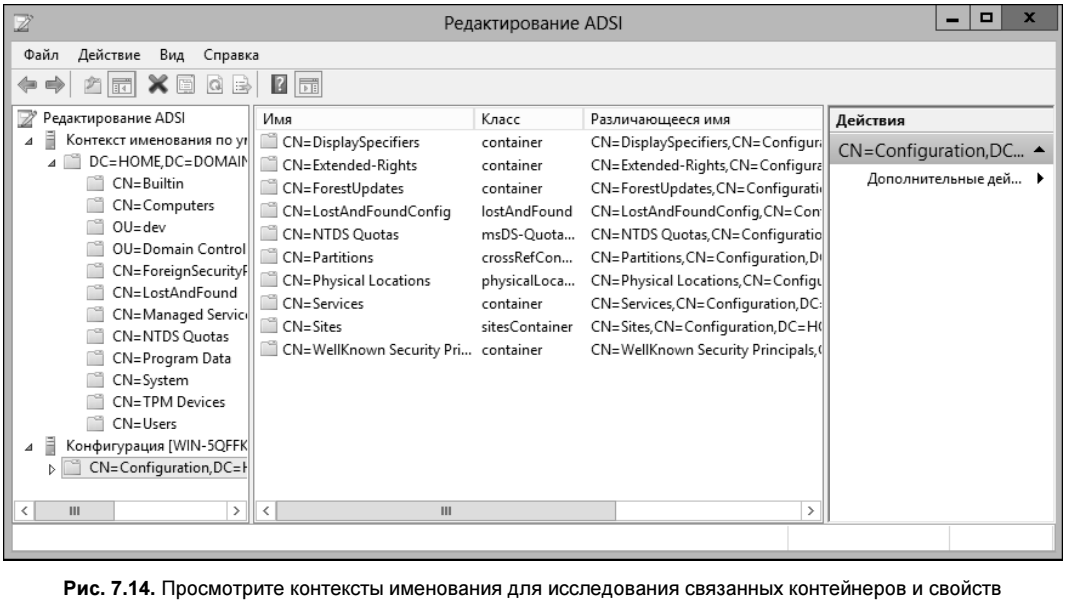


Рис. 7.14. Просмотрите контексты именования для исследования связанных контейнеров и свойств

для управления каждым контекстом отдельно (рис. 7.14). Для решения проблем можно подключиться к одному и тому же контексту именования на разных серверах в одном домене. Сравнивая значения, связанные со свойствами на одном сервере, с аналогичными значениями на другом сервере, можно идентифицировать проблему репликации.

Исследование межсайтовой топологии

Генератор межсайтовой топологии (Inter-Site Topology Generator, ISTG) — это сайт, ответственный за генерацию межсайтовой топологии репликации. Когда вычисляется топология репликации, ISTG может использовать значительную вычислительную мощность, особенно когда размер сети растет. Именно поэтому нужно контролировать генератор межсайтовой топологии в каждом сайте, чтобы убедиться, что они не перегружены.

Чтобы определить, какой контроллер домена является генератором межсайтовой топологии, выполните следующие действия:

1. В оснастке **Active Directory — сайты и службы** разверните контейнер **Sites**, а затем — узел сайта, в котором нужно найти генератор межсайтовой топологии.
2. Дважды щелкните на имени **NTDS Site Settings**. В окне **Свойства: NTDS Site Settings** (NTDS Site Settings) текущий генератор приведен в панели **Автоматическое формирование топологии между сайтами** (Inter-Site Topology Generator).

Репликация между сайтами обычно производится *серверами-плацдармами* (bridgehead server). Сервер-плацдарм — это контроллер домена, назначенный генератором межсайтовой топологии для осуществления межсайтовой репликации. ISTG конфигурирует сервер для каждого раздела Active Directory, который нуждается в репликации и обслуживает отдельную топологию репликации для раздела каждого типа. Хотя единственный сервер-плацдарм может отвечать за репликацию нескольких разделов каталогов, топология репликации для каждого раздела обслуживается отдельно.

У контроллеров домена, которые действуют как серверы-плацдармы, есть дополнительная рабочая нагрузка, увеличивающаяся с числом и частотой репликаций. Нужно периодически наблюдать за сервером-плацдармом и убедиться, что он не перегружен. Можно вывести серверы-плацдармы сайта с помощью следующей команды, введенной в командной строке:

```
repadmin /bridgeheads site:SiteName
```

Здесь *SiteName* — это имя сайта, например:

```
repadmin /bridgeheads site:SacramentoSite
```

Если текущие серверы-плацдармы перегружены или есть контроллеры домена, которые нужно сделать серверами-плацдармами, можно назначить эти серверы серверами-плацдармами. После назначения сервера-плацдарма для сайта генератор межсайтовой топологии будет использовать его для межсайтовой репликации. Если предпочитаемый сервер-плацдарм станет недоступным или будет не в состоянии провести репликацию по одной из причин, межсайтовая репликация будет приостановлена, пока сервер снова не станет доступным или не будет назначен другой предпочитаемый сервер-плацдарм.

При назначении предпочитаемых плацдармов всегда нужно настроить несколько серверов-плацдармов в каждом сайте. Тогда генератор межсайтовой топологии сможет выбрать один из предпочитаемых серверов. Если один из серверов будет недоступным, генератор выберет другой сервер из списка предпочитаемых.

Необходимо настроить сервер-плацдарм для каждого раздела, который нуждается в репликации. Это означает, что нужно настроить как минимум один контроллер домена с копией

каждого раздела каталога в качестве сервера-плацдарма. Если не сделаете это, произойдет сбой репликации раздела и генератор межсайтовой топологии запишет событие в журнал событий Directory Services об этом сбое.

Можно настроить контроллер домена в качестве сервера-плацдарма с помощью следующих действий:

1. В оснастке **Active Directory — сайты и службы** контроллеры домена, ассоциируемые с сайтом, выводятся в узле **Servers**. Щелкните правой кнопкой мыши на сервере, который нужно назначить предпочитаемым плацдармом, и выберите команду **Свойства**.
2. В окне **Свойства** выберите межсайтовый транспортный протокол, для которого сервер должен быть предпочитаемым плацдармом, в списке **Транспорты для передачи данных между сайтами** (Transports Available For Inter-Site Data Transfer) и нажмите кнопку **Добавить**. Повторите этот процесс для IP и SMTP в случае необходимости. Затем нажмите кнопку **OK**.

При назначении серверов-плацдармов можно восстановить систему после сбоя репликации несколькими способами. Можно удалить отказавшие серверы из списка предпочитаемых серверов-плацдармов, а затем указать другие предпочитаемые серверы, или можно удалить все предпочитаемые серверы и затем разрешить генератору межсайтовой топологии выбрать подходящий плацдарм автоматически. Чтобы удалить сервер из списка предпочитаемых плацдармов для выбранного транспортного протокола, выполните следующие действия:

1. В оснастке **Active Directory — сайты и службы** контроллеры домена, ассоциируемые с сайтом, выводятся в узле **Servers**. Щелкните правой кнопкой мыши на сервере, который больше не должен быть предпочитаемым плацдармом, и выберите команду **Свойства**.
2. Выберите транспортный протокол в списке **Это — основной сервер-плацдарм для следующих транспортов** (This Server Is A Preferred Bridgehead Server For The Following Transports) и нажмите кнопку **Удалить** (Remove). Нажмите кнопку **OK**.

Решение проблем с Active Directory

Администратору приходится выполнять рутинное обслуживание, в том числе наблюдать за доменными контроллерами, серверами глобальных каталогов, серверами-плацдармами и связями сайта. Если есть подозрение проблемы с Active Directory, нужно обратить внимание на репликацию — в большинстве случаев это начальная точка для диагностики. Настроив мониторинг репликации внутри сайта и между сайтами, можно диагностировать и решать множество проблем репликации. Помните, что репликация Active Directory зависит от нескольких служб, в том числе LDAP, DNS (Domain Name System), аутентификации Kerberos v5 и RPC (Remote Procedure Call).

Все эти важные службы должны правильно функционировать, чтобы разрешить репликацию обновлений каталога. Во время репликации Active Directory задействует различные TCP- и UDP-порты между контроллерами домена. По умолчанию используются следующие порты:

- LDAP использует TCP/UDP-порт 389 для стандартного трафика и TCP-порт 686 для безопасного трафика;
- глобальные каталоги используют TCP-порт 3268, Kerberos v5 — TCP/UDP-порты 88;
- DNS использует TCP/UDP-порты 53;
- SMB over IP использует TCP/UDP-порты 445.

Дополнительно для репликации файлов в общих папках SYSVOL (System Volume) на контроллерах доменов, Active Directory использует службы репликации файлов (File Replication Service, FRS) или репликации DFS (DFS Replication Service). Соответствующая служба репликации должна быть запущена и настроена для репликации SYSVOL.

Active Directory отслеживает изменения, используя номера последовательности обновления (USN, update sequence numbers). Каждый раз, когда происходит изменение каталога, контроллер домена обрабатывает изменение, присваивая ему USN. Каждый контроллер домена обслуживает свои локальные USN и увеличивает значение каждый раз, как происходит изменение. Контроллер домена также присваивает локальный USN измененному атрибуту объекта. У каждого объекта есть относительный атрибут uSNChanged, хранящийся вместе с объектом и идентифицирующий наивысший USN, который был назначен любому атрибуту объекта.

Каждый контроллер домена отслеживает свои локальные USN, а также локальные USN других контроллеров домена. Во время репликации контроллеры домена сравнивают полученные значения USN с теми, что сохранены. Если текущее значение USN для определенного контроллера домена выше, чем сохраненное значение, нужно реплицировать изменения, связанные с более высокоуровневым контроллером домена. Если текущее значение для определенного контроллера домена такое же, как и сохраненное значение, изменения от другого контроллера домена не будут реплицированы.

Можно контролировать репликацию из командной строки с помощью утилиты Repadmin. Большинство параметров командной строки данной утилиты — это список контроллеров домена, он называется DCList. Можно определить значения DCList следующим образом:

- `*` — звездочка означает, что будут включены все контроллеры домена в организации;
- *`PartialName`* — часть имени сервера, сопровождаемая символом подстановки `*` (замещает остаток имени сервера);
- `Site:`*`SiteName`* — имя сайта, контроллеры домена которого нужно включить;
- `Gc` — включает все серверы глобального каталога в организации.

Хотя у Repadmin много параметров и можно использовать их по-разному, есть определенные задачи, которые приходится выполнять чаще, чем другие. В табл. 7.2 приведены некоторые такие задачи.

Таблица 7.2. *Общие задачи и команды репликации*

Задача	Команда
Принудительный запуск проверки целостности знаний (Knowledge Consistency Checker, KCC) для пересчета топологии репликации внутри сайта для определенного контроллера домена	`repadmin /kcc DCList [/async]`
Вывод серверов-плацдармов, соответствующих списку DCList	`repadmin /bridgeheads [DCList] [/verbose]`
Вывод списка записей в кэше привязки DS — это исходящие вызовы	`repadmin /showoutcalls [DCList]`
Вывод списка доменов, которые имеют доверие указанного домена	`repadmin /showtrust [DCList]`
Вывод списка сбоев репликации, обнаруженных KCC	`repadmin /failcache [DCList]`

Таблица 7.2 *(окончание)*

Задача	Команда
Отображение объектов подключения для указанного контроллера домена. По умолчанию для локального сайта	`repadmin /showconn [DCList]`
Вывод списка компьютеров, на которых открыты сеансы с определенным контроллером домена	`repadmin /showctx [DCList]`
Вывод имени генератора межсайтовой топологии для определенного сайта	`repadmin istg [DCList] [/verbose]`
Вывод партнеров репликации для каждого раздела каталога на указанном контроллере домена	`repadmin /showrepl [DCList]`
Вывод состояния репликации	`repadmin /replsummary [DCList]`
Вывод сертификатов сервера, загруженных на указанном контроллере домена	`repadmin /showcert [DCList]`
Отображение задач, ожидающих в очереди репликации	`repadmin /queue [DCList]`
Отображение времени между репликациями внутри сайта с использованием временной метки повторной отправки пакетов генератора межсайтовой топологии	`repadmin /latency [DCList] [/verbose]`

ГЛАВА 8

Создание учетных записей пользователя и группы

Управление учетными записями — одна из основных задач администратора Microsoft Windows. В *главе 7* обсуждались учетные записи компьютера. В этой главе будут рассмотрены учетные записи пользователя и группы. С помощью учетных записей пользователя можно разрешить отдельным пользователям входить в сеть и получать доступ к сетевым ресурсам. Посредством учетных записей группы можно управлять ресурсами сразу для множества пользователей. Разрешения и привилегии, назначаемые учетным записям пользователя и группы, определяют, какие действия пользователи могут выполнить и к каким системам и ресурсам они смогут получить доступ.

Несмотря на желание предоставить пользователям широкий доступ, нужно балансировать между потребностью пользователя в необходимых ему для работы ресурсах и потребностью защитить критичные ресурсы или секретную информацию. Например, нельзя, чтобы у всех на предприятии был доступ к платежной ведомости. Следовательно, необходимо убедиться, что доступ есть только у тех, кто нуждается в этой информации.

В этой главе будет показано, как управлять учетными записями домена. Несмотря на то, что также будут обсуждаться локальные системные учетные записи, основное внимание будет удалено не им. Для более подробной информации о локальных системных учетных записях *см. главу 7* книги "Microsoft® Windows 8. Справочник администратора"[1]. Помните, что в Windows 8 появился специальный тип локальной учетной записи — **Учетная запись Майкрософт**. Записи этого типа могут считаться синхронизируемыми локальными учетными записями. Несмотря на то, что в доменах нельзя использовать учетные записи Майкрософт, пользователи могут получать доступ к Магазину Windows посредством сохраненных учетных данных Windows, а также использовать приложения. Автор этой книги использует термин "приложения" для разграничения понятий "настольные приложения" и "настольные программы". Чтобы узнать, как управлять приложениями и получить доступ к Магазину Windows, *см. главу 8* книги "Microsoft® Windows 8. Справочник администратора".

Модель безопасности Windows Server

Доступ к сетевым ресурсам контролируется компонентами модели безопасности Windows Server. Администратору следует разбираться в ключевых компонентах, которые используются для аутентификации и управления доступом.

---

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

Протоколы аутентификации

Аутентификация Windows Server состоит из двух частей — интерактивная аутентификация, когда пользователь входит в систему, и сетевая аутентификация. Когда пользователь входит в компьютер, используя учетную запись домена, интерактивный процесс входа проверяет учетные данные пользователя, подтверждает идентификацию пользователя по отношению к локальному компьютеру и предоставляет доступ к доменным службам Active Directory (AD DS). Позже, каждый раз, когда пользователь будет попытаться получить доступ к ресурсам сети, будет применяться сетевая аутентификация для определения, есть ли у пользователя необходимые разрешения.

Операционная система Windows Server 2012 поддерживает много сетевых протоколов аутентификации. Active Directory использует Kerberos v5 в качестве протокола аутентификации по умолчанию. Аутентификация NTLM сохраняется только для обратной совместимости. С помощью параметра **Сетевая безопасность: уровень проверки подлинности LAN Manager**[1] (Network Security: LAN Manager Authentication Level) групповой политики можно задать, как используется NTLM. В большинстве случаев по умолчанию используется уровень аутентификации **Отправлять только NTLMv2 ответ** (Send NTLMv2 Response Only), что позволяет клиентам использовать протокол NTLMv2 для аутентификации и сеанса безопасности, если сервер поддерживает его. Active Directory может также использовать для аутентификации сертификаты клиентов.

Ключевая функция модели аутентификации Windows Server — технология единого входа, которая работает так:

1. Пользователь входит в домен с помощью имени пользователя и пароля или же путем вставки смарт-карты в кардридер.
2. Интерактивный процесс входа аутентифицирует доступ пользователя. При использовании локальной учетной записи учетные данные аутентифицируются локально, а пользователь получает доступ к локальному компьютеру. При использовании учетной записи домена учетные данные аутентифицируются в Active Directory, а пользователь получает доступ к локальным и сетевым ресурсам.
3. Теперь пользователь может аутентифицироваться на любом компьютере в домене с помощью сетевого процесса аутентификации.

При использовании учетных записей домена процесс сетевой аутентификации обычно автоматический (с поддержкой единого входа). При использовании локальных учетных записей пользователи должны предоставить имя пользователя и пароль при каждом обращении к сетевому ресурсу.

ОС Windows Server содержит **Службы федерации Active Directory** (Active Directory Federation Services, AD FS), расширяющие единый вход до доверяемых ресурсов в Интернете. Используя AD FS, организации могут расширить существующую инфраструктуру Active Directory для предоставления доступа к доверяемым интернет-ресурсам, которые могут быть либо третьими сторонами, либо географически удаленными подразделениями организации. После того как федеративные серверы будут настроены, пользователи в организации могут войти всего один раз в сеть организации, а затем автоматически использовать доверяемые веб-приложения, размещенные партнерами в Интернете. Единый федеративный вход в веб-приложения использует федеративную авторизацию для прямого доступа. В до-

---

[1] Этот параметр находится в узле **Конфигурация компьютера\Политики\Конфигурация Windows\ Параметры безопасности\Локальные политики\Параметры безопасности** (Computer Configuration\ Policies\Windows Settings\Security Settings\Local Policies\Security Options). — *Прим. пер.*

полнение к идентификации пользователя и информации учетной записи, в федеративной авторизации используются маркеры (токены) безопасности, что делает возможным идентификацию на основе заявок.

Контроль доступа

Active Directory объектно-ориентирован. Пользователи, компьютеры, группы, общие ресурсы и множество других сущностей определены как объекты. Контроль доступа к этим объектам осуществляется с помощью дескрипторов безопасности, которые:

- выводят список пользователей и групп, которым предоставлен доступ к объектам;
- определяют разрешения, присвоенные пользователям и группам;
- отслеживают события аудита объектов;
- определяют владельцев объектов.

Отдельные записи в дескрипторе безопасности ссылаются на записи управления доступом (Access Control Entries, ACE). Объекты Active Directory могут наследовать записи управления доступом от своих родительских объектов. Это означает, что полномочия родительского объекта могут быть применены к дочернему объекту. Например, все элементы группы **Администраторы домена** наследуют полномочия, предоставленные этой группе.

При работе с записями управления доступом помните следующее:

- наследование для ACE включено по умолчанию;
- наследование вступает в силу сразу после создания и сохранения ACE;
- все записи управления доступом содержат информацию, определяющую, разрешено ли наследование или запись присвоена только к определенному объекту.

Технология идентификации на основе требований

К стандартным средствам управления доступом Windows Server 2012 добавляет защиту Kerberos (Kerberos armoring), комплексную проверку подлинности и предоставление доступа на основе требований (утверждений). Защита Kerberos увеличивает безопасность домена, позволяя клиентам и контроллерам домена взаимодействовать по безопасным, зашифрованным каналам. Комплексная проверка подлинности включает также требования пользователя, требования устройства и свойства ресурса.

Контроль доступа на основе требований может быть настроен несколькими способами. Основной подход заключается в определении условий, ограничивающих доступ как часть расширенных прав доступа ресурса. Обычно эти условия добавляют требования устройства или требования пользователя для контроля доступа. Требования пользователя идентифицируют пользователей; требования устройства — устройства. Например, чтобы получить доступ к общему ресурсу Human Resources, можно добавить требование устройства и убедиться, что компьютер, используемый для доступа к ресурсу — член группы **HR Computers**, также можно добавить требование пользователя и убедиться, что пользователь — это член группы **HR Managers**.

Защита Kerberos, комплексная проверка подлинности и управление доступом на основе требований могут также работать вместе как часть новой платформы авторизации, что предоставляет динамический доступ к ресурсам с использованием централизованных политик доступа. Посредством централизованных политик доступа администратор определяет цен-

трализованные правила доступа в Active Directory, и эти правила будут динамически применены на всем предприятии. Централизованные правила доступа используют условные выражения, требующие определения свойств ресурсов, необходимые для политики, типы требований и группы безопасности, необходимые для политики, а также серверы, где политика должна быть применена.

Прежде чем определить и применить правило доступа, нужно определить свойства ресурса и тип требования.

- *Свойства ресурса* создают определения свойств для ресурса. Например, можно добавить свойство Department и Country к файлам так, что появится возможность динамически управлять доступом отдела и страны.
- *Тип требования* создает определение требования для ресурсов. Например, можно создать требование пользователя добавить свойства Department и Country в объекты User так, чтобы появилась возможность динамически управлять доступом отдела и страны.

После задания свойств ресурса и типа требования и определения, где должна применяться политика, можно создать правило доступа и затем добавить его в централизованную политику доступа. Добавление правила в политику сделает ее доступной для динамического управления. Затем нужно применить политику по всем файловым сервером с помощью групповой политики.

Политика на основе требований должна быть включена для политики Default Domain Controllers. Для этого перейдите в узел **Конфигурация компьютера\Политики\Административные шаблоны\Система\Центр распространения ключей** (Administrative Templates policies for Computer Configuration under System\KDC), здесь находится параметр политики **Поддержка KDC требований, комплексной проверки подлинности и защиты Kerberos** (KDC Support For Claims, Compound Authentication And Kerberos Armoring). Политика должна быть настроена на использование определенного режима. Доступны следующие режимы.

- **Поддерживается** (Supported). Контроллеры домена будут поддерживать требования (утверждения), комплексную проверку подлинности и защиту Kerberos. Клиентские компьютеры, не поддерживающие защиту Kerberos, могут быть аутентифицированы.
- **Всегда предоставлять утверждения** (Always Provide Claims). Режим аналогичен предыдущему, но контроллеры домена всегда возвращают требования для учетных записей.
- **Отклонять запросы проверки подлинности без защиты** (Fail Unarmored Authentication Requests). Защита Kerberos обязательна. Клиенты, не поддерживающие Kerberos, не могут быть аутентифицированы.

В разделе **Конфигурация компьютера\Политики\Административные шаблоны\Система\Kerberos** (Computer Configuration\Policies\Administrative Templates\System\Kerberos) находится параметр **Поддержка клиентами Kerberos требований, комплексной проверки подлинности и защиты Kerberos** (Kerberos Client Support For Claims, Compound Authentication And Kerberos Armoring). Этот параметр политики указывает, будет ли клиент, работающий под управлением ОС Windows 8 и Windows Server 2012, запрашивать требования, комплексную проверку подлинности и защиту Kerberos. Политика должна быть включена для Kerberos-совместимых клиентов, чтобы они запрашивали требования и комплексную проверку подлинности для динамического контроля доступа и защиты Kerberos.

Практический совет

Политика на основе требований должна быть включена для всех контроллеров домена в домене, чтобы обеспечить непротиворечивое приложение. В домене должен быть как минимум один контроллер домена под управлением Windows Server 2012, и файловые серве-

ры должны работать тоже под управлением Windows Server 2012. По умолчанию контроллеры домена помещаются в организационное подразделение **Domain Controllers**, а у политики **Default Domain Controllers** — наивысший приоритет среди объектов групповой политики (Group Policy Objects, GPO), соединенных с подразделением **Domain Controllers**. Если организация использует другой подход, нужно убедиться, что объект групповой политики с наивысшим приоритетом для надлежащего подразделения содержит включенную политику на основе требований и настроен должным образом.

Централизованные политики доступа

Централизованные политики доступа не заменяют традиционные средства управления доступом. Они разработаны, чтобы расширить существующие средства управления доступа путем определения очень точных специфических атрибутов пользователей и устройств, которые должны иметь доступ к ресурсам. Самый простой способ управлять централизованными политиками доступа — использовать Центр администрирования Active Directory.

Обзор процесса создания и размещения политики:

1. Откройте Центр администрирования Active Directory. В левой панели по умолчанию выбран вид **Список** (List View). Выберите вид **Дерево** (Tree View) для отображения дерева. Разверните узел **Динамический контроль доступа** (Dynamic Access Control), а затем — **Claim Types** (Claim Types).
2. Используйте узел **Claim Types** для создания и управления требованием. Например, для создания нового требования щелкните правой кнопкой мыши на узле **Claim Types**, выберите команду **Создать | Тип утверждения** (New | Claim Type).
3. Используйте узел **Resource Properties** (Resource Properties) для создания и управления свойствами ресурсов. Например, щелкните правой кнопкой мыши по этому узлу и выберите команду **Создать | Свойство ресурса** (New | Resource Property).

   Примечание

   Свойства ресурса добавляются, как правило, как свойства определения классификации на файловых серверах.

4. Используйте узел **Central Access Rules** (Central Access Rules) для создания и управления централизованными правами доступа. Например, щелкните по узлу **Central Access Rules** правой кнопкой мыши и выберите команду **Создать | Централизованное правило доступа** (New | Central Access Rule) для создания нового правила доступа.
5. Используйте узел **Central Access Policies** (Central Access Policies) для создания и управления централизованными политиками доступа. Например, щелкните на узле **Central Access Policies** правой кнопкой мыши и выберите команду **Создать | Централизованная политика доступа** (New | Central Access Policy).

Для завершения разворачивания нужно отредактировать GPO с высшим приоритетом, связанный с организационным подразделением, в который планируется поместить файловые серверы и включить централизованные политики доступа. Чтобы сделать это, выполните следующие действия:

1. В редакторе **Управление групповой политикой** (Group Policy Management) откройте GPO для редактирования.
2. В разделе **Конфигурация компьютера** (Computer Configuration) перейдите в узел **Конфигурация Windows\Параметры безопасности\Файловая система** (Windows Settings\Security Settings\File System).

3. Щелкните правой кнопкой мыши по узлу **Централизованная политика доступа** (Central Access Policy) и выберите команду **Управление централизованными политиками доступа** (Manage Central Access Policies). Откроется окно **Конфигурация централизованных политик доступа** (Central Access Policies Configuration).
4. В открытом окне доступные политики выводятся в левой панели, а примененные в данный момент политики — в правой панели. Чтобы применить политику, выберите ее в левой панели и нажмите кнопку **Добавить**. Для удаления политики выберите ее в правой панели и нажмите кнопку **Удалить**. Нажмите кнопку **OK**.

Как только изменения групповой политики вступят в силу на серверах, станут доступны динамические средства управления. Ускорить обновление групповой политики можно с помощью команды `gpupdate /force`, введенной в командной строке с правами администратора.

У серверов, к которым нужно применить динамические средства управления, должна быть роль **Файловые службы и службы хранилища** (File And Storage Services) со службами ролей **Службы хранения** (File Server, Storage Services) и **Диспетчер ресурсов файлового сервера** (File Server Resource Manager). Служба роли **Диспетчер ресурсов файлового сервера** и связанные с ней средства нужны, чтобы применить определения свойства классификации папкам.

После включения централизованной политики доступа и каждый раз после обновления определений свойств классификации необходимо подождать Global Resource Properties из Active Directory для обновления файловых серверов. Ускорить этот процесс можно с помощью команды `update-fsrmclassificationpropertydefinition`, которую нужно ввести в приглашении Windows Powershell. Выполните эту команду на каждом файловом сервере, на котором нужно настроить централизованную политику доступа.

Для завершения развертывания центральных политик доступа отредактируйте свойства каждой папки, где будет применяться централизованная политика доступа, и сделайте следующее:

1. Добавьте надлежащие определения классификации на вкладке **Классификация** (Classification) папки. На этой вкладке будут перечислены созданные свойства ресурса. Выберите поочередно свойства и установите их значения.
2. Включите соответствующую политику, используя расширенные параметры безопасности для папки. На вкладке **Безопасность** (Security) нажмите кнопку **Дополнительно** (Advanced) и выберите вкладку **Централизованная политика** (Central Policy). Любая выбранная или примененная политика выводится с описанием, позволяющим просмотреть правила политики. После нажатия кнопки **Изменить** (Change) можно использовать список, предоставляемый для выбора политики для применения или же выбрать опцию **Нет централизованной политики доступа** (No Central Access Policy) для остановки использования политики. Нажмите кнопку **OK**.

Повторите этот процесс для каждой корневой папки или для другой папки, доступ к которой нужно ограничить. Файлы и папки внутри выбранной папки будут наследовать правила доступа автоматически, если будет определено иное. Например, если создается правило доступа с названием "HR Managers in the US" и задаются определения ресурса **Department и Country**, можно отредактировать свойства папки HR, выбрав вкладку **Классификация**, и, используя доступные опции, установить Department в HR, а Country в US. Затем можно применить политику **HR Managers in the US**, используя расширенные настройки безопасности папки.

Различия между учетными записями пользователя и группы

Операционная система Windows Server 2012 предоставляет учетные записи пользователя и группы (членом которых являются пользователи). Учетные записи пользователя предназначены для отдельных пользователей. Учетные записи групп разработаны для упрощения администрирования множества пользователей. Хотя можно войти в систему, используя учетную запись пользователя, нельзя использовать для входа учетную запись группы. Учетные записи группы часто называют просто *группами*.

> ***Практический совет***
>
> ОС Windows Server поддерживает объект InetOrgPerson. По сути, этот объект — то же самое, что и объект пользователя. Однако настоящее предназначение этого объекта — обеспечение совместимости и переход от сторонних служб каталогов X.500 и Lightweight Directory Access Protocol (LDAP), которые используют этот объект для представления пользователей. При миграции со сторонней службы каталогов можно получить много объектов InetOrgPerson. Эти объекты можно использовать в качестве принципалов безопасности точно так же, как учетные записи пользователей. Объект InetOrgPerson доступен только в режиме Windows Server 2003 или более высокой версии. В этом режиме можно установить пароли для объектов InetOrgPerson и изменить класс объекта, если нужно. При изменении класса объекта объект InetOrgPerson конвертируется в объект пользователя (тип User в оснастке **Active Directory — пользователи и компьютеры**).

Учетные записи пользователей

В Windows Server определены два типа учетных записей пользователей.

- Учетные записи пользователей, определенные в Active Directory, называются *учетными записями пользователей домена*. Посредством единого входа в систему учетные записи пользователей домена могут получить доступ ко всем ресурсам домена. Учетные записи пользователей домена создаются в оснастке **Active Directory — пользователи и компьютеры**.
- Учетные записи пользователей, определенные на локальном компьютере, называются *локальными учетными записями пользователей*. Локальные учетные записи пользователей имеют доступ только к локальному компьютеру и должны пройти аутентификацию перед обращением к сетевым ресурсам. Создать локальные учетные записи можно с помощью утилиты **Локальные пользователи и группы** (Local Users And Groups).

> ***Примечание***
>
> В домене только рядовые серверы и рабочие станции имеют локальные учетные записи пользователей и групп. На основном контроллере домена эти учетные записи перемещаются из локальной базы данных SAM (Security Account Manager) в Active Directory и становятся учетными записями домена.

Имена входа, пароли и публичные сертификаты

Все учетные записи пользователей идентифицируются с помощью имени входа. В Windows Server имя входа состоит из двух частей:

- *имя пользователя* — текстовая метка учетной записи;
- *домен пользователя* или *рабочая группа* — рабочая группа или домен, где существует учетная запись пользователя.

Для пользователя wrstanek, чья учетная запись создана в домене cpandl.com, полное имя входа будет wrstanek@cpandl.com. Имя входа в старом формате (в ОС, предшествовавших Windows 2000) — CPANDL\wrstanek.

При работе с Active Directory также нужно указать *полное имя пользователя* — комбинации доменного имени пользователя DNS (Domain Name System), контейнера или организационного подразделения, где находится учетная запись пользователя, и имени пользователя. Для пользователя cpandl.com\users\wrstanek, cpandl.com — это доменное имя DNS, users — контейнер или организационное подразделение, а wrstanek — имя пользователя.

Учетные записи пользователей также имеют пароли и публичные сертификаты, связанные с ними. Пароли — это аутентификационные строки для учетной записи. Публичные сертификаты состоят из публичного и частного ключей для идентификации пользователей. Можно войти интерактивно, используя пароль. Также можно войти, предоставив сертификат на смарт-карте.

Идентификаторы безопасности и учетные записи пользователей

Хотя Windows Server отображает имя пользователя для описания его привилегий и разрешений, ключевыми идентификаторами для учетных записей являются *идентификаторы безопасности* (Security Identifiers, SID). SID — это уникальные идентификаторы, которые генерируются при создании учетных записей. Каждый SID учетной записи состоит из ID безопасности домена и уникального относительного ID (relative ID, RID), который выделен хозяином относительных идентификаторов.

Операционная система Windows Server использует эти идентификаторы для отслеживания учетных записей отдельно от имен пользователей. SID применяется для разных целей. Две самые важные цели: простое изменение имен и безопасное удаление учетных записей (не нужно волноваться, что кто-то получит доступ к ресурсам, воссоздав учетную запись с таким же именем).

При изменении имени пользователя Windows Server связывает определенный SID с новым именем. При удалении учетной записи SID, связанный с ней, больше не является действительным. Позже, даже если кто-то создаст учетную запись с тем же именем пользователя, у новой учетной записи не будет тех же полномочий и разрешений, как у предыдущей. Потому что у новой учетной записи будет новый SID.

Учетные записи групп

В дополнение к учетным записям пользователей Windows Server предоставляет группы. Вообще говоря, группы используются для предоставления полномочий пользователям, выполняющим похожие действия, и упрощения администрирования учетных записей. Если пользователь — участник группы, которая может получить доступ к ресурсу, то и этот определенный пользователь тоже может получить доступ к этому ресурсу. Таким образом, можно предоставить доступ пользователю к различным необходимым ему для выполнения своих обязанностей ресурсам, сделав его членом определенной группы. Обратите внимание, несмотря на то, что можно войти в систему, используя учетную запись пользователя, нельзя войти в систему с помощью учетной записи группы.

Поскольку разные домены Active Directory могут иметь группы с одинаковым названием, группы часто указываются в виде *домен\группа*, например, cpandl\gmarketing для группы Gmarketing в домене cpandl. При работе с Active Directory также нужно указать FQDN для группы. FQDN для группы — это конкатенация DNS-имени, контейнера или организацион-

ного подразделения и имени группы. Для группы cpandl.com\user\gmarketing: cpandl.com — DNS-имя домена, users — название контейнера или организационного подразделения и gmarketing — имя группы.

> ***Практический совет***
>
> Сотрудники отдела маркетинга нуждаются в доступе ко всем ресурсам, относящимся к маркетингу. Вместо предоставления необходимого доступа к этим ресурсам каждому отдельному сотруднику, можно сделать пользователей членами группы маркетинга. В этом случае будут автоматически получены привилегии группы. Позже, если пользователь переходит в другой отдел, нужно просто удалить пользователя из этой группы, и он потеряет все разрешения доступа. По сравнению с закрытием доступа к каждому отдельному ресурсу эта техника довольно проста, и администратор сможет использовать группы везде, где это возможно.

Типы групп

ОС Windows Server поддерживает группы трех типов.

- **Локальные группы** (Local groups) — группы, определенные на локальном компьютере. Они используются только на локальном компьютере и создаются с помощью утилиты **Локальные пользователи и группы** (Local Users And Groups).
- **Группы безопасности** (Security groups) — группы, которые имеют связанные с ними дескрипторы безопасности. Группы безопасности в доменах создаются с помощью оснастки **Active Directory — пользователи и компьютеры**.
- **Группы рассылки** (Distribution group) — группы, которые используются в списках рассылки электронной почты. Они не имеют дескрипторов безопасности, связанных с ними. Создаются оснасткой **Active Directory — пользователи и компьютеры**.

> ***Примечание***
>
> В большинстве случаев речь идет либо о локальных группах, либо о группах безопасности, но не о группах рассылки. Группы рассылки используются только для рассылки e-mail, а не для назначения или управления доступом.

Область действия группы

В Active Directory есть несколько областей (диапазонов) групп — локальный домен, встроенный локальный, глобальный и универсальный. То есть группы можно создавать и использовать в разных областях.

- *Локальные группы домена* — группы в основном используются для назначения разрешений доступа к ресурсам в пределах одного домена. Локальные группы домена могут включать членов из любого домена в лесу и из доверяемых доменов в других лесах. Обычно глобальные и универсальные группы являются членами локальных групп домена.
- *Встроенные локальные группы* — группы со специальной областью группы, имеют разрешения локального домена и часто, для простоты, относятся к *локальным группам домена*. Разница между локальными встроенными группами и другими группами в том, что нельзя создавать или удалять встроенные локальные группы. Можно только модифицировать встроенные локальные группы. Упоминание локальных групп домена относится и к встроенным локальным группам, если явно не указано иное.
- *Глобальные группы* — группы, которые используются преимущественно для определения прав пользователей и компьютеров в одном и том же домене, разделяющих подоб-

ную роль, функцию или работу. Члены глобальных групп — только учетные записи и группы из домена, где они были определены.

- *Универсальные группы* — группы, используемые преимущественно для определения наборов пользователей или компьютеров, которые должны иметь широкие разрешения по всему домену или лесу. Членами универсальных групп могут быть учетные записи пользователей, глобальные группы и другие универсальные группы из любого домена в дереве доменов или лесу.

> ***РЕКОМЕНДАЦИИ***
>
> Универсальные группы очень полезны в больших предприятиях, где есть несколько доменов. При надлежащем планировании можно использовать универсальные группы для упрощения системного администрирования. Не нужно часто изменять состав универсальных групп. При каждом изменении состава универсальной группы нужно реплицировать эти изменения во всех глобальных каталогах в дереве доменов или лесу. Чтобы уменьшить эти изменения и снизить нагрузку на сеть, назначьте другие группы, а не используйте универсальные группы. Для получения дополнительной информации обратитесь к *разд. "Когда использовать локальные группы домена, глобальные и универсальные группы" далее в этой главе*.

Область группы определяет, что можно сделать, а что — нет. В табл. 8.1 приводится подробное описание возможностей групп. Для получения более подробной информации *см. разд. "Добавление учетной записи группы" далее в этой главе.*

Таблица 8.1. *Как область группы влияет на ее возможности*

Возможность	Локальная группа домена	Глобальная группа	Универсальная группа
Члены	Учетные записи пользователей, глобальные и универсальные группы из любого домена; локальные группы домена из того же домена	Учетные записи и глобальные группы из того же домена	Учетные записи из любого домена, глобальные и универсальные группы из любого домена
Может быть членом	Можно поместить в любую локальную группу домена и назначить разрешения только в том домене	Можно поместить в другую группу и назначить разрешения в любом домене	Можно поместить в другие группы и назначить разрешения в любом домене
Преобразование области	Можно конвертировать в универсальный диапазон при условии, что в этой группе нет другой группы, имеющей диапазон локального домена	Можно конвертировать в универсальный диапазон при условии, что эта группа не является членом любой другой группы с глобальным диапазоном	Нельзя конвертировать в любой другой диапазон группы

Идентификаторы безопасности и учетные записи групп

Как и с учетными записями пользователей, ОС Windows Server отслеживает учетные записи группы с помощью уникальных SID. Это означает, что невозможно удалить учетную запись группы, воссоздать ее снова и затем ожидать, что все полномочия останутся теми же. У новой группы будет новый SID, и все полномочия старой группы будут потеряны.

ОС Windows Server создает маркеры безопасности для каждого входа пользователя. Маркеры безопасности определяют ID учетной записи и SID всех групп безопасности, к которым принадлежит пользователь. Размер маркера увеличивается по мере добавления пользователя в дополнительные группы безопасности, и у этого есть последствия:

- маркер безопасности должен быть передан процессу входа пользователя перед завершением входа. Когда число групп безопасности высокое, процесс входа занимает больше времени;
- чтобы определить права доступа, маркер безопасности отправляется на каждый компьютер, к которому пользователь хочет получить доступ. Поэтому у размера маркера безопасности есть прямое влияние на загрузку сети.

> ***Примечание***
>
> Членство в группе рассылки не распространяется с маркерами безопасности, поэтому группы рассылки не влияют на размер маркера.

Когда использовать локальные группы домена, глобальные и универсальные группы

Локальные группы домена, глобальные и универсальные группы предоставляют много опций настройки групп на предприятии. Хотя эти области групп разработаны для упрощения администрирования, плохое планирование может превратить их в ночной кошмар администратора. Идеально, если области групп призваны помочь в создании иерархии групп, которые отражают структуру организации и обязанности определенных групп пользователей. Лучшее использование локальных, глобальных и универсальных групп следующее.

- *Локальные группы домена* — используйте эти группы для управления доступом к ресурсам, таким как принтеры и совместно используемые папки.
- *Глобальные группы* — использование групп с глобальной областью поможет управлять учетными записями пользователей и компьютеров в определенном домене. Можно предоставить разрешения доступа к ресурсу, сделав группу с глобальной областью членом группы с областью локального домена.
- *Универсальные группы* — диапазон применения групп с универсальной областью наиболее широк. Используйте такие группы, чтобы консолидировать группы, которые охватывают домены. Можно сделать это путем добавления глобальных групп в качестве членов. Затем, после изменения членства глобальных групп, изменения не будут реплицированы во все глобальные каталоги, потому что членство универсальной группы не было изменено.

> ***Совет***
>
> Если у организации единственный домен, нет необходимости использовать универсальные группы. Вместо этого постройте свою структуру групп с использованием локальных групп домена и глобальных групп. Затем, если даже появится новый домен в дереве доменов, можно будет легко расширить иерархию групп.

Рассмотрим следующий сценарий. Допустим, у некоторой компании есть филиалы в Сиэтле, Чикаго и Нью-Йорке. У каждого офиса — собственный домен, который является частью одного и того же дерева домена или леса. Эти домены называются Seattle, Chicago и NY. Задача администратора — упростить каждому администратору (из любого офиса) управление сетевыми ресурсами. Поэтому нужно создать одинаковые структуры групп в каждом из офисов. Несмотря на то, что у компании есть отделы маркетинга, IT и технические отделы,

давайте сфокусируемся именно на структуре маркетингового отдела. В каждом офисе членам отдела маркетинга необходим доступ к совместно используемому принтеру MarketingPrinter и совместно используемой папке данных MarketingData. Также нужно, чтобы пользователи могли разделять и печатать документы. Например, Боб в Сиэтле должен иметь возможность напечатать документы так, чтобы Ральф в Нью-Йорке смог получить их на своем локальном принтере, а также Боб должен иметь доступ к квартальному отчету, находящемуся в совместно используемой папке в нью-йоркском офисе.

Для настройки групп в подразделениях маркетинга в трех офисах нужно выполнить следующие действия:

1. Начните с создания глобальных групп для каждой группы маркетинга. В домене Seattle создайте группу GMarketing и добавьте в нее членов отдела маркетинга в Сиэтле. В домене Chicago создайте группу также с названием GMarketing и добавьте в нее членов отдела маркетинга в Чикаго. Аналогично, в домене NY создайте группу с названием GMarketing и добавьте в нее пользователей отдела маркетинга в Нью-Йорке.
2. В каждом расположении создайте локальные группы домена, предоставляющие доступ к общим принтерам и папкам. Назовите группу принтеров LocalMarketingPrinter, а группу для общей папки — LocalMarketingData. В каждом домене Seattle, Chicago и NY должны быть собственные такие группы.
3. Создайте группу с универсальной областью в домене каждой ветки офиса. Назовите группу UMarketing. Добавьте в нее группы Seattle\GMarketing, Chicago\GMarketing и NY\GMarketing.
4. Добавьте группу UMarketing в группы LocalMarketingPrinter и LocalMarketingData в каждом офисе. Теперь сотрудники отдела маркетинга смогут делиться данными и принтерами.

Учетные записи пользователей и групп по умолчанию

При установке Windows Server 2012 операционная система устанавливает учетные записи групп и пользователей по умолчанию. Эти учетные записи разработаны для обеспечения базовой установки, необходимой для построения сети. По умолчанию доступны учетные записи трех типов:

- *встроенные* (Built-in) — учетные записи пользователя и группы, устанавливаемые с операционной системой, приложениями и службами;
- *предопределенные* (Predefined) — учетные записи пользователя и группы, установленные с операционной системой;
- *неявные* (Implicit) — специальные группы, также известные как специальные идентификаторы, создаваемые неявно, когда происходит доступ к сетевым ресурсам.

> ***Примечание***
>
> Хотя можно модифицировать учетные записи пользователя и группы по умолчанию, нельзя удалить пользователей и группы, созданные операционной системой, поскольку потом нельзя их создать заново. SID старой и новой учетных записей не будет совпадать, следовательно, разрешения и привилегии этих учетных записей будут потеряны.

Встроенные учетные записи пользователей

Встроенные учетные записи пользователей имеют специальное назначение в Windows Server. Все системы Windows Server имеют несколько встроенных учетных записей пользователей:

- LocalSystem — псевдоучетная запись для запуска системных процессов и управления задачами уровня системы. Эта учетная запись — часть группы **Администраторы** (Administrators) на сервере и имеет все права пользователя на сервере. Если настраиваете приложения или службы на использование этой учетной записи, все связанные процессы получат полный доступ к системе сервера. Много служб запускается с помощью учетной записи LocalSystem. В некоторых случаях эти службы имеют привилегии взаимодействовать с рабочим столом. Службы, которым нужны альтернативные привилегии или права входа, запускаются под учетными записями LocalService или NetworkService.
- LocalService — псевдоучетная запись с ограниченными привилегиями, которая предоставляет доступ только к локальной системе, является частью группы **Пользователи** (Users) на сервере и имеет те же права, что и учетная запись NetworkService, за исключением, что она ограничена только локальным компьютером. Настройте приложения и службы на использование этой учетной записи, когда соответствующим процессам не нужно получать доступ к другим серверам.
- NetworkService — псевдоучетная запись для запуска служб с необходимыми дополнительными привилегиями и правами входа в локальную систему и сеть. Эта учетная запись — часть группы **Пользователи** на сервере и предоставляет меньше разрешений и привилегий по сравнению с учетной записью LocalSystem (но больше, чем LocalService). В частности, процесс, запущенный с этой учетной записью, может взаимодействовать всюду по сети, используя учетные данные учетной записи компьютера.

При установке дополнений или приложений на сервер могут быть установлены другие учетные записи по умолчанию.

Предопределенные учетные записи пользователя

С Windows Server устанавливается несколько предопределенных учетных записей пользователя, в том числе **Администратор** (Administrator) и **Гость** (Guest). На рядовых серверах предопределенные учетные записи являются локальными для отдельной системы, на которой они установлены.

У предопределенных учетных записей есть дубликаты в Active Directory. Эти учетные записи распространяются на весь домен и отличаются от локальных учетных записей на отдельных системах.

Учетная запись *Администратор*

Администратор — предопределенная учетная запись, обеспечивающая полный доступ к файлам, каталогам, службам и другим объектам. В Active Directory у учетной записи **Администратор** есть полный доступ и полные полномочия, распространяющиеся на весь домен. В противном случае у учетной записи **Администратор** есть доступ только к локальной системе. Несмотря на то, что некоторые файлы и каталоги могут быть временно защищены от учетной записи **Администратор**, она может взять под свой контроль эти ресурсы в любое время, изменив права доступа. По умолчанию учетная запись **Администратор** включена, но можно отключить или переименовать ее, чтобы улучшить безопасность.

Внимание!

Для предотвращения неавторизированного доступа к системе или домену убедитесь, что назначили учетной записи **Администратор** безопасный пароль. Также, поскольку это известная учетная запись Windows, можно переименовать ее в качестве дополнительной меры предосторожности. Если переименовать исходную учетную запись **Администратор**, то можно создать фиктивную учетную запись администратора. У этой фиктивной учетной записи не должно быть полномочий или прав, и нужно отключить ее.

Обычно не нужно изменять базовые параметры учетной записи **Администратор**. Однако, возможно, придется изменить ее расширенные параметры, например, членство в определенных группах. По умолчанию учетная запись **Администратор** для домена — член групп **Администраторы** (Administrators), **Администраторы домена** (Domain Admins), **Пользователи домена** (Domain Users), **Администраторы предприятий** (Enterprise Admins), **Владельцы-создатели групповой политики** (Group Policy Creator Owners) и **Администраторы схемы** (Schema Admins). Информацию об этих группах можно найти в следующем разделе.

Практический совет

В среде домена локальная учетная запись **Администратор** используется для управления системой сразу после установки. Это позволяет настроить систему без ее блокировки. Некоторые администраторы предпочитают не использовать данную учетную запись сразу после установки. Вместо этого нужно сделать всех администраторов членами группы **Администраторы**. Это позволит отозвать привилегии администратора без необходимости изменения паролей для всех учетных записей **Администратор**.

В рабочей группе, где каждым компьютером управляют отдельно, можно использовать эту учетную запись всякий раз, когда требуется выполнить индивидуальные задачи системного администрирования. Здесь не нужно настраивать отдельные учетные записи для каждого пользователя, у которого есть административный доступ к системе. Вместо этого используйте отдельную учетную запись **Администратор** на каждом компьютере.

Учетная запись *Гость*

Учетная запись **Гость** предназначена для пользователей, которым необходим одноразовый или случайный доступ. Хотя гости получают ограниченный доступ к системе, нужно быть очень осторожными при использовании этой учетной записи. При каждом использовании этой учетной записи гарантированы потенциальные проблемы безопасности. Риск настолько большой, что по умолчанию в Windows Server эта учетная запись отключена.

Учетная запись **Гость** по умолчанию является членом групп **Гости домена** (Domain Guests) и **Гости** (Guests). Обратите внимание, что учетная запись **Гость**, как и другие именованные учетные записи, также является членом неявной группы **Все** (Everyone). Группа **Все** обычно имеет доступ к файлам и папкам. Также у этой группы есть набор прав пользователя по умолчанию.

Внимание!

Если принято решение включить учетную запись **Гость**, убедитесь, что она ограничена в правах, и регулярно изменяйте пароль. Как и в случае с записью **Администратор**, нужно переименовать учетную запись из соображений безопасности.

Встроенные и предопределенные группы

Встроенные группы установлены во всех системах Windows Server. Используйте встроенные и предопределенные группы для предоставления привилегий и разрешений группе.

Сделать это можно путем помещения пользователя в состав группы. Например, чтобы предоставить пользователю административный доступ к системе, нужно сделать его членом локальной группы **Администраторы**. Предоставить пользователю административный доступ к домену можно, сделав его членом группы **Администраторы домена** в Active Directory.

Неявные группы и специальные идентификаторы

В Windows NT неявные группы назначаются неявно во время входа и основаны на том, как пользователь получает доступ к сетевому ресурсу. Например, если пользователь получает доступ к ресурсу с помощью интерактивного входа, пользователь автоматически становится членом неявной группы **Интерактивные** (Interactive). В Windows 2000 и более поздних версиях объектно-ориентированный подход к структуре каталога изменил исходные правила для неявных групп. Несмотря на то, что все еще нельзя просмотреть членство специальных идентификаторов, можно предоставить членство в неявных группах пользователям, группам и компьютерам.

Чтобы отразить измененную роль, неявные группы также называют *специальными идентификаторами*. Специальный идентификатор — это группа, членство в которой устанавливается неявно, например во время входа в систему, или явно через специальные разрешения доступа. Как и в случае с другими группами по умолчанию, доступность определенной неявной группы зависит от текущей конфигурации. Неявные группы будут обсуждаться далее в этой главе.

Возможности учетной записи

При настройке учетной записи можно предоставить пользователю определенные возможности, сделав пользователя членом одной или нескольких групп, предоставляя, таким образом, пользователю возможности этих групп. Отозвать возможности можно, удалив пользователя из состава группы.

В Windows Server можно назначить следующие типы возможностей учетной записи.

- *Привилегия* — тип права пользователя, предоставляющий разрешения на выполнение определенных административных задач. Можно назначить привилегии учетным записям пользователя и группы. Примером привилегии является возможность завершать работу системы.
- *Права входа* — тип права пользователя, предоставляющий разрешения входа в систему. Можно назначить право входа как учетной записи пользователя, так и группы. Примером права входа является право входа локально.
- *Встроенные возможности* — тип права пользователя, который назначается группам и включает автоматические возможности группы. Встроенные возможности предопределены и неизменны, но они могут быть делегированы пользователям с разрешением управлять объектами, организационными подразделениями и другими контейнерами. Пример встроенной возможности — возможность создавать, удалять и управлять учетными записями пользователей. Эта возможность присвоена операторам учетной записи и администраторам. Таким образом, если пользователь — участник группы **Администраторы**, то он может создавать, удалять и управлять учетными записями пользователей.
- *Разрешения доступа* — тип права пользователя, определяющий операции, которые могут быть выполнены на сетевых ресурсах. Можно назначить разрешения доступа поль-

зователям, компьютерам и группам. Пример разрешения доступа — возможность создавать файл в каталоге. Разрешения доступа рассмотрены в *главе 12*.

Администратор имеет дело с возможностями учетной записи каждый день. Чтобы разобраться во встроенных возможностях, прочитайте следующие разделы. Помните, что хотя нельзя изменить встроенные возможности группы, можно изменить права группы по умолчанию. Например, администратор может отозвать сетевой доступ к компьютеру, удалив право группы получать доступ к компьютеру из сети.

Привилегии

Привилегии — это назначение права пользователя, предоставляющее разрешения на выполнение определенных административных задач. Можно назначить привилегии с помощью групповых политик, которые могут быть применены к отдельным компьютерам, организационным подразделениям и доменам. Хотя можно назначить привилегии как пользователям, так и группам, обычно нужно назначать привилегии группам. В этом случае пользователи автоматически получат соответствующие права, как только они станут членами группы. Назначение привилегий группам также упрощает управление учетными записями.

В табл. 8.2 приведено краткое описание каждой привилегии, которую можно назначить пользователям и группам. Чтобы узнать, как назначить привилегии, *см. разд. "Настройка политик прав пользователя" далее в этой главе.*

Таблица 8.2. *Привилегии пользователей и групп в Windows Server 2012*

Привилегия	Описание
Работа в режиме операционной системы (Act As Part Of The Operating System)	Позволяет процессу допускать любого пользователя к работе в системе без проверки подлинности. Процессы, для которых требуется такая привилегия, должны использовать учетную запись LocalSystem, которая уже содержит эту привилегию
Добавление рабочих станций к домену (Add Workstations To Domain)	Разрешает пользователям добавлять компьютеры в домен
Настройка квот памяти для процесса (Adjust Memory Quotas For A Process)	Разрешает пользователям изменять максимальный объем памяти, используемый процессом
Архивация папок и каталогов (Back Up Files And Directories)	Позволяет пользователям архивировать систему, независимо от разрешений, установленных для файлов и каталогов
Обход перекрестной проверки (Bypass Traverse Checking)	Позволяет пользователям производить обзор деревьев каталога, даже если у этих пользователей отсутствуют разрешения на каталог. Привилегия не позволяет пользователям просматривать содержимое каталога, а только производить его обзор
Изменение системного времени (Change The System Time)	Разрешает пользователям устанавливать время системных часов
Изменение часового пояса (Change The Time Zone)	Разрешает пользователям устанавливать часовой пояс системных часов. По умолчанию эта привилегия есть у всех пользователей

Таблица 8.2 *(продолжение)*

Привилегия	Описание
Создание файла подкачки (Create A Pagefile)	Позволяет пользователям создавать и изменять размер файла подкачки для виртуальной памяти
Создание маркерного объекта (Create A Token Object)	Позволяет процессам создавать маркерные объекты, которые могут использоваться для предоставления доступа к локальным ресурсам. Процессы, которым нужна эта привилегия, должны использовать учетную запись LocalSystem
Создание глобальных объектов (Create Global Objects)	Позволяет процессам создавать глобальные объекты. Эта привилегия по умолчанию есть у учетных записей LocalService и NetworkService
Создание постоянных общих объектов (Create Permanent Shared Objects)	Позволяет процессам создавать объекты каталога в диспетчере объектов. У большинства компонентов уже есть эта привилегия, и не нужно назначать ее специально
Создание символических ссылок (Create Symbolic Links)	Определяет для пользователя возможность создавать символические ссылки. Символические ссылки позволяют файлу или папке появиться в определенном расположении, когда на самом деле этот файл или папка находится в другом расположении. Использование символических ссылок по умолчанию ограничено из соображений безопасности
Отладка программ (Debug Programs)	Разрешает пользователям осуществить отладку программ
Разрешение доверия к учетным записям компьютеров и пользователей при делегировании (Enable Computer And User Accounts To Be Trusted For Delegation)	Определяет, какие пользователи могут устанавливать параметр **Делегирование разрешено** для пользователя или объекта-компьютера
Принудительное удаленное завершение работы (Force Shutdown From A Remote System)	Позволяет пользователям завершать работу компьютера с удаленной системы
Создание аудитов безопасности (Generate Security Audits)	Разрешает процессам создавать записи журнала для аудита доступа к объектам
Имитация клиента после проверки подлинности (Impersonate A Client After Authentication)	Позволяет веб-приложениям действовать как клиентам во время обработки запросов. Службы и пользователи также могут работать как клиенты
Увеличение рабочего набора процесса (Increase A Process Working Set)	Разрешает пользователю увеличить размер рабочего набора процесса. Рабочий набор процесса — это набор страниц памяти, видимых в данный момент процессу в физической памяти. При увеличении рабочего набора снижается количество ошибок страниц и повышается производительность

Таблица 8.2 *(продолжение)*

Привилегия	Описание
Увеличение приоритета выполнения (Increase Scheduling Priority)	Позволяет процессам повышать приоритет выполнения другого процесса, при условии, что у них есть доступ для записи к процессу
Загрузка и выгрузка драйверов устройства (Load And Unload Device Drivers)	Позволяет пользователям устанавливать и деинсталлировать драйверы PnP-устройств. Это не влияет на драйверы не-PnP-устройств, которые могут устанавливать только администраторы
Блокировка страниц в памяти (Lock Pages in Memory)	Позволяет процессам хранить данные в физической памяти, запрещая системе выгружать данные в виртуальную память на диск
Управление аудитом и журналом безопасности (Manage Auditing And Security Log)	Позволяет пользователям указывать опции аудита и получать доступ к журналу безопасности. Сначала нужно включить аудит в политике группы
Изменение метки объекта (Modify An Object Label)	Позволяет пользовательскому процессу изменять метки целостности объектов, таких как файлы, разделы реестра или процессы, владельцами которых являются другие пользователи. Эти привилегии могут быть использованы для понижения приоритета других процессов. Процессы, запущенные под учетной записью пользователя, могут модифицировать любой объект, который принадлежит пользователю без запроса этой привилегии
Изменение параметров среды изготовителя (Modify Firmware Environment Values)	Разрешает пользователям и процессам изменять системные переменные среды
Выполнение задач по обслуживанию томов (Perform Volume Maintenance Tasks)	Разрешает администрирование сменных носителей, дефрагментацию диска и управление диском
Профилирование одного процесса (Profile A Single Process)	Разрешает пользователям контролировать производительность несистемных процессов
Профилирование производительности системы (Profile System Performance)	Позволяет пользователям следить за производительностью системных процессов
Отключение компьютера от стыковочного узла (Remove Computer From Docking Station)	Разрешает отключение лэптопа от стыковочного узла и его удаление из сети
Замена маркера уровня процесса (Replace A Process Level Token)	Позволяет процессам заменять маркер по умолчанию для подпроцессов
Восстановление файлов и каталогов (Restore Files And Directories)	Разрешает пользователям восстанавливать заархивированные файлы и каталоги, независимо от разрешений, установленных для файлов и каталогов
Завершение работы системы (Shut Down The System)	Разрешает пользователям выключать локальный компьютер
Синхронизация данных службы каталога (Synchronize Directory Service Data)	Позволяет пользователям синхронизировать данные службы каталога на контроллерах домена

Таблица 8.2 *(окончание)*

Привилегия	Описание
Смена владельцев файлов и других объектов (Take Ownership Of Files Or Other Objects)	Разрешает пользователям сменять владельцев файлов и любых других объектов Active Directory

Права входа

Право входа — право пользователя, предоставляющее полномочия входа в систему. Можно назначить право входа как учетной записи пользователя, так и учетной записи группы. Как и в случае с привилегиями, права входа назначаются через групповые политики, кроме того, права входа проще назначать сразу группам, нежели отдельным пользователям.

В табл. 8.3 приведено краткое описание каждого права входа, которое можно назначить пользователям и группам. Назначение прав входа описано в *разд. "Настройка политик прав пользователя" далее в этой главе*.

Таблица 8.3. *Права входа Windows Server 2012 для пользователей и групп*

Право входа	Описание
Доступ к диспетчеру учетных данных от имени доверенного вызывающего (Act As Part Of The Operating System)	Предоставляет разрешение устанавливать доверенное соединение с диспетчером учетных данных (Credential Manager). Учетные данные (имя пользователя и пароль или смарт-карта) обеспечивают идентификацию
Доступ к компьютеру из сети (Add Workstations To Domain)	Предоставляет удаленный доступ к компьютеру
Локальный вход в систему (Allow Log On Locally)	Предоставляет разрешение войти в систему с клавиатуры компьютера. На контроллерах домена это право по умолчанию ограничено и доступно только следующим группам: **Администраторы** (Administrators), **Операторы учета** (Account Operators), **Операторы архива** (Backup Operators), **Операторы печати** (Print Operators) и **Операторы сервера** (Server Operator)
Разрешить вход в систему через службу удаленных рабочих столов (Allow Log On Through Remote Desktop Services)	Предоставляет доступ с помощью службы удаленных рабочих столов. Это право необходимо для удаленной помощи и удаленного использования рабочего стола
Отказать в доступе к этому компьютеру из сети (Deny Access To This Computer From The Network)	Запрещает удаленный доступ к этому компьютеру по сети
Отказать во входе в качестве пакетного задания (Deny Logon As Batch Job)	Запрещает право входа в качестве пакетного задания или сценария
Отказать во входе в качестве службы (Deny Logon As Service)	Запрещает вход в качестве службы
Запретить локальный вход (Deny Logon As Service)	Запрещает локальный вход в систему с использованием клавиатуры компьютера

Таблица 8.3 *(окончание)*

Право входа	Описание
Запретить вход в систему через службу удаленных рабочих столов (Deny Logon Through Remote Desktop Services)	Запрещает вход в систему с использованием удаленных рабочих столов
Вход в качестве пакетного задания (Log On As A Batch Job)	Предоставляет разрешение войти в систему в качестве пакетного задания
Вход в качестве службы (Log On As A Service)	Предоставляет разрешение войти в систему в качестве службы. Это право есть у учетной записи LocalSystem. Данное право нужно назначить учетной записи службы

Встроенные возможности для групп в Active Directory

Встроенные возможности, назначаемые группам в Active Directory, зависят от конфигурации компьютера. С помощью **Редактора локальной групповой политики** (Local Group Policy Editor) (рис. 8.1) можно просмотреть возможности, которые назначаются каждой группе, раскрыв узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики** (Computer Configuration\Windows Settings\Security Settings\Local Policies) и выбрав узел **Назначение прав пользователя** (User Rights Assignment).

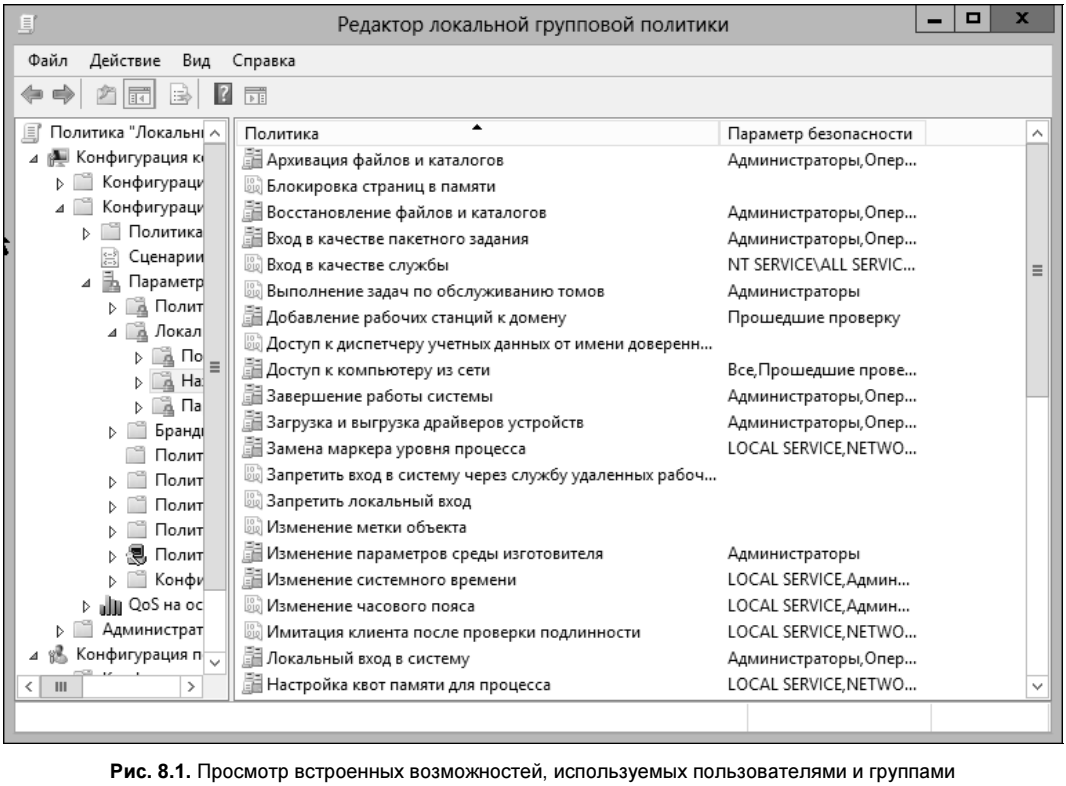


Рис. 8.1. Просмотр встроенных возможностей, используемых пользователями и группами

Заметьте, что любое действие, доступное группе **Все** (Everyone), доступно всем группам, в том числе группе **Гости** (Guests). Это означает, что, несмотря на то, что группе **Гости** не назначено явных разрешений на получение доступа к компьютеру из сети, члены этой группы все еще могут получить доступ к системе, поскольку есть права у группы **Все**.

В табл. 8.4 представлены возможности, которые можно делегировать другим пользователям и группам. Обратите внимание, что ограниченные учетные записи включают: учетную запись пользователя **Администратор**, учетные записи пользователей-администраторов, учетные записи групп **Администраторы**, **Операторы сервера** (Server Operator), **Операторы учета** (Account Operators), **Операторы архива** (Backup Operators) и **Операторы печати** (Print Operators). Поскольку эти учетные записи ограничены, операторы учета не могут создать или изменить их.

Таблица 8.4. *Другие возможности встроенных и локальных групп*

Задача	**Описание**	**Обычно назначено группе**
Назначение прав пользователей (Assign User Rights)	Позволяет пользователям назначать права других пользователей	**Администраторы**
Создание, удаление и управление группами (Create And Delete Groups)	Позволяет пользователям создавать новые группы и удалять существующие	**Администраторы**, **Операторы учета**
Создание и удаление принтеров (Create And Delete Printers)	Разрешает пользователям создавать и удалять принтеры	**Администраторы**, **Операторы сервера**, **Операторы печати**
Создание, удаление и управление учетными записями пользователей (Create, Delete, And Manage User Accounts)	Разрешает пользователям администрировать учетные записи домена	**Администраторы**, **Операторы учета**
Управление ссылками на групповые политики (Manage Group Policy Links)	Разрешает пользователям применять существующие групповые политики к сайтам, доменам и организационным подразделениям, для которых у них есть доступ для записи к соответствующим объектам	**Администраторы**
Управление настройкой сети (Manage Network Configuration)	Разрешает пользователям настраивать сеть	**Администраторы**, **Операторы настройки сети**
Manage Performance Logs	Позволяет настраивать журналы производительности	**Администраторы**, **Пользователи журналов производительности** (Performance Log Users)
Управление принтерами (Manage Printers)	Разрешает пользователям управлять принтерами и очередью печати	**Администраторы**, **Операторы сервера**, **Операторы печати**

Таблица 8.4 *(окончание)*

Задача	Описание	Обычно назначено группе
Изменение членства в группах (Modify The Membership Of A Group)	Позволяет пользователям добавлять других пользователей в группы домена и удалять их	**Администраторы**, **Операторы учета**
Monitor Performance Logs	Разрешает пользователям настраивать журналирование производительности	**Администраторы**, **Пользователи журналов производительности**
Осуществление криптографических операций (Perform Cryptographic Operations)	Разрешает пользователям управлять параметрами криптографии	**Криптографические операторы** (Cryptographic Operators)
Чтение информации обо всех пользователях (Read All User Information)	Позволяет просматривать информацию об учетной записи пользователя	**Администраторы**, **Операторы сервера**, **Операторы учета**
Чтение журнала событий (Read Event Logs)	Разрешает читать журнал событий	**Администраторы**, **Читатели журнала событий** (Event Log Readers)
Переустановить пароли пользователей (Reset Passwords On User Accounts)	Позволяет пользователям сбрасывать пароли других пользователей	**Администраторы**, **Операторы учета**

Использование учетных записей групп по умолчанию

Универсальные учетные записи групп разрабатывались, чтобы быть универсальными. Назначая пользователя в правильную группу, можно сделать управление рабочей группой или доменом Windows Server 2012 намного проще. К сожалению, когда есть много разных групп, не просто понять, для чего используется та или иная группа. Давайте внимательно рассмотрим группы, используемые администраторами, и группы, которые создаются неявно.

Группы, используемые администраторами

Администратор — тот, у кого есть широкий доступ к сетевым ресурсам. Администраторы могут создавать учетные записи, изменять права пользователей, устанавливать принтеры, управлять общими ресурсами и т. д. Основные группы администратора — **Администраторы** (Administrators), **Администраторы домена** (Domain Admins) и **Администраторы предприятия** (Enterprise Admins). В табл. 8.5 сравниваются группы администратора.

Совет

Учетная запись **Администратор** и глобальные группы **Администраторы домена** и **Администраторы предприятия** являются членами группы **Администраторы**. Учетная запись **Администратор** используется для получения доступа к локальному компьютеру. Членство в группе **Администраторы домена** позволяет другим администраторам получить доступ

к системе из любого места домена. Членство в группе **Администраторы предприятия** позволяет другим администраторам получить доступ к системе с любого домена в текущем дереве домена или лесу. Если не хотите, чтобы к системе получал доступ любой администратор предприятия, просто удалите группу **Администраторы домена** из этой группы.

Таблица 8.5. *Обзор групп администратора*

Тип группы администратора	Сетевая среда	Действие группы	Членство
Администраторы	Домены Active Directory	Локальный домен	**Администратор**, **Администраторы домена**, **Администраторы предприятия**
Администраторы	Рабочие группы, компьютеры, не входящие в домен	Локальное	**Администратор**
Администраторы домена	Домены Active Directory	Глобальное	**Администратор**
Администраторы предприятия	Домены Active Directory	Глобальное или универсальное	**Администратор**
Администраторы схемы	Домены Active Directory	Универсальное	**Администратор**

Администраторы — это локальная группа, предоставляющая полный административный доступ к отдельным компьютерам или к единственному домену, в зависимости от его расположения. Поскольку у этой учетной записи есть полный доступ, нужно быть очень осторожными при добавлении пользователей в эту группу. Чтобы назначить кого-то администратором локального компьютера или домена, все, что нужно сделать — это добавить человека в эту группу. Только члены группы **Администраторы** могут изменить эту учетную запись.

Администраторы домена — глобальная группа, разработанная, чтобы помочь управлять ресурсами в домене. Члены этой группы имеют полный контроль над доменом. Эта группа обладает административным контролем над всеми компьютерами в домене, потому что она — член группы **Администраторы** по умолчанию на всех контроллерах домена, всех рабочих станциях и всех рядовых серверах домена, как только они присоединяются к домену. Чтобы назначить кого-то администратором домена, сделайте этого человека членом данной группы.

Совет

Учетная запись **Администратор** — это член **Администраторы домена** по умолчанию. Это означает, что если пользователь входит по учетной записи администратора в систему компьютера, являющегося членом домена, у пользователя будет полный доступ ко всем ресурсам домена.

Администраторы предприятия — глобальная группа, призванная помочь управлять ресурсами леса. Члены этой группы имеют полный контроль над всеми доменами в лесу. Эта группа обладает полным административным контролем над контроллерами домена в предприятии, потому что эта группа является членом группы **Администраторы** по умолчанию

на всех контроллерах домена в лесу. Чтобы сделать кого-то администратором предприятия, просто добавьте его в эту группу.

> ***Совет***
>
> Учетная запись **Администратор** по умолчанию является членом группы **Администраторы предприятия**. Это означает, что если кто-то входит с правами администратора в систему компьютера, являющегося членом домена, этот пользователь получит полный доступ к доменному дереву и лесу.

Администраторы схемы — универсальная группа, разработанная для управления схемой в Active Directory. Члены этой группы могут работать со схемой и изменять схему Active Directory. Перед тем, как кто-либо сможет редактировать схему, нужно сделать его членом этой группы.

Неявные группы и идентификаторы

Операционная система Windows Server определяет ряд специальных идентификаторов, которые можно использовать, чтобы присвоить разрешения в конкретных ситуациях. Обычно разрешения неявно присваиваются специальным идентификаторам. Однако можно назначить разрешения специальным идентификаторам непосредственно при модификации объектов Active Directory. Список специальных идентификаторов приведен далее.

- **Анонимный вход** (Anonymous Logon) — в эту группу зачисляется любой пользователь, получивший доступ к системе посредством анонимного входа. Эта группа разрешает анонимный доступ к ресурсам, например, к веб-странице, опубликованной на корпоративном сервере.
- **Прошедшие проверку** (Authenticated Users) — в эту группу попадает пользователь, прошедший проверку подлинности. Идентификатор разрешает доступ к общим ресурсам в пределах домена, например, к файлам в общей папке, которые должны быть доступны всем сотрудникам организации.
- **Пакетные файлы** (Batch) — к этой группе относится любой пользователь, получивший доступ к системе в качестве пакетного задания. Позволяет запускать запланированные задачи, например, ночное удаление временных файлов.
- **Группа-создатель** (Creator Group) — Windows Server использует эту специальную группу для автоматичного предоставления доступа пользователям, являющимся членами той же группы, что и создатель файла или каталога.
- **Создатель владелец** (Creator Owner) — лицо, создавшее файл или каталог, становится членом этой специальной группы. Windows Server использует эту группу для автоматического предоставления разрешений создателю файла или каталога.
- **Удаленный доступ** (Dial-Up) — любой пользователь, получивший доступ в систему с помощью коммутируемого соединения, попадает в группу **Удаленный доступ**. Эта группа позволяет разграничить пользователей dial-up от других типов аутентифицированных пользователей.
- **Контроллеры домена предприятия** (Enterprise Domain Controllers) — контроллеры домена, выполняющие роли уровня предприятия. Эта группа позволяет выполнять определенные задачи с помощью транзитивного доверия.
- **Все** (Everyone) — все интерактивные, сетевые, dial-up и аутентифицированные пользователи являются членами данной группы. Это специальная группа предоставляет широкий доступ к ресурсам системы.

- **Интерактивные** (Interactive) — любой пользователь, выполнивший локальный вход в систему. Данная группа позволяет предоставить доступ к ресурсу только локальным пользователям.
- **Сеть** (Network) — членом этой группы является любой пользователь, вошедший в систему по сети. Данная группа позволяет предоставить доступ к ресурсу только удаленным пользователям.
- **Proxy** — пользователи и компьютеры, получающие доступ к ресурсам через прокси, попадают в эту группу. Группа используется, когда в сети реализованы прокси-серверы.
- **Пользователи удаленного рабочего стола** (Remote Desktop Services User) — любой пользователь, получивший доступ к системе с помощью служб удаленного рабочего стола. Позволяет пользователям удаленного рабочего стола получать доступ к приложениям служб удаленного рабочего стола и осуществлять другие необходимые задачи с этими службами.
- **Ограниченные** (Restricted) — пользователи и компьютеры с ограниченными возможностями.
- **Self** — указывает на сам объект и позволяет объекту изменять самого себя.
- **Служба** (Service) — любая служба, получающая доступ к системе. Данная группа предоставляет доступ к процессам, запущенным службами Windows Server.
- **Система** (System) — сама операционная система Windows Server. Группа используется, когда операционной системе нужно выполнить действия на уровне системы.

Установка и организация учетной записи пользователя

Ключевая часть работы администратора — создавать учетные записи, и в этом разделе будет рассказано, как это сделать. Учетные записи пользователя и группы позволяют Windows Server 2012 отслеживать и управлять информацией о пользователях, в том числе разрешениями и привилегиями. Для создания учетной записи пользователя обычно применяются две следующие административные утилиты:

- **Active Directory — пользователи и компьютеры**, разработанная для администрирования учетных записей через домен Active Directory;
- **Локальные пользователи и группы**, разработанная для администрирования учетных записей на локальном компьютере.

Наиболее важный аспект создания учетной записи — ее установка и организация. Без надлежащих инструкций и политик можно обнаружить, что необходимо переделать все учетные записи пользователей. Перед созданием учетных записей нужно определить политики, которые будут использоваться для установки и организации.

Политики именования учетных записей

Ключевая политика нуждается в установке схемы имен для учетных записей. У учетных записей есть отображаемые имена и имена входа. *Отображаемое имя* (или полное имя) — имя, отображаемое пользователям, и имя, показываемое в сеансах пользователя. *Имя входа* — это имя, используемое для входа в домен. Имена входа были кратко рассмотрены в *разд. "Имена входа, пароли и публичные сертификаты" ранее в этой главе.*

Правила для отображаемых имен

Для учетных записей домена отображаемое имя обычно состоит из фамилии, имени и отчества, но можно указать любую строку. Отображаемое имя должно соответствовать следующим правилам:

- локальные отображаемые имена должны быть уникальными на отдельном компьютере;
- отображаемые имена должны быть уникальными в пределах домена;
- максимальная длина отображаемого имени — 64 символа;
- отображаемые имена могут содержать алфавитно-цифровые и специальные символы.

Правила для имен входа

Имена входа должны следовать этим правилам:

- локальные имена входа должны быть уникальными в пределах отдельного компьютера, глобальные имена входа должны быть уникальными в пределах домена;
- имена входа могут состоять из 256 символов. Однако очень непрактично использовать имена входа длиной более 64 символов;
- старые имена входа (в формате для ОС, предшествовавших Windows 2000) назначаются всем учетным записям. По умолчанию, в качестве этого имени входа используются первые 20 символов обычного имени входа. Имена входа в старом формате тоже должны быть уникальными в пределах домена;
- пользователи, входящие в домен с компьютера, работающего под управлением Windows 2000 или более поздней версии, могут использовать свои стандартные имена входа или свои имена в старом формате (для ОС, предшествовавших Windows 2000) независимо от режима работы домена;
- имена входа не могут содержать определенных символов. Следующие символы недопустимы: `" / \ [ ] ; | = , + * ? < >`;
- имена входа могут содержать все остальные специальные символы, в том числе пробелы, двоеточия, тире и символы подчеркивания. Однако использовать данные символы в именах учетных записей — не очень хорошая идея.

> ***Примечание***
>
> Хотя Windows Server сохраняет имена пользователей в регистре, в котором они были указаны, имена пользователей не чувствительны к регистру. Например, можно получить доступ к учетной записи администратора, используя имена пользователя **Администратор**, **администратор** или **АДМИНИСТРАТОР**. Таким образом, регистр символов сохраняется, но не учитывается.

Схемы имен

Большинство небольших организаций склонно назначать имена входа с использованием имени и фамилии пользователя. Но в большой организации может быть несколько лиц с одинаковыми именами. Чтобы в будущем не пришлось изменять схему имен, лучше сразу выбрать хорошую схему имен и убедиться, что другие администраторы используют ее. Необходимо использовать непротиворечивую процедуру именования учетных записей, которая позволила бы расти базе пользователей, ограничить возможность конфликта имен и убедиться, что у учетных записей безопасные имена, которые не будут скомпрометированы.

Если следовать данным инструкциям, можно использовать эти схемы имен:

- имя пользователя и последний инициал;
- первый инициал и фамилия пользователя;
- инициалы пользователя и фамилия;
- инициалы пользователя и первые пять символов фамилии;
- имя пользователя и фамилия.

> ***Внимание!***
>
> В среде со строгой безопасностью можно в качестве имени входа использовать числовой код. Он должен состоять как минимум из 20 символов. Объедините этот строгий метод именования со смарт-картами и кардридерами, чтобы позволить пользователям быстро входить в домен без необходимости ввода всех этих символов. Не волнуйтесь, у пользователя все еще может быть отображаемое имя, которое смогут прочитать люди.

Политики паролей и учетных записей

Учетные записи домена используют пароли или приватные ключи из сертификатов для аутентификации доступа к сетевым ресурсам. В этом разделе мы сфокусируемся на паролях.

Использование безопасных паролей

Пароль — это чувствительная к регистру строка, которая может содержать 127 символов и более при использовании Active Directory и до 14 символов при использовании Windows NT Security Manager. Допустимые символы для паролей — буквы, цифры и другие символы. При установке пароля для учетной записи Windows Server сохраняет пароль в зашифрованном виде в базе данных учетных записей.

Но простого наличия пароля недостаточно. Ключ к предотвращению несанкционированного доступа к сетевым ресурсам — использование безопасных паролей. Разница между среднестатистическим и безопасным паролем — безопасные пароли трудно подобрать и взломать. Сделать пароль сложным для подбора и взлома можно, используя комбинацию всех доступных типов символов, в том числе символов разного регистра, цифр и прочих символов. Например, вместо того, чтобы использовать happydays в качестве пароля, лучше выбрать haPPy2Days&, Ha**y!day5 или даже h*99Y%d*ys.

Также можно использовать парольные фразы. В этом случае пароль содержит несколько слов и знаки пунктуации, как в предложении. Например, "This problem is 99 times ten!". Эта фраза содержит знаки пунктуации, цифры и удовлетворяет всем требованиям сложности и невероятно трудна для взлома.

К сожалению, нет никакой разницы, насколько безопасным будет начальный пароль, пользователь со временем может установить собственный пароль. Поэтому необходимо установить политики учетных записей, определяющие, каким будет безопасный пароль для имеющихся систем. Политики учетных записей — это подмножество политик, настраиваемых в групповой политике.

Установка политик учетных записей

Как было отмечено в предыдущих главах, можно применить групповые политики на различных уровнях структуры сети. Управление локальными групповыми политиками было рассмотрено в *разд. "Управление локальными групповыми политиками" главы 4*, а управле-

ние глобальными групповыми политиками — в *разд. "Управление политиками сайта, домена и организационной единицы" той же главы*.

Политики учетной записи должны быть сконфигурированы в GPO с наивысшим приоритетом, связанным с доменом. По умолчанию GPO с наивысшим приоритетом называется Default Domain Policy GPO. Как только будет получен доступ к Default Domain Policy GPO или другому надлежащему GPO, можно установить политики учетных записей с помощью этих действий:

1. В утилите **Редактор управления групповыми политиками** (рис. 8.2) разверните узел **Политики учетных записей** (Account Policies), находящийся в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности** (Computer Configuration\Windows Settings\Security Settings). Дерево консоли покажет имя настраиваемого компьютера или домена. Убедитесь, что выполняется настройка нужного сетевого ресурса.

   Примечание

   Политики домена имеют приоритет над локальными политиками. GPO с порядком ссылки 1 в домене всегда имеет наивысший приоритет.

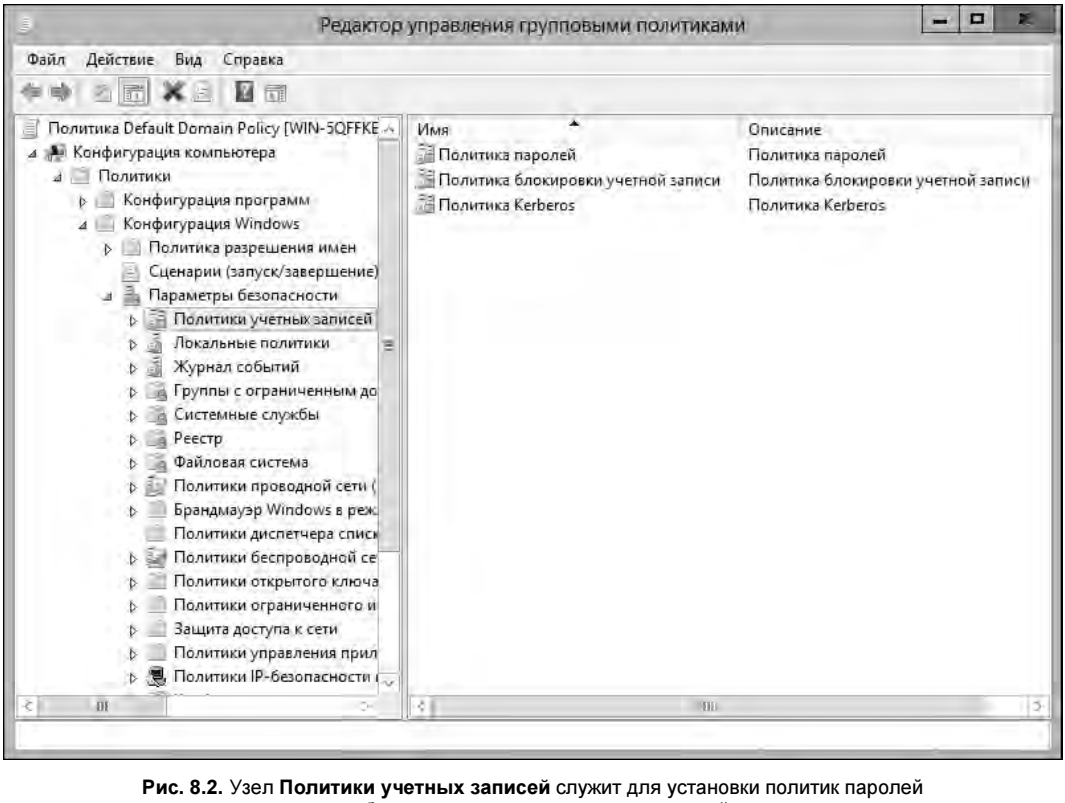


Рис. 8.2. Узел **Политики учетных записей** служит для установки политик паролей и общего использования учетных записей

2. Теперь можно управлять политиками учетных записей с помощью узлов **Политика паролей** (Password Policy), **Политика блокировки учетной записи** (Account Lockout Policy) и **Политика Kerberos** (Kerberos Policy). Чтобы настроить политику, дважды щелкните по ней или щелкните правой кнопкой мыши и выберите команду **Свойства**.

Откроется одноименное окно (рис. 8.3). Все политики могут быть или определены, или не определены. Это означает, что они могут быть либо настроены, либо не настроены для использования. Политика, не определенная в текущем контейнере, может быть наследована из следующего контейнера.

Примечание

Политики Kerberos не используются на локальных компьютерах и доступны только в групповых политиках, применяемых к доменам. Для автономных серверов можно изменить параметры локальных политик. Однако нельзя изменить настройки локальной политики для контроллеров доменов или рядовых серверов.

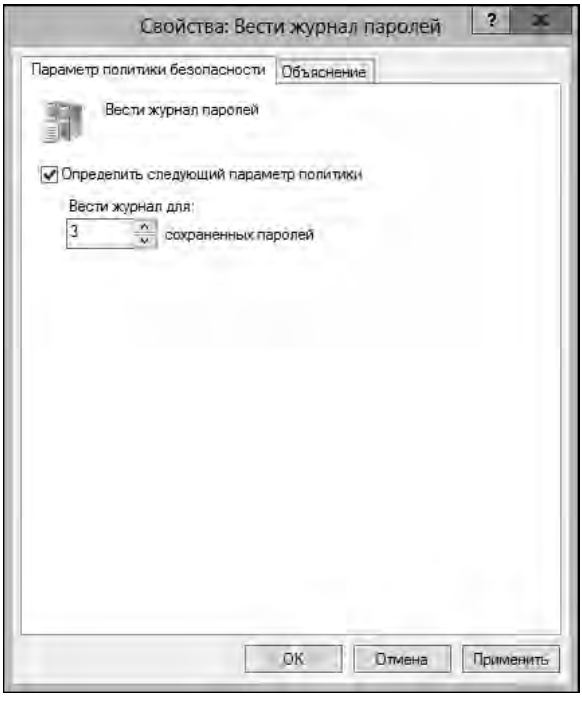


Рис. 8.3. Определите и настройте глобальную политику групп в диалоге **Свойства**

3. Установите или сбросьте флажок **Определить следующий параметр политики** (Define This Policy Setting), чтобы указать, определена ли политика.

Совет

Политики могут иметь дополнительные параметры для настройки. Часто эти параметры — кнопки с надписями **Включить** (Enabled) или **Отключить** (Disabled). Нажатие кнопки **Включить** включает ограничение политики. Нажатие кнопки **Отключить** выключает ограничение политики. Некоторые политики являются отрицательными, т. е. включение таких политик фактически инвертирует элемент. Например, политика **Отказать во входе в качестве службы** (Disable Log On As A Service) является обратной для политики **Вход в качестве службы** (Log On As A Service).

Некоторые процедуры для работы с политиками учетных записей обсуждаются в *разд. "Настройка политик паролей"*, *"Настройка политик блокировки учетных записей"* и *"Настройка политик Kerberos" далее в этой главе*.

Настройка политик учетной записи

Как было упомянуто в предыдущем разделе, есть три типа политик учетных записей: политика паролей, политика блокировки учетной записи и политика Kerberos. Следующие разделы показывают, как настроить эти политики.

Настройка политик паролей

Политики паролей, приведенные здесь, контролируют безопасность паролей:

- вести журнал паролей;
- максимальный срок действия пароля;
- минимальная длина пароля;
- минимальный срок действия пароля;
- пароль должен отвечать требованиям сложности;
- хранить пароли, используя обратимое шифрование.

Использование этих политик обсуждается в следующих разделах.

Ведение журнала паролей

Политика **Вести журнал паролей** (Enforce Password History) устанавливает, как часто старые пароли могут использоваться повторно. С помощью этой политики можно отучить пользователей использовать несколько общих паролей. В журнале паролей Windows Server может хранить до 24 паролей для каждого пользователя.

Чтобы отключить эту опцию, установите число паролей, равное 0. Чтобы активировать ее, установите значение истории паролей, используя поле **Вести журнал для** (Passwords Remembered). После этого Windows Server будет отслеживать старые пароли на основе истории паролей, уникальной для каждого пользователя. Пользователям не разрешается устанавливать ранее использованные пароли.

> ***Примечание***
>
> Чтобы помешать пользователям обойти настройки политики **Вести журнал паролей**, не позволяйте пользователям сразу изменять пароли. Это мешает пользователям изменить пароли несколько раз, чтобы вернуться к старому паролю. Это можно сделать с помощью политики **Минимальный срок действия пароля** (Minimum Password Age), как будет показано позже в этой главе.

Максимальный срок действия пароля

Политика **Максимальный срок действия пароля** (Maximum Password Age) определяет, сколько дней пользователи могут хранить пароль перед его обязательным изменением. Цель этой политики — заставить пользователей периодически менять свои пароли. Установите значение, имеющее смысл в конкретной сети. В целом, нужно использовать более короткий период, когда безопасность очень важна, и более длительный период, когда безопасность менее важна.

Можно установить максимальный срок действия пароля от 0 до 999 дней. Величина 0 означает, что пароли не истекают. Несмотря на желание не устанавливать дату истечения пароля, пользователи должны менять пароль регулярно, чтобы обеспечить безопасность сети.

Там, где важна безопасность, используйте значение 30, 60 или 90 дней. Где безопасность менее важна, хорошие значения равны 120, 150 или 180 дней.

Примечание

ОС Windows Server уведомляет пользователей, когда срок действия пароля истечет. Как только до даты окончания действия пароля останется меньше 30 дней, пользователи увидят предупреждение (сразу после входа в систему), что через определенный период нужно будет изменить пароль.

Минимальный срок действия пароля

Минимальный срок действия пароля (Minimum Password Age) определяет, сколько дней должно пройти перед тем, как пользователь сможет изменить его. Можно использовать эту политику, чтобы помешать пользователям несколько раз подряд менять пароль, чтобы установить старый пароль.

Если минимальный срок действия пароля установлен в 0, пользователи сразу могут изменить свои пароли. Чтобы предотвратить это, установите определенный минимальный срок. Имеет смысл использовать значения от 3 до 7 дней. Таким образом, пользователи не смогут сразу перейти на старый пароль, но при необходимости смогут изменить пароль, не дожидаясь максимального срока действия. Имейте в виду, что минимальный срок действия пароля может препятствовать смене скомпрометированного пароля. Если пользователь не может изменить пароль, это должен сделать администратор.

Минимальная длина пароля

Политика **Минимальная длина пароля** (Minimum Password Length) устанавливает минимальное число символов пароля. Если значение по умолчанию не было изменено, сделайте это немедленно. Значение по умолчанию в некоторых случаях позволяет устанавливать пустые пароли (пароли с 0 символов), что определенно не очень хорошая идея.

Из соображений безопасности нужно использовать пароли длиной минимум 8 символов. Если необходима еще большая безопасность, установите минимальную длину пароля, равную 14 символов.

Пароль должен отвечать требованиям сложности

Кроме политик паролей и учетных записей, Windows Server содержит средства для дополнительного управления паролем. Эти средства заставляют использовать безопасные пароли, которые устанавливаются в соответствии со следующими требованиями:

- минимальная длина паролей — 6 символов;
- пароли не могут содержать имя пользователя, например stevew, или часть полного имени, например steve;
- пароли должны содержать как минимум три из четырех типов символов: буквы в нижнем регистре, буквы в верхнем регистре, цифры и неалфавитные символы.

Для применения этих правил включите политику **Пароль должен отвечать требованиям сложности** (Passwords Must Meet Complexity Requirements).

Хранение паролей с использованием обратимого шифрования

Пароли в базе данных хранятся в зашифрованном виде. Обычно это шифрование не может быть обращено. Единственный случай, когда нужно изменить это поведение — ситуация,

когда организация использует приложения, которым нужно считать пароль. Если это так, включите политику **Хранить пароли, используя обратимое шифрование** (Store Password Using Reversible Encryption) для всех пользователей.

При включении этой политики пароли так же могут быть сохранены, как обычный текст. Это тоже представляет угрозу безопасности. Помните это. Намного лучше включить эту опцию для конкретных пользователей, как только она будет действительно необходима им.

Настройка политик блокировки учетной записи

Политики блокировки учетной записи, приведенные здесь, контролируют, как и когда учетные записи будут заблокированы доменом или локальной системой:

- пороговое значение блокировки;
- продолжительность блокировки учетной записи;
- время до сброса счетчика блокировки.

Эти политики обсуждаются в следующих разделах.

Пороговое значение блокировки

Пороговое значение блокировки (Account Lockout Threshold) определяет число попыток входа в систему, которые может сделать пользователь, прежде чем учетная запись будет заблокирована. Если решите использовать управление блокировкой, вам придется балансировать между предотвращением взлома учетной записи и потребностями пользователей, которые испытывают затруднения при получении доступа к своим учетным записям.

Главная причина того, что пользователи не могут получить доступ к своим учетным записям, заключается в том, что они забыли свой пароль. Если это так, им понадобится несколько попыток входа в систему. У пользователей рабочей группы также могут быть проблемы при доступе к удаленной системе, если их текущие пароли не совпадают с паролями, которые ожидает удаленная система. Например, удаленная система могла записать несколько неудачных попыток входа в систему, прежде чем пользователь получит приглашение ввести правильный пароль, потому что Windows Server попытался автоматически войти в удаленную систему. В доменной среде это обычно не происходит, благодаря функции единого входа в систему.

Можно установить значение порога блокировки от 0 до 99. Значение 0 установлено по умолчанию — учетные записи не будут заблокированы из-за неуспешных попыток входа. Любое другое значение указывает порог блокировки. Помните, что высокое значение повышает риск взлома системы хакером. Рекомендуемый диапазон для этого порога — от 7 до 15 попыток. Этого достаточно, чтобы пользователь ввел правильный пароль, и снижает вероятность взлома хакером.

Продолжительность блокировки учетной записи

Если чья-то учетная запись будет заблокирована, политика **Продолжительность блокировки учетной записи** (Account Lockout Duration) установит время блокировки. Можно установить продолжительность блокировки от 1 до 99 999 минут или же задать неограниченное время блокировки, установив значение 0.

Наилучшая политика безопасности — блокировать учетную запись навсегда. Тогда только администратор сможет ее разблокировать. Это предотвращает повторные попытки взлома

хакерами и заставляет обратиться пользователей, чья учетная запись заблокирована, за помощью к администратору, что обычно — хорошая идея. Поговорив с пользователем, можно определить, что пользователь делает неправильно, а затем поможете ему избежать будущих проблем.

Совет

Когда учетная запись пользователя заблокирована, откройте окно **Свойства** учетной записи в оснастке **Active Directory — пользователи и компьютеры**. Перейдите на вкладку **Учетная запись** (Account) и установите флажок **Разблокировать учетную запись** (Unlock Account).

Время до сброса счетчика блокировки

ОС Windows Server отслеживает каждую неудачную попытку входа и увеличивает число неудачных попыток входа. Чтобы поддерживать баланс между потенциальными блокировками от допустимых проблем безопасности и блокировками, которые могут произойти от простой человеческой ошибки, другая политика определяет, сколько времени поддерживать информацию о неудачных попытках входа в систему. Эта политика называется **Время до сброса счетчика блокировки** (Reset Account Lockout Counter After). Используйте ее, чтобы сбросить счетчик неудачных попыток входа в 0 после определенного периода ожидания. Способ работы политики прост: если период ожидания истек с момента последней неудачной попытки входа, счетчик плохих попыток сбрасывается в 0. Счетчик плохих попыток входа также сбрасывается, когда пользователь успешно входит в систему.

Если политика **Время до сброса счетчика блокировки** включена, можно установить любое значение — от 1 до 99 999 минут. Как и с пороговым значением блокировки, необходимо выбрать оптимальное значение между нуждами безопасности и потребностями пользователя. Хорошее значение — от одного до двух часов. Такой период ожидания должен быть достаточно продолжительным, чтобы заставить хакеров ждать дольше, чем они хотят перед повторной попыткой получить доступ к учетной записи.

Если политика **Время до сброса счетчика блокировки** не установлена или отключена, счетчик плохих попыток сбрасывается только при успешном входе пользователя в систему.

Примечание

Попытки неудачного входа в систему через защищенную паролем экранную заставку не увеличивают порог блокировки. Аналогично, если нажать комбинацию клавиш <Ctrl>+<Alt>+<Del> для блокировки сервера или рабочей станции, неудачные попытки не будут засчитаны, если кто-то после этого попытается войти в систему.

Настройка политик Kerberos

Kerberos v5 — основной механизм аутентификации, используемый в домене Active Directory. Протокол Kerberos применяет билеты для проверки идентификации пользователей и сетевых служб. Билеты содержат зашифрованные данные, которые подтверждают идентификационные данные в целях аутентификации и авторизации.

Можно контролировать продолжительность билета, его обновление и принудительное ограничение с помощью следующих политик:

- принудительное ограничение входа пользователей;
- максимальный срок жизни билета службы;

- максимальный срок жизни билета пользователя;
- максимальный срок жизни для возобновления билета пользователя;
- максимальная погрешность синхронизации часов компьютера.

Эти политики рассмотрены в следующих разделах.

> ***Внимание!***
>
> Только администраторы, понимающие Kerberos, должны изменять эти политики. Если установить неэффективные настройки, можно вызвать серьезные проблемы в сети. Настройки политики Kerberos по умолчанию обычно работают просто великолепно.

Принудительное ограничение входа пользователей

Политика **Принудительное ограничение входа пользователей** (Enforce User Logon Restrictions) позволяет убедиться, что применены все ограничения, установленные для учетной записи пользователя. Например, если лимитированы часы регистрации пользователя, эта политика осуществляет ограничение. По умолчанию политика включена, а ее отключение требуется лишь в очень редких случаях.

Максимальный срок жизни

Политики **Максимальный срок жизни билета службы** (Maximum Lifetime For Service Ticket) и **Максимальный срок жизни билета пользователя** (Maximum Lifetime For User Ticket) устанавливают максимальную продолжительность действия билета службы или пользователя. По умолчанию у билетов службы максимальная продолжительность жизни — 600 минут, у билетов пользователя — 10 часов.

Можно изменить срок жизни билетов. Для билетов службы допустимый диапазон — от 0 до 99 999 минут, для билетов пользователя — от 0 до 99 999 часов. Значение 0 отключает отслеживание срока жизни. Любое другое значение устанавливает определенное время жизни.

Истекающий билет пользователя может быть возобновлен при условии, что возобновление допустимо настройками политики **Максимальный срок жизни для возобновления билета пользователя** (Maximum Lifetime For User Ticket Renewal). По умолчанию максимальный период возобновления составляет 7 дней. Можно изменить период возобновления на любое значение от 0 до 99 999 дней. Значение 0 выключает максимальный период возобновления, а любые другие значения устанавливают определенный период возобновления.

Максимальная погрешность

Политика **Максимальная погрешность синхронизации часов компьютера** (Maximum Tolerance For Computer Clock Synchronization) — одна из политик Kerberos, которую, возможно, следует изменить. По умолчанию все компьютеры в домене должны синхронизироваться с разницей в 5 минут. Если это не так, будет сбой аутентификации.

Если есть удаленные пользователи, входящие в домен без синхронизации своих часов с сервером времени сети, возможно, нужно скорректировать это значение. Можно установить любое значение от 0 до 99 999. Значение 0 не устанавливает погрешность, т. е. удаленные системы должны точно синхронизировать время, иначе произойдет сбой аутентификации.

Настройка политик прав пользователя

Учетные записи пользователей обладают встроенными возможностями и правами пользователей. Хотя нельзя изменить встроенные возможности для учетных записей, можно изменить права пользователя. Обычно права пользователям назначаются путем добавления их в соответствующую группу или группы. Также можно применить права непосредственно, это можно сделать путем управления правами для учетной записи пользователя.

> ***Внимание!***
>
> Любой пользователь, являющийся членом группы, обладает всеми правами, назначенными этой группе. Например, если группа **Операторы архива** (Backup operators) имеет какое-то право доступа и jsmith является членом этой группы, то пользователь jsmith также обладает этим правом. Имейте в виду, все, что делаете с правами пользователя, может иметь далеко идущие последствия. Поэтому вносить изменения в политику прав пользователя должны только опытные администраторы.

Присвоить права пользователей можно через узел **Локальные политики** (Local Policies) групповой политики. Эти политики принадлежат только локальному компьютеру, что ясно из названия. Однако можно настроить локальные политики, а потом импортировать их в Active Directory. Также можно настроить эти локальные политики как часть существующего GPO для сайта, домена или организационного подразделения. После этого локальные политики будут применены к учетным записям компьютера сайта, домена или организационного подразделения.

Для администрирования политик прав пользователя воспользуйтесь следующими инструкциями:

1. Откройте GPO, с которым нужно работать, а затем разверните узел **Локальные политики** (Local Policies), раскрыв дерево консоли. Этот узел находится в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности** (Computer Configuration\Windows Settings\Security Settings\Local Policies).
2. Выберите политику **Назначение прав пользователя** (User Rights Assignment) для управления правами пользователя. Для настройки назначения прав пользователя дважды щелкните на праве пользователя или щелкните правой кнопкой мыши и выберите команду **Свойства**. Откроется одноименное окно.
3. Теперь можно настроить права пользователей. Для настройки локальных прав пользователя следуйте шагам 1—3 из *разд. "Настройка локальных прав пользователей" далее в этой главе*. Для настройки глобальных прав пользователей следуйте шагам 1—6 в следующем разделе.

Настройка глобальных прав пользователей

Для сайта, домена или организационного подразделения можно настроить права отдельных пользователей так:

1. Откройте окно **Свойства** для права пользователя, подобное изображенному на рис. 8.4. Если политика не включена, сбросьте флажок **Определить следующие параметры политики** (Define These Policy Settings).
2. Для применения права к пользователю или группе нажмите кнопку **Добавить пользователя или группу** (Add User or Group). Появится окно **Добавление пользователя или группы** (Add User Or Group). Нажмите кнопку **Обзор**. Откроется окно **Выбор: "Поль-**

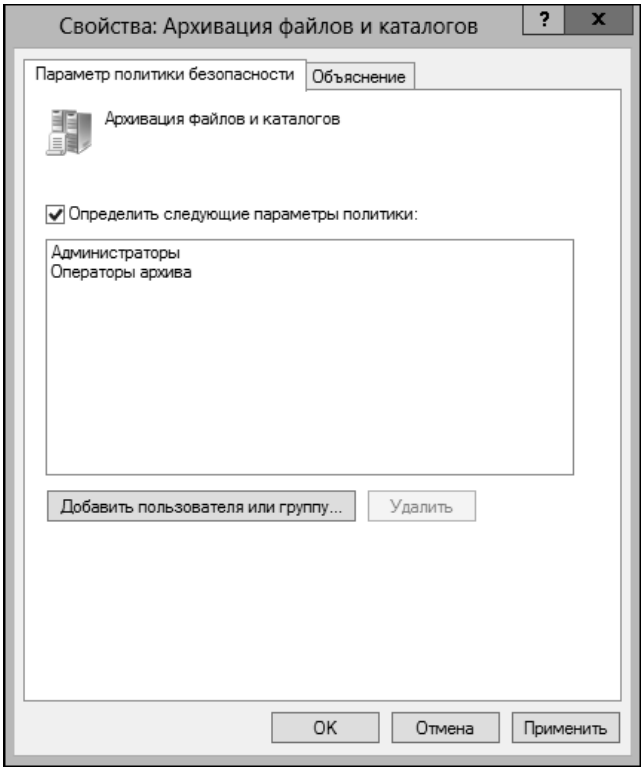


Рис. 8.4. Диалоговое окно свойств определяет право пользователя и затем применяет право к пользователям и группам

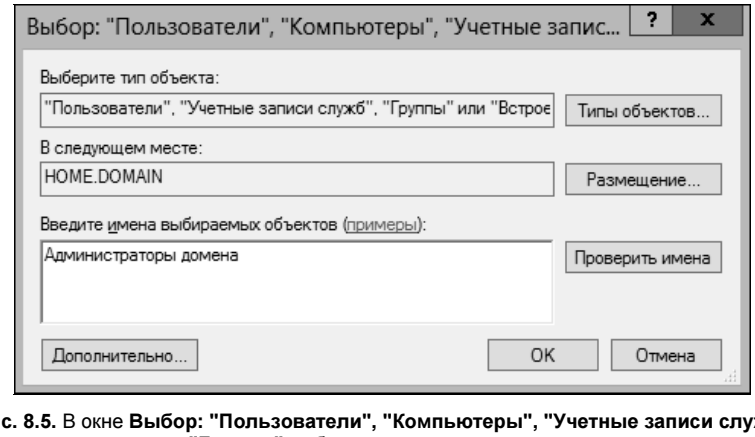


Рис. 8.5. В окне **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"** выберите пользователя или группу

зователи", "Компьютеры", "Учетные записи служб" или "Группы" (Select Users, Computers, Service Accounts, Or Groups), показанное на рис. 8.5.

> ***Внимание!***
>
> Брандмауэр Windows, запущенный на контроллере домена, может препятствовать использованию окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**. Это может произойти, когда администратор не зарегистрирован локально на контроллере домена и работает удаленно. Возможно, нужно настроить исключения на контроллере домена для входящего порта TCP 445. Это можно сделать, развернув узел **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена** (Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile). Далее в области деталей дважды щелкните по **Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования** (Windows Firewall: Allow Inbound Remote Administration Exception). Затем выберите значение **Включено** (Enabled). Альтернативно можно настроить исключение с помощью следующей команды в командной строке удаленного компьютера: `netsh firewall set portopening tcp 445 smb enable`. Для более подробной информации см. Microsoft Knowledge Base Article 840634 (**support.microsoft.com/default.aspx?scid=kb;en-us;840634**).

3. Введите имя пользователя или группы, которые нужно использовать, в предоставленное текстовое поле, а затем нажмите кнопку **Проверить имена** (Check Names). По умолчанию поиск производится по встроенным принципалам безопасности и учетным записям пользователей. Для добавления групп в поиск нажмите кнопку **Типы объектов** (Object Types), выберите элемент **Группы** (Groups) в списке и нажмите кнопку **OK**.
4. После того как выберете имена учетных записей или групп, нажмите кнопку **OK**. В окне **Добавление пользователя или группы** будет отображена выбранная учетная запись. Нажмите кнопку **OK** снова.
5. Окно **Свойства** будет обновлено в соответствии с произведенным выбором. Если была допущена ошибка, выберите имя и нажмите кнопку **Удалить** (Remove).
6. Как только будете готовы, нажмите кнопку **OK**.

Настройка локальных прав пользователей

Для локальных компьютеров можно применить права пользователя так:

1. Откройте окно **Свойства** для права пользователя (рис. 8.6). Запомните, что у политик сайта, домена и организационного подразделения есть приоритет над локальными политиками.
2. Окно **Свойства** показывает, каким пользователям и группам назначено право пользователя. Для удаления права пользователя выберите пользователя или группу и нажмите кнопку **Удалить** (Remove).
3. Можно применить право пользователя к дополнительным пользователям и группам, нажав кнопку **Добавить пользователя или группу**. Откроется окно **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"** (см. рис. 8.4). Теперь можно добавить пользователей или группы.

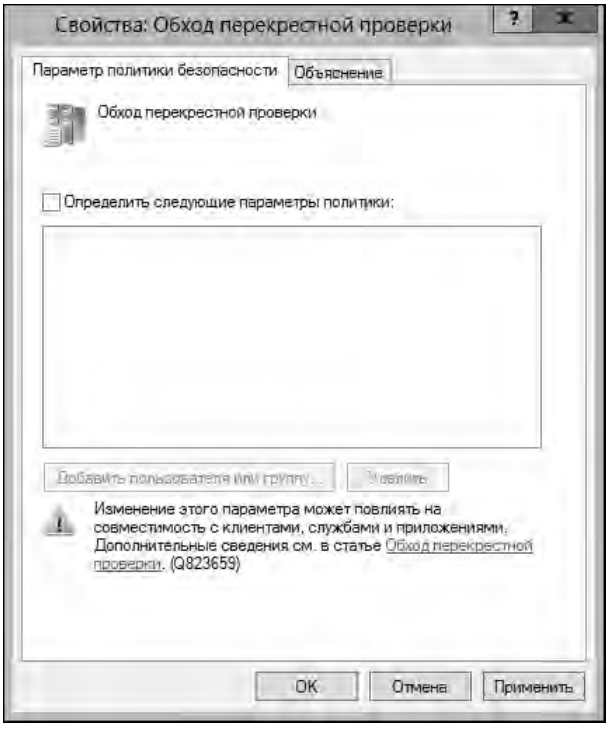


Рис. 8.6. В окне **Свойства** определите право для пользователей или групп. На контроллере домена невозможно отредактировать локальные права пользователей

Добавление учетной записи пользователя

Для каждого пользователя, которому необходим доступ к сетевым ресурсам, требуется создать учетную запись пользователя. Для создания учетных записей пользователей домена применяется оснастка **Active Directory — пользователи и компьютеры**. Локальные учетные записи пользователей можно создать с помощью утилиты **Локальные пользователи и группы**.

Создание учетных записей пользователей домена

Вообще говоря, можно создать новые учетные записи домена двумя способами.

- **Создать полностью новую учетную запись.** Щелкните правой кнопкой мыши по контейнеру, в который нужно поместить учетную запись, и выберите команду **Создать | Пользователь** (New | User). Откроется окно **Новый объект — Пользователь** (New Object — User Wizard), показанное на рис. 8.7. После создания новой учетной записи используются настройки по умолчанию.
- **Создать новую учетную запись на базе существующей учетной записи.** Щелкните на пользователе, которого нужно скопировать (в оснастке **Active Directory — пользователи и компьютеры**), и выберите команду **Копировать** (Copy). Откроется окно **Копировать объект — Пользователь** (Copy Object — User Wizard), которое очень похоже на окно **Новый объект — Пользователь**. Однако после создания копии учетной записи

новая учетная запись получит все настройки окружения существующей учетной записи. Более подробную информацию *см. в разд. "Копирование учетных записей пользователя домена" главы 9*.

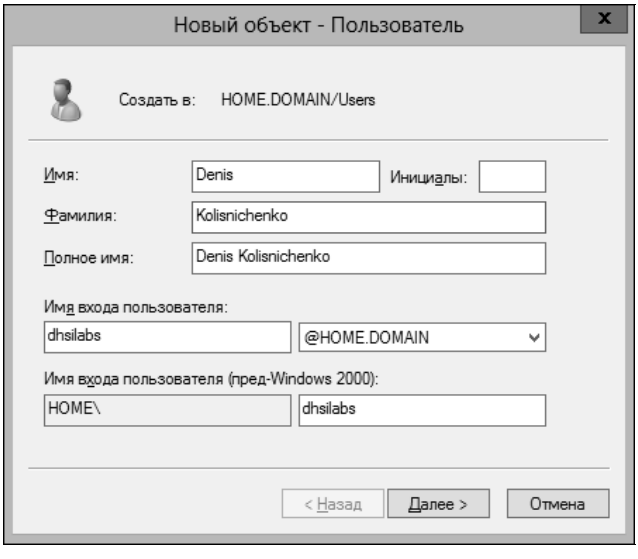


Рис. 8.7. Настройки имя входа и отображаемое имя пользователя

Используя окно **Новый объект — Пользователь** (New Object — User Wizard) или **Копировать объект — Пользователь** (Copy Object — User Wizard), можно создать учетную запись с помощью следующих действий:

1. Первые страницы мастера позволяют настроить отображаемое имя и имя входа (см. рис. 8.7). Введите имя, инициалы, фамилию пользователя в соответствующие текстовые поля. Эти текстовые поля используются для создания полного имени, которое и является отображаемым именем.
2. Вносить изменения в поле **Полное имя** (Full Name) не обязательно. Например, можно ввести имя в формате "Фамилия Имя Инициалы" или в формате "Имя Инициалы Фамилия". Полное имя должно быть уникальным в домене, максимальная длина — 64 символа.
3. В поле **Имя входа пользователя** (User Logon Name) введите имя входа. Используйте раскрывающийся список для выбора домена для ассоциации с ним. Это действие установит полное имя входа.
4. Первые 20 символов имени входа используются для установки имени входа в старом формате (для ОС, предшествовавших Windows 2000). Если необходимо, измените это имя входа.
5. Нажмите кнопку **Далее** и затем настройте пароль пользователя на следующей странице (рис. 8.8). Здесь можно установить такие параметры:
   - **Пароль** (Password) — пароль для учетной записи. Этот пароль должен соответствовать политике паролей;
   - **Подтверждение** (Confirm Password) — текстовое поле, позволяющее убедиться, что пароль был присвоен правильно. Просто повторно введите пароль, чтобы подтвердить его;

- **Требовать смены пароля при следующем входе в систему** (User Must Change Password At Next Logon) — если флажок установлен, пользователь должен изменить пароль сразу после входа в систему;
- **Запретить смену пароля пользователем** (User Cannot Change Password) — если флажок установлен, пользователь не сможет изменить пароль;
- **Срок действия пароля не ограничен** (Password Never Expires) — если флажок установлен, время действия пароля для этой учетной записи никогда не истекает. Эта установка переопределяет политику учетной записи домена. Неограниченный срок действия пароля — плохая идея, поскольку она не мотивирует пользователя изменять свой пароль;
- **Отключить учетную запись** (Account Is Disabled) — если флажок установлен, учетная запись будет отключена и не может использоваться. Установите эту опцию, чтобы временно запретить использование учетной записи.

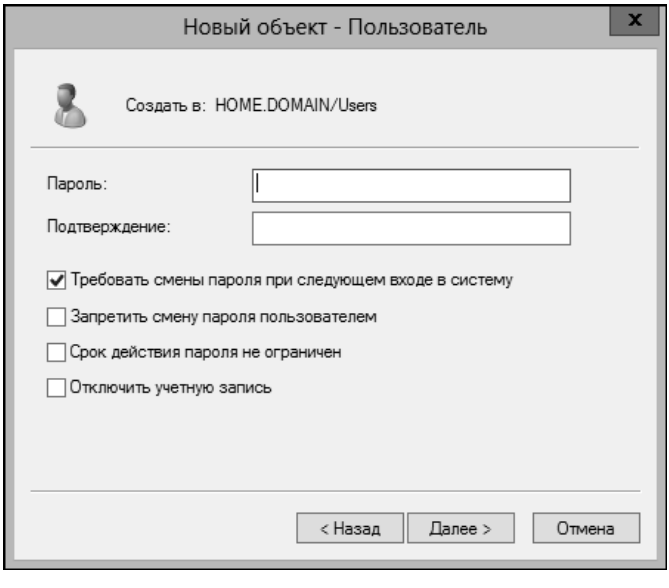


Рис. 8.8. Используйте окно **Новый объект — Пользователь** для настройки пароля

6. Нажмите кнопку **Далее**, а затем — кнопку **Готово** для создания учетной записи. Если есть проблемы с созданием учетной записи, просмотрите текст предупреждения, а затем используйте кнопку **Назад** (Back), чтобы повторно ввести информацию о пользователе и пароль, если это необходимо.

После создания учетной записи можно установить ее расширенные свойства, как будет показано далее в этой главе.

Создать учетные записи пользователя можно и средствами Центра администрирования Active Directory. Чтобы сделать это, выполните следующие действия:

1. В дереве консоли Центра управления Active Directory щелкните правой кнопкой мыши на контейнере, в который нужно поместить учетную запись пользователя, а затем выберите команду **Создать | Пользователь** (New | User). Откроется окно **Создать Пользователь** (Create User), изображенное на рис. 8.9.

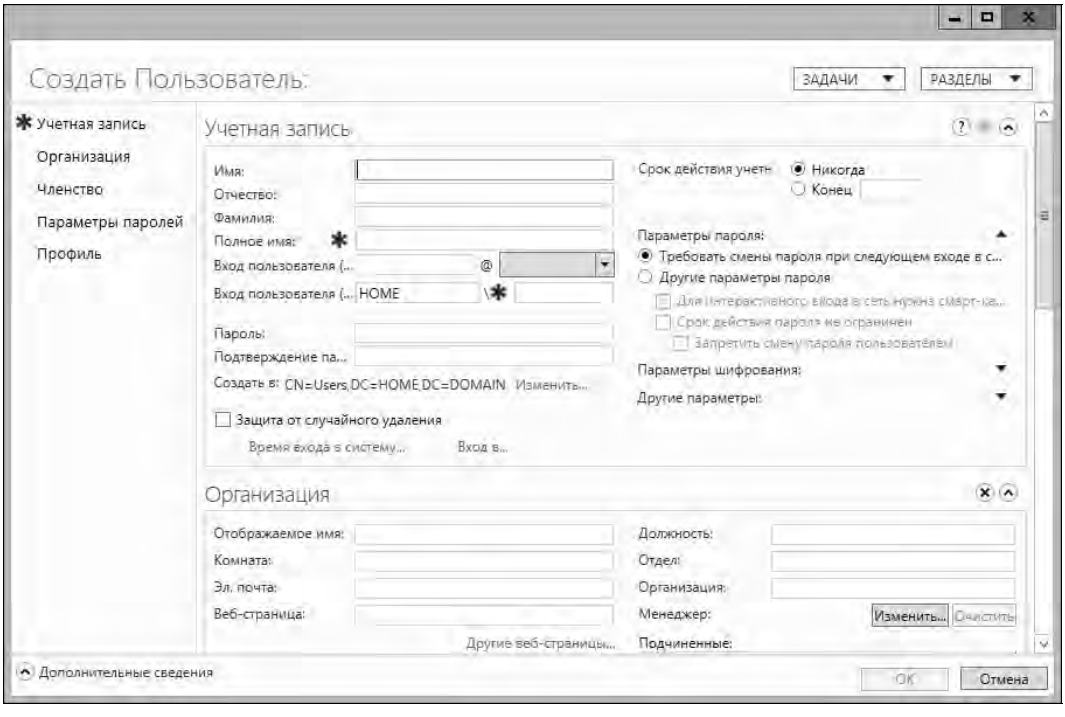


Рис. 8.9. Создание новой учетной записи в Центре администрирования Active Directory

2. Введите имя, отчество и фамилию в предоставленные текстовые поля. Эти текстовые поля используются для создания полного имени, которое также является отображаемым именем.

3. При необходимости внесите изменения в поле **Полное имя** (Full Name). Полное имя должно быть уникальным в пределах домена, максимальная длина — 64 символа.

4. В поле **Вход пользователя (UPN)** (User UPN Logon) введите имя входа пользователя. Из раскрывающегося списка выберите домен, с которым нужно связать учетную запись. Это действие установит полное имя входа.

5. Первые 20 символов имени входа используются для заполнения поля **Вход пользователя (SAMAccountName)** (User SamAccountName Logon). Это имя пользователя в старом формате (для ОС, предшествовавших Windows 2000), оно должно быть уникальным в пределах домена.

6. Все другие текстовые поля в окне являются необязательные. Установите и подтвердите пароль пользователя (при желании). Дополнительно установите флажок **Защита от случайного удаления** (Protect From Accidental Deletion), чтобы отметить учетную запись как защищенную в Active Directory. Защищенные учетные записи могут быть удалены только, если флаг защиты будет удален перед попыткой удаления учетной записи.

7. Нажмите кнопку **OK** для создания учетной записи пользователя.

Создание локальных учетных записей

Создать локальные учетные записи пользователей можно с помощью утилиты **Локальные пользователи и группы**. Открыть эту утилиту и создать учетную запись можно с помощью следующих действий:

1. В диспетчере серверов выберите команду **Средства** (Tools), а затем **Управление компьютером** (Computer Management). Либо можно нажать комбинацию клавиш <Windows>+<X> и выбрать из появившегося меню команду **Управление компьютером**.
2. Щелкните правой кнопкой мыши на записи **Управление компьютером** (Computer Management) в дереве консоли и выберите команду **Подключиться к другому компьютеру** (Connect To Another Computer). Теперь можно выбрать систему, локальными записями которой нужно управлять. У контроллеров домена нет локальных пользователей и групп.
3. В узле **Служебные программы** (System Tools) выберите узел **Локальные пользователи и группы**.
4. Щелкните правой кнопкой мыши на узле **Пользователи** (User), а затем выберите команду **Новый пользователь** (New User). Откроется одноименное диалоговое окно (рис. 8.10). Заполните следующие поля:
   - **Пользователь** (User Name) — имя входа для учетной записи, которое должно соответствовать политике для имен локальных пользователей;

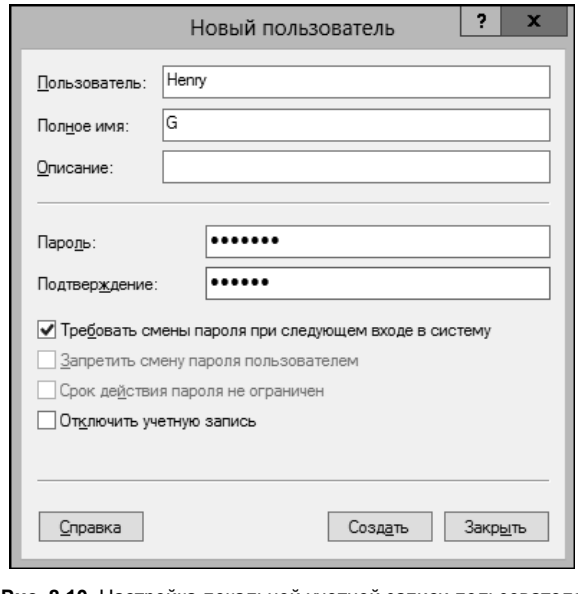


Рис. 8.10. Настройка локальной учетной записи пользователя отличается от настройки учетной записи пользователя домена

   - **Полное имя** (Full Name) — полное имя пользователя, например, William R. Stanek;
   - **Описание** (Description) — описание пользователя. Обычно это занимаемая пользователем должность, например веб-мастер. Также можно указать должность и отдел пользователя;

- **Пароль** (Password) — пароль для учетной записи, который должен соответствовать политике паролей;
- **Подтверждение** (Confirm Password) — поле, в котором повторяется пароль;
- **Требовать смены пароля при следующем входе в систему** (User Must Change Password At Next Logon) — если флажок установлен, пользователь должен изменить пароль сразу после входа в систему;
- **Запретить смену пароля пользователем** (User Cannot Change Password) — если флажок установлен, пользователь не сможет изменить пароль;
- **Срок действия пароля не ограничен** (Password Never Expires) — если флажок установлен, время действия пароля для этой учетной записи никогда не истекает. Эта установка переопределяет локальную политику учетной записи;
- **Отключить учетную запись** (Account Is Disabled) — если флажок установлен, учетная запись будет отключена и не может использоваться. Установите эту опцию, чтобы временно запретить использование учетной записи.

5. Нажмите кнопку **Создать** (Create), когда закончите настройку новой учетной записи.

Добавление учетной записи группы

Учетные записи групп применяются для управления привилегиями сразу для многих пользователей. Создать глобальные учетные записи групп можно в оснастке **Active Directory — пользователи и компьютеры**. Локальные учетные записи групп создаются в утилите **Локальные пользователи и группы**.

Если вы собираетесь создавать учетные записи группы, помните, что учетные записи групп обычно создаются для подобных типов пользователей. Следующие типы групп, возможно, придется создать.

- *Группы для подразделений в пределах организации* — в большинстве случаев пользователи, которые работают в одном отделе (подразделении), нуждаются в доступе к одним и тем же ресурсам. Часто нужно создавать группы, организованные по подразделению, например, **Отдел продаж**, **Маркетинг**, **Инженеры** и т. д.
- *Группы для определенных приложений* — пользователи часто нуждаются в доступе к приложению и ресурсам, относящимся к приложению. Если создать группу для приложения, можно быть уверены в том, что у пользователей есть соответствующий доступ к необходимым ресурсам и файлам приложения.
- *Группы для ролей в пределах организации* — также можно организовать группы по ролям пользователей в пределах организации. Например, руководители нуждаются в доступе к одним ресурсам, а супервизоры и обычные пользователи — к другим. Создавая группы на основе ролей в организации, можно убедиться, что вы предоставляете пользователям доступ, в котором они нуждаются.

Создание глобальной группы

Для создания глобальной группы выполните следующие действия:

1. Запустите оснастку **Active Directory — пользователи и компьютеры**, щелкните правой кнопкой мыши по контейнеру, в который нужно поместить группу, затем выберите команду **Создать | Группа** (New | Group). Откроется окно **Новый объект — Группа** (New Object — Group), показанное на рис. 8.11.

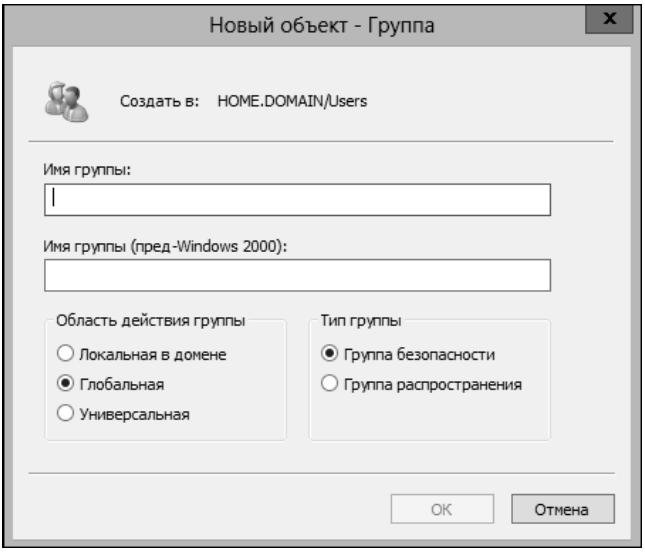


Рис. 8.11. Окно **Новый объект — Группа** позволяет добавить новую группу в домен

2. Введите имя группы. Имена учетных записей групп должны следовать тем же правилам имен, что и отображаемые имена учетных записей пользователей. Они не чувствительны к регистрам символов и могут быть длиной до 64 символов.
3. Первые 20 символов имени группы используются для установки имени группы в старом формате (для ОС, предшествовавших Windows 2000). Это имя группы должно быть уникальным в домене. Если необходимо, измените это старое имя группы.
4. Выберите область действия группы (**Локальная в домене** (Domain Local), **Глобальная** (Global), **Универсальная** (Universal)).
5. Выберите тип группы (**Группа безопасности** (Security), **Группа распространения** (Distribution)).
6. Нажмите кнопку **OK** для создания группы. После создания группы можно добавить членов группы и установить дополнительные свойства, как будет показано далее в этой главе.

Создать группы также можно с помощью Центра администрирования Active Directory. Для этого:

1. В консоли Центра администрирования Active Directory щелкните правой кнопкой мыши по контейнеру, в который нужно поместить группу. Выберите команду **Создать** на панели контейнера, а затем команду **Группа**. Откроется окно **Создать Группа** (Create Group), изображенное на рис. 8.12.
2. Введите имя группы. Имена глобальных групп должны следовать тем же правилам, что и отображаемые имена учетных записей пользователей. Они не чувствительны к регистру, а максимальная длина — до 64 символов.
3. Первые 20 символов имени группы используются для установки имени группы SAMAccountName. Это имя группы для ОС, предшествовавших Windows 2000, которое должно быть уникальным в домене.
4. Выберите тип группы (**Безопасность** (Security) или **Распространение** (Distribution)).

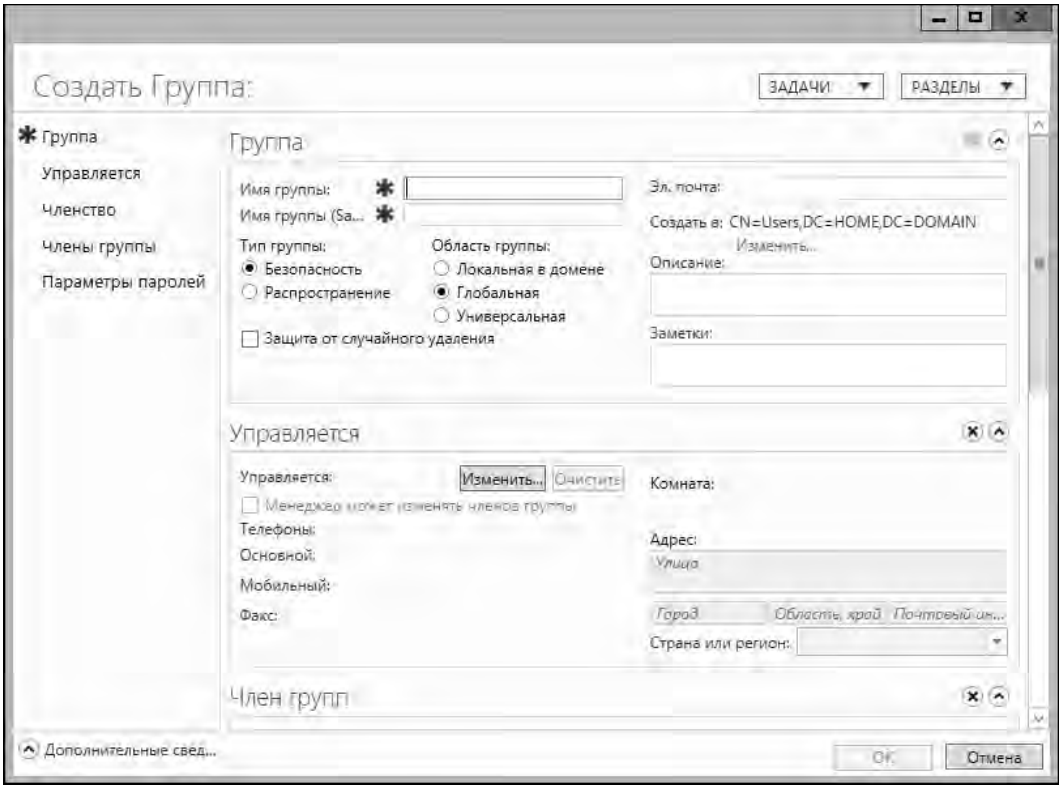


Рис. 8.12. Создание новой группы в Центре администрирования Active Directory

5. Выберите область группы (**Локальная в домене** (Domain Local), **Глобальная** (Global) или **Универсальная** (Universal)).
6. Все остальные параметры в диалоговом окне необязательны. Дополнительно установите флажок **Защита от случайного удаления** (Protect From Accidental Deletion), чтобы отметить эту учетную запись как защищенную в Active Directory. Защищенные учетные записи не могут быть удалены, пока флаг защиты не будет снят.
7. Нажмите кнопку **OK** для создания группы.

Создание локальной группы и назначение ее членов

Создать локальную группу можно с помощью утилиты **Локальные пользователи и группы**. Открыть ее и создать группу можно с помощью следующих действий:

1. В диспетчере серверов выберите команду **Средства**, а затем **Управление компьютером**. Щелкните правой кнопкой на записи **Управление компьютером** в дереве консоли и выберите команду **Подключиться к другому компьютеру**. Теперь можно выбрать систему, локальными записями которой нужно управлять. У контроллеров домена нет локальных пользователей и групп.
2. В узле **Служебные программы** (System Tools) выберите узел **Локальные пользователи и группы** (Local Users And Groups).

3. Щелкните правой кнопкой по элементу **Группы** (Groups), а затем выберите команду **Создать группу** (New Group). В результате будет отображено окно **Новая группа** (New Group), показанное на рис. 8.13.

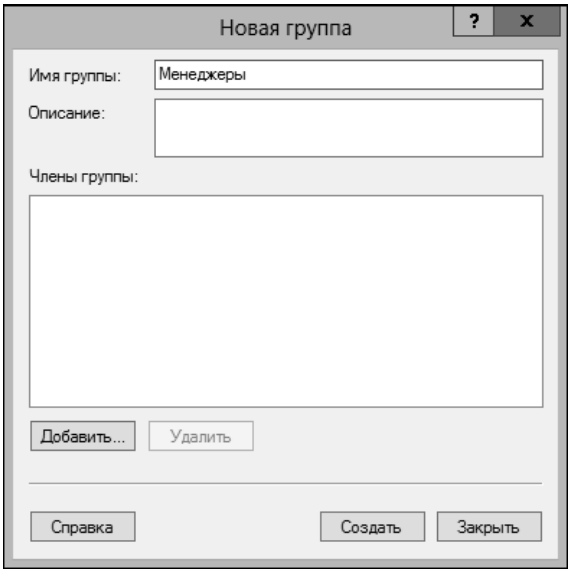


Рис. 8.13. В окне **Новая группа** можно добавить новую локальную группу в компьютер

4. После ввода имени и описания группы, нажмите кнопку **Добавить** для добавления имен пользователей в группу. Откроется окно **Выбор: "Пользователи"** (Select Users).
5. В окне **Выбор: "Пользователи"** введите имя пользователя и нажмите кнопку **Проверить имена**. Если совпадения будут найдены, выберите учетную запись, которую нужно использовать, и нажмите кнопку **OK**. Если совпадения не найдены, обновите введенное имя и повторите поиск. Повторите при необходимости этот шаг, а затем нажмите кнопку **OK**.
6. Окно **Новая группа** обновится, чтобы отразить сделанный выбор. Если была допущена ошибка, выберите имя и нажмите кнопку **Удалить**.
7. Нажмите кнопку **Создать** (Create), когда закончите добавлять или удалять членов группы.

Обработка членства глобальной группы

Для настройки членства в группе используется или оснастка **Active Directory — пользователи и компьютеры**, или Центр администрирования Active Directory. Когда работаете с группами, помните о следующем:

- все новые пользователи домена являются членами группы **Пользователи домена** (Domain Users), их основная группа указывается как **Пользователи домена**;
- все новые рабочие станции домена и рядовые серверы являются членами группы **Компьютеры домена** (Domain Computers), их основная группа — **Компьютеры домена**;
- все новые контроллеры домена становятся членами группы **Контроллеры домена** (Domain Controllers), их основная группа — **Контроллеры домена**.

Можно управлять членством в группе несколькими способами:

- индивидуально управлять членством в группе;
- множественно управлять членством в группе;
- установить основную группу для отдельных пользователей и компьютеров.

Индивидуальное управление членством в группе

Можно быстро добавить пользователя или группы в одну или более группу, щелкнув правой кнопкой мыши и выбрав команду **Добавить в группу** (Add To Group). Откроется окно **Выбор: "Группа"** (Select Groups). Далее можно выбрать группы, в которые нужно добавить выбранную учетную запись.

Управлять членством в группе для учетной записи любого типа можно так:

1. Дважды щелкните на пользователе, компьютере или группе в оснастке **Active Directory — пользователи и компьютеры** или в Центре администрирования Active Directory. Откроется окно **Свойства** учетной записи.
2. На вкладке или панели **Член групп** (Member Of) выбраны группы, членом которых является выбранная учетная запись. Нажмите кнопку **Добавить**, чтобы сделать учетную запись членом дополнительной группы. Откроется окно **Выбор: "Группа"** (Select Groups). Теперь можно выбрать группы членом которых должна стать учетная запись.
3. Для удаления учетной записи из группы выберите группу и затем нажмите кнопку **Удалить** (Remove).
4. Нажмите кнопку **OK**.

При работе исключительно с учетными записями пользователей можно добавить пользователей в группы так:

1. В оснастке **Active Directory — пользователи и компьютеры** или в Центре администрирования Active Directory выберите учетную запись пользователя, с которой нужно работать.

   Совет

   Для непоследовательного выбора нескольких учетных записей нажмите клавишу <Ctrl>, а затем с помощью левой кнопки мыши щелкните на каждой учетной записи пользователя, которые нужно выбрать. Для последовательного выбора учетных записей удерживайте клавишу <Shift> и выберите первую запись пользователя, а затем — последнюю учетную запись.

2. Щелкните правой кнопкой на выбранном пользователе (или пользователях), выберите команду **Добавить в группу** (Add To A Group). Откроется окно **Выбор: "Группа"** (Select Groups). Теперь можно выбрать группы, членом которых должна стать выбранная учетная запись.
3. Нажмите кнопку **OK**.

Множественное управление членством в группе

Другой способ управления членством в группе — использовать окно **Свойства** для добавления или удаления сразу множества учетных записей. Для этого выполните следующие действия:

1. Дважды щелкните на записи группы в оснастке **Active Directory — пользователи и компьютеры** или в Центре управления Active Directory. Откроется окно **Свойства**.

2. На вкладке или панели **Члены группы** (Members Of) показаны текущие члены группы в алфавитном порядке. Чтобы добавить учетные записи в группу, нажмите кнопку **Добавить**. Откроется окно **Выбор: "Пользователи", "Контакты", "Компьютеры", "Учетные записи служб" или "Группы"** (Select Users, Computers, Service Accounts, Or Groups). Теперь можно выбрать пользователей, компьютеры, учетные записи службы или группы, которые должны быть членами выбранной в данный момент группы.
3. Для удаления членов из группы выберите учетную запись и нажмите кнопку **Удалить**.
4. Нажмите кнопку **OK**.

Установка основной группы для отдельных пользователей и компьютеров

Пользователи, получающие доступ к Windows Server через **Службы для Macintosh** (Services for Macintosh), используют основные группы. Когда пользователь Macintosh создает файлы или каталоги в системе, работающей под управлением Windows Server, этим файлам и каталогам назначаются основные группы.

> ***Примечание***
>
> Windows Server 2008 и более поздние версии не содержат **Службы для Macintosh**. Этот компонент имеется только в ранних версиях Windows Server. У всех учетных записей пользователей и компьютеров, которые получают доступ к Windows Server через Macintosh, должна быть основная группа, причем с глобальной или универсальной областью действия, например, **Пользователи домена** или **Компьютеры домена**.

Для установки основной группы выполните следующие действия:

1. Дважды щелкните на записи пользователя или компьютера в оснастке **Active Directory — пользователи и компьютеры** или в Центре администрирования Active Directory. Откроется окно **Свойства**.
2. На панели или вкладке **Член группы** выберите глобальную или универсальную группу из области **Член групп**.
3. Нажмите кнопку **Задать основную группу** (Set Primary Group).

Все пользователи должны быть членом как минимум одной основной группы. Нельзя отозвать членство из основной группы без предварительного назначения другой основной группы пользователя. Чтобы сделать это, выполните следующие действия:

1. Выберите другую глобальную или универсальную группу в списке **Член групп** и нажмите кнопку **Задать основную группу**.
2. В списке **Член групп** выделите предыдущую основную группу и нажмите кнопку **Удалить**. Членство в группе будет отозвано.

Реализация управляемых учетных записей

Microsoft Exchange Server, Internet Information Services, SQL Server и другие типы приложений используют служебные учетные записи. На локальном компьютере можно настроить приложения для запуска от имени встроенной учетной записи пользователя, например, Local Service, Network Service или Local System. Хотя эти служебные учетные записи легко настроить и использовать, они обычно нужны множеству приложений и служб и не управляемы на уровне домена. Если приложение настроено использовать учетную запись домена,

можно изолировать привилегии для приложения, но затем нужно вручную управлять паролем учетной записи и именами SPN, необходимыми для аутентификации Kerberos.

Windows 7 и все более поздние выпуски Windows поддерживают два дополнительных типа учетных записей:

- управляемые служебные учетные записи;
- управляемые виртуальные учетные записи.

Управляемые служебные учетные записи — специальный тип учетной записи пользователя домена для управляемых служб. Эти учетные записи уменьшают приостановки обслуживания и другие проблемы, поскольку Windows автоматически управляет паролями и соответственными SPN.

Управляемые виртуальные учетные записи — специальный тип учетных записей локальных компьютеров для управляемых служб. Эти учетные записи предоставляют возможности доступа к сети с идентификационными данными компьютера в среде домена. Поскольку используются идентификационные данные компьютера, управление паролями не требуется.

Управлять этими учетными записями можно посредством модуля Active Directory для Windows PowerShell. Поскольку модуль Active Directory не импортируется в Windows PowerShell по умолчанию, нужно импортировать эту модель перед использованием предоставляемых ним командлетов. Поддержка управляемых служебных учетных записей есть в Windows 8 и Windows Server 2012, однако ее нет в Windows 7 и Windows Server 2008 R2. Групповые управляемые учетные записи службы обеспечивают ту же функциональность, что и стандартные управляемые учетные записи службы, но расширяют функциональность на множество серверов. Например, когда клиентский компьютер соединяется со службой, размещенной на ферме серверов, взаимная аутентификация не может быть успешно выполнена, если все экземпляры служб не используют один и тот же принципал. С помощью групповой управляемой учетной записи службы администратор позволяет каждому серверу в ферме использовать один и тот же принципал службы, которым управляет сама Windows, а не администратор.

Групповые управляемые учетные записи службы, фактически, являются типом учетной записи службы по умолчанию в Windows 8 и Windows Server 2012. Из-за этого управляемые учетные записи службы могут охватить множество компьютеров по умолчанию. Это означает, что можно добавить учетную запись на несколько компьютеров за один раз при необходимости поддержки узлов кластера, фермы серверов балансировки сетевой нагрузки и т. д. Если нужно ограничить управляемую учетную запись службы единственным компьютером, необходимо использовать опцию `-RestrictToSingleComputer` при создании учетной записи. Не забывайте, что у одного компьютера может быть несколько управляемых учетных записей служб.

В схеме Active Directory управляемые учетные записи служб представлены объектом `msDS-ManagedServiceAccounts`. Этот класс объекта наследует свои атрибуты из объекта класса `Computer`, но объекты также являются пользователями. Управляемые учетные записи служб используют такой же механизм обновления пароля, как и обычные учетные записи компьютера. Это означает, что пароль учетной записи обновляется при обновлении пароля компьютера, которое по умолчанию происходит каждые 30 дней. Управляемые учетные записи служб могут автоматически обслуживать свои Kerberos SPN и поддерживают делегацию.

> ***Совет***
>
> Некоторые приложения, например SQL Server и IIS, широко используют Kerberos и знают, как зарегистрировать себя с SPN. Если приложение поддерживает написание собственных SPN, управляемые учетные записи будут учитывать автоматическое управление SPN.

Примечание

По умолчанию все управляемые учетные записи служб создаются в контейнере Managed Service в Active Directory. Этот контейнер отображается в оснастке **Active Directory — пользователи и компьютеры** при включении отображения расширенных функций.

Подобно учетным записям компьютера, управляемые учетные записи служб не используют политики паролей. Вместо этого они используют случайным образом сгенерированные 240-байтные (120-символьные) пароли. Управляемые учетные записи служб не могут выполнить интерактивный вход в систему или быть заблокированы, как учетные записи пользователей. Можно добавить управляемые учетные записи службы в группы, используя оснастку **Active Directory — пользователи и компьютеры**.

Создание и использование управляемых учетных записей служб

Управляемые учетные записи служб — это учетные записи, сохраняемые по умолчанию в контейнере **Managed Service Accounts** в Active Directory. Далее, нужно ассоциировать учетную запись с компьютером в Active Directory и затем установить управляемую учетную запись службы на локальный сервер для добавления ее в учетную запись как локального пользователя. Останется настроить локальную службу для использования учетной записи. Другими словами, нужно сделать следующее:

1. Создать управляемую учетную запись службы.
2. Ассоциировать учетную запись с компьютером в Active Directory.
3. Установить управляемую учетную запись службы на компьютер, который был ассоциирован.
4. Настроить локальную службу для использования учетной записи.

Можно использовать командлеты Windows PowerShell для установки, удаления и сброса паролей управляемых учетных записей служб (далее УУЗС). После установки УУЗС можно настроить службу или приложение для использования учетной записи, после этого нельзя указать или изменить пароли, поскольку пароль учетной записи обслуживается компьютером. Также можно настроить SPN учетной записи службы без привилегий администратора домена.

Создать УУЗС можно с использованием командлета New-ADServiceAccount. Базовый синтаксис следующий:

```
New-ADServiceAccount -DisplayName DisplayName -SamAccountName SAMName -Name Name
[-RestrictToSingleComputer]
```

Здесь *DisplayName* — отображаемое имя для учетной записи; *SAMName* — имя в формате ОС, предшествовавших Windows 2000, для учетной записи; *Name* — имя учетной записи. Например:

```
New-ADServiceAccount -DisplayName "SQL Agent Account" -SamAccountName sqlagent -Name
"SQL Agent"
```

По умолчанию учетная запись будет создана как учетная запись группы. У нее будет случайным образом сгенерированный 240-байтный (120-символьный) пароль, и она будет создана в контейнере **Managed Service Accounts**. По умолчанию учетная запись будет включена, но можно создать ее в выключенном состоянии, добавив параметр `-Enabled $false`. Если нужно передать учетные данные для создания учетной записи, используйте параметр `-Credential`, как показано в этом примере:

```
$cred = Get-Credential New-ADServiceAccount –DisplayName "IIS App Pool 1"
–SamAccountName pool1 –Name "IIS Pool 1" –Credential $cred
```

Хотя учетная запись отображается в оснастке **Active Directory — пользователи и компьютеры**, не нужно использовать эту утилиту для работы с учетной записью. Вместо этого необходимо использовать командлеты Windows PowerShell:

- Get-ADServiceAccount — для получения информации об одной или нескольких УУЗС;
- Set-ADServiceAccount — для установки свойств существующей УУЗС;
- Remove-ADServiceAccount — для удаления УУЗС из Active Directory.

После создания управляемой учетной записи службы в Active Directory нужно ассоциировать ее с целевым компьютером в Active Directory посредством командлета Add-ADComputerServiceAccount. Используйте командлет Remove-ADComputerServiceAccount для удаления ассоциации компьютера из Active Directory.

Базовый синтаксис для Add-ADComputerServiceAccount следующий:

```
Add-ADComputerServiceAccount [-Identity] ComputerName [-ServiceAccount] MSAName
```

Здесь *ComputerName* — имя целевого компьютера, *MSAName* — имя управляемой учетной записи службы, например:

```
Add-ADComputerServiceAccount IISServer84 WebServicesAccount
```

Если нужно передать учетные данные для создания учетной записи, используйте параметр `-Credential`, как показано в этом примере:

```
$cred = Get-Credential Add-ADComputerServiceAccount IISServer32
FarmFourServicesAccount
```

Можно установить учетную запись на локальном компьютере с помощью командлета Install-ADServiceAccount. Базовый синтаксис следующий:

```
Install-ADServiceAccount [-Identity] ServiceAccountId
```

Здесь *ServiceAccountID* — отображаемое имя или SAM-имя учетной записи службы, например:

```
Install-ADServiceAccount sqlagent
```

Если нужно передать учетные данные для создания учетной записи, используйте параметр `-Credential`. Используйте командлет Uninstall-ADServiceAccount для удаления учетной записи.

Настройка служб на использование управляемых учетных записей служб

Для настройки службы с целью запуска с управляемой учетной записью службы выполните следующие действия:

1. В диспетчере серверов в меню **Средства** выберите команду **Управление компьютером**.
2. При необходимости подключитесь к компьютеру, которым нужно управлять. Щелкните правой кнопкой на записи **Управление компьютером** в дереве консоли и затем выберите команду **Подключиться к другому компьютеру**. Введите имя узла, полное доменное имя или IP-адрес удаленного сервера, а затем нажмите кнопку **OK**.

3. На левой панели разверните узел **Службы и приложения** (Services and Applications), а затем выберите узел **Службы** (Services).
4. Щелкните правой кнопкой мыши по службе, с которой нужно работать, и затем выберите команду **Свойства**.
5. На вкладке **Вход в систему** (Log On) установите переключатель **С этой учетной записью** (This Account) и введите имя управляемой учетной записи в формате *ИмяДомена\ИмяУчетнойЗаписи* или нажмите кнопку **Обзор** для поиска учетной записи.
6. Подтвердите, что поле пароля остается пустым, и нажмите кнопку **OK**.
7. Выберите имя службы и нажмите кнопку **Запуск службы** (Start) для запуска службы или **Перезапуск службы** (Restart) для перезапуска службы соответственно. Обратите внимание, что в колонке **Вход от имени** (Log On As) отображается только что настроенное имя учетной записи.

> ***Примечание***
>
> В оснастке **Службы** (Services) в конце имени учетной записи появляется знак доллара ($). При использовании этой оснастки право входа **Вход в качестве службы** (Service Logon Right) устанавливается автоматически для учетной записи. При использовании другой утилиты нужно явно предоставить это право.

Удаление управляемых учетных записей служб

Если управляемая учетная запись службы больше не используется на компьютере, ее нужно удалить. Перед этим, однако, следует проверить оснастку **Службы** и убедиться, что учетная запись не используется. Для удаления УУЗС с локального компьютера используйте командлет Uninstall-ADServiceAccount. Базовый синтаксис таков:

```
Uninstall-ADServiceAccount -Identity ServiceAccountId
```

Здесь *ServiceAccountID* — отображаемое имя или имя SAM учетной записи службы, например:

```
Uninstall-ADServiceAccount -Identity sqlagent
```

Если нужно передать учетные данные для удаления учетной записи, используйте параметр `-Credential`.

Пароли УУЗС сбрасываются в обычном порядке на основе требований сброса пароля домена, но можно сбросить пароль вручную, если нужно. Чтобы сбросить пароль для управляемой учетной записи службы, используйте командлет Reset-ADServiceAccountPassword. Основной синтаксис такой:

```
Reset-ADServiceAccountPassword -Identity ServiceAccountId
```

Здесь *ServiceAccountID* — отображаемое имя или имя SAM учетной записи службы, например:

```
Reset-ADServiceAccountPassword -Identity sqlagent
```

Если нужно передать учетные данные для удаления учетной записи, используйте параметр `-Credential`. Изменить интервал изменения пароля по умолчанию для управляемой учетной записи можно с использованием политики **Член домена: максимальный срок действия пароля учетных записей компьютера** (Domain Member: Maximum Machine Account Password Age), которая находится в узле **Локальные политики\Параметры безопасности**

(Local Policy\Security Options). Ни групповая политика **Политики учетных записей\ Политика паролей** (Account Policies\Password Policy), ни команда `NLTEST /SC_CHANGE_PWD`, не может сбросить пароль управляемой учетной записи службы.

Перемещение управляемых учетных записей служб

Для перемещения учетной записи службы с одного компьютера на другой нужно сделать следующее:

1. На исходном компьютере настройте все службы, которые используют управляемую учетную запись, на использование другой учетной записи, а затем выполните командлет Uninstall-ADServiceAccount.
2. На компьютере-назначении выполните командлет Install-ADServiceAccount, а затем используйте оснастку **Службы** для настройки службы, которая будет запускаться от имени этой учетной записи.

Для миграции службы из учетной записи пользователя в управляемую учетную запись службы нужно выполнить следующее:

1. Создайте новую управляемую учетную запись в Active Directory, используя командлет New-ADServiceAccount.
2. Установите УУЗС на соответствующий компьютер, используя командлет Install-ADServiceAccount, а затем запустите оснастку **Службы** для настройки службы, которая будет выполняться от имени управляемой учетной записи службы.
3. Также нужно настроить списки управления доступом на ресурсах службы для УУЗС.

Использование виртуальных учетных записей

Виртуальные учетные записи практически не требуют администрирования. Они не могут быть созданы или удалены, они не требуют управления паролями. Вместо этого они существуют автоматически и представлены идентификационными данными машины локального компьютера.

С виртуальными учетными записями можно настроить доступ локальной службы к сети с учетными данными компьютера в окружении домена. Поскольку используются учетные записи компьютера, не нужно создавать учетные записи и управлять паролями.

Настроить службу для запуска с виртуальной учетной записью можно с помощью следующих действий:

1. В диспетчере серверов в меню **Средства** выберите команду **Управление компьютером**.
2. При необходимости подключитесь к компьютеру, которым нужно управлять. Щелкните правой кнопкой на записи **Управление компьютером** в дереве консоли и затем выберите команду **Подключиться к другому компьютеру**. Введите имя узла, полное доменное имя или IP-адрес удаленного сервера, а затем нажмите кнопку **OK**.
3. На левой панели разверните узел **Службы и приложения**, а затем выберите узел **Службы**.
4. Щелкните правой кнопкой мыши по службе, с которой нужно работать, и выберите команду **Свойства**.
5. На вкладке **Вход в систему** (Log On) установите переключатель **С этой учетной записью** (This Account) и введите имя управляемой учетной записи в формате *СЛУЖБА\ ИмяКомпьютера*.

6. Подтвердите, что поле пароля остается пустым, и нажмите кнопку **OK**.
7. Выберите имя службы и нажмите кнопку **Запуск службы** для запуска службы или **Перезапуск службы** для перезапуска службы соответственно. Обратите внимание, что в колонке **Вход от имени** отображается только что настроенное имя учетной записи.

Примечание

В оснастке **Службы** в конце имени учетной записи появляется знак доллара ($). При использовании этой оснастки право входа **Вход в качестве службы** устанавливается автоматически для учетной записи. При использовании других утилит это право нужно предоставить самостоятельно.

ГЛАВА 9

Управление учетными записями пользователя и группы

Идеально, когда можно создать учетные записи пользователя и группы и забыть о них. К сожалению, мы живем в реальном мире. После создания учетных записей нужно потратить много времени на управление ими. В этой главе приведены инструкции и рекомендации, позволяющие облегчить эту задачу.

Управление контактной информацией пользователя

Active Directory — это служба каталогов. Учетные записи пользователей обладают подробной контактной информацией. Контактная информация доступна всем в дереве доменов или лесу — при поиске пользователей и создании записей адресной книги.

Установка контактной информации

Установить контактную информацию в оснастке **Active Directory — пользователи и компьютеры** можно с помощью следующих действий:

1. Дважды щелкните по имени пользователя в оснастке **Active Directory — пользователи и компьютеры**. Откроется окно **Свойства**.
2. Перейдите на вкладку **Общие** (General) (рис. 9.1), где представлена общая информация о пользователе:
   - **Имя** (First Name), **Инициалы** (Initials), **Фамилия** (Last Name) — полное имя пользователя;
   - **Выводимое имя** (Display Name) — отображаемое в сеансах входа и в Active Directory имя пользователя;
   - **Описание** (Description) — описание пользователя;
   - **Комната** (Office) — комната пользователя;
   - **Номер телефона** (Telephone Number) — основной деловой номер телефона. Если у пользователя есть несколько номеров, нажмите кнопку **Другой** (Other) и задайте дополнительные номера телефона в окне **Номер телефона (прочие)** (Phone Number (Others));
   - **E-mail** — корпоративный e-mail пользователя;

- **Веб-страница** (Web Page) — веб-страница пользователя, которая может находиться либо в Интернете, либо в корпоративной сети. Если у пользователя несколько страниц, нажмите кнопку **Другой** (Other) и в окне **Адрес страницы в Интернете (прочие)** (Web Page Address (Others)) введите дополнительные адреса страниц.

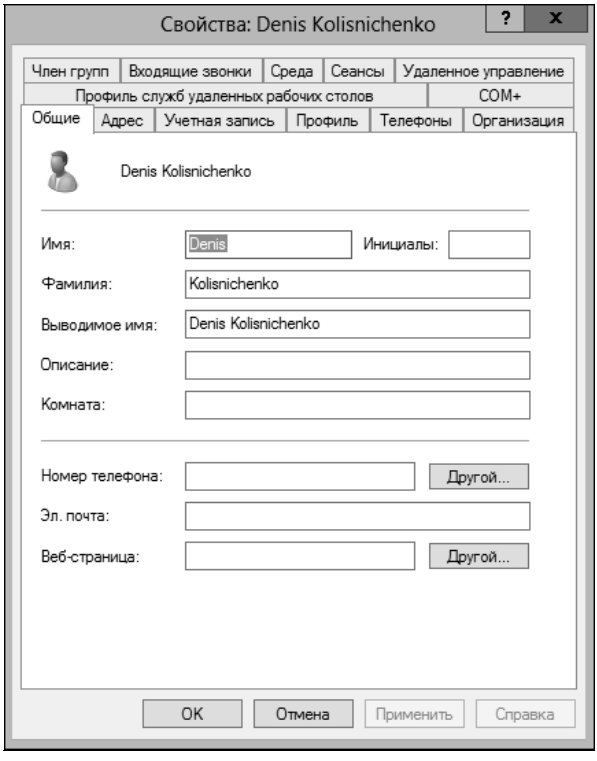


Рис. 9.1. Настройте общую контактную информацию на вкладке **Общие**

Совет

Устанавливать e-mail и веб-страницу нужно только в случае, если требуется использовать команды **Отправить почту** (Send Mail) и **Открыть домашнюю** (Open Home Page) страницу в оснастке **Active Directory — пользователи и компьютеры**. Для получения более подробной информации *см. разд. "Обновление учетных записей пользователя и группы" далее в этой главе*.

3. Перейдите на вкладку **Адрес** (Address). Установите деловой или домашний адрес пользователя. Обычно нужно вводить деловой адрес, поскольку придется отслеживать именно деловой адрес и деловой e-mail (чтобы знать, в каком офисе пользователь находится физически).

Примечание

Перед вводом домашнего адреса пользователя убедитесь, что не нарушаете закон "О персональных данных". Лучше обсудить это с отделом кадров или юридическим отделом, а также получить личное разрешение пользователя на ввод его домашнего адреса.

4. Перейдите на вкладку **Телефоны** (Telephones). Введите номера основных телефонов, по которым можно связаться с пользователем — домашний, пейджер, мобильный, факс и IP-телефон.

5. Для каждого типа телефонного номера можно указать дополнительные номера, нажав кнопку **Другой**. После этого нужно ввести номера телефонов в соответствующие поля.
6. Теперь перейдите на вкладку **Организация** (Organization). Введите должность пользователя, названия отдела и организации.
7. Чтобы указать руководителя пользователя, нажмите кнопку **Изменить** (Change), а затем выберите пользователя в окне **Выбор: "Пользователь" или "Контакт"** (Select User or Contact). После определения руководителя для пользователя в свойствах учетной записи руководителя имя пользователя будет приведено в области **Прямые подчиненные** (Direct reports).
8. Нажмите кнопку **OK** или кнопку **Применить** (Apply) для сохранения изменений.

Также можно ввести контактную информацию с помощью утилиты Центр администрирования Active Directory. Дважды щелкните на учетной записи пользователя. В окне **Свойства** нажмите кнопку **Организация** (Organization) для отображения одноименной панели. Как показано на рис. 9.2, здесь, на одной панели, можно задать общую контактную информацию, телефоны, адрес и информацию об организации.

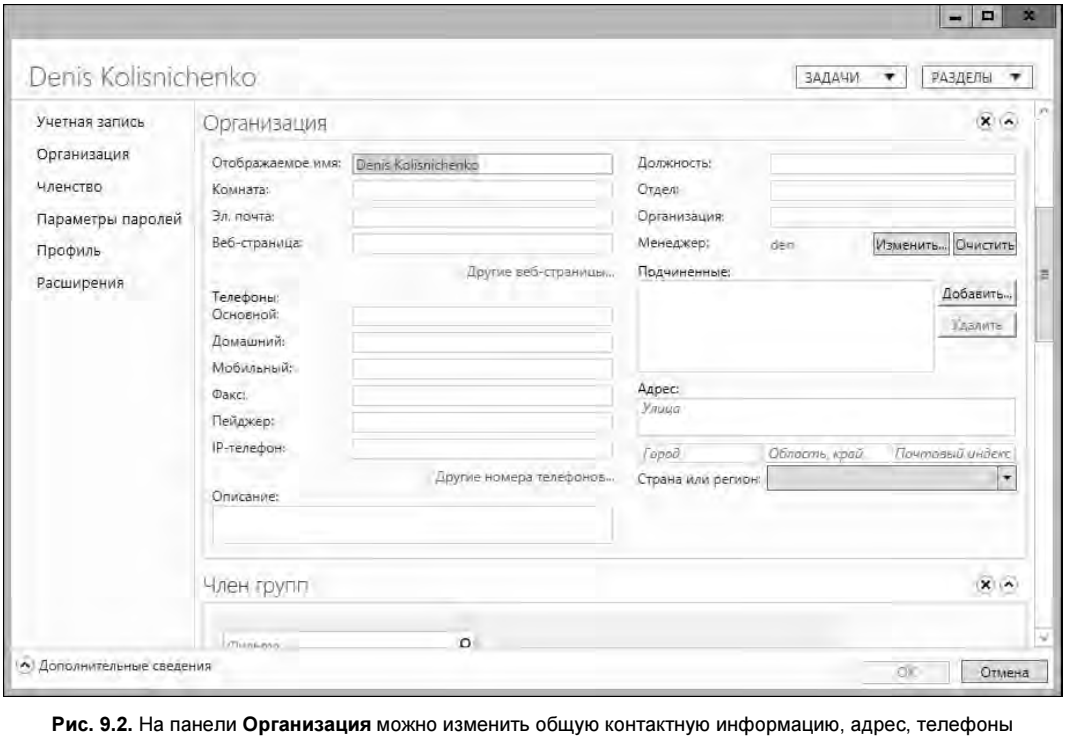


Рис. 9.2. На панели **Организация** можно изменить общую контактную информацию, адрес, телефоны и информацию об организации

В поле **Веб-страница** указывается домашняя страница пользователя, которая может быть либо в Интернете, либо в корпоративной сети. Если у пользователя есть несколько веб-страниц, щелкните по ссылке **Другие веб-страницы** (Other Web Pages) и введите дополнительные адреса в окне **Адрес веб-страницы (другие)** (Web Page Address (Others)).

В области **Телефоны** (Phone Numbers) можно ввести номера телефонов пользователя — основной, домашний, мобильный, факс, пейджер, IP-телефонов. Также можно настроить

дополнительные номера телефонов. Щелкните по ссылке **Другие номера телефонов** (Other Phone Numbers) и укажите дополнительные номера в предоставленном окне.

Если у пользователя есть руководитель, он будет отображен в поле **Менеджер** (Manager). Если менеджер не установлен или нужно его изменить, нажмите кнопку **Изменить** (Change) для выбора пользователя в окне **Выбор: "Пользователь" или "Контакт"**. После определения руководителя для пользователя, в свойствах учетной записи руководителя имя пользователя будет приведено в поле **Подчиненные** (Direct Reports).

Если у пользователя есть подчиненные, они будут отображены в поле **Подчиненные**. Добавлять и удалять подчиненных можно с помощью кнопок **Добавить** и **Удалить**. Чтобы добавить подчиненного, нажмите кнопку **Добавить**, а затем выберите пользователя в окне **Выбор: "Пользователь" или "Контакт"** и нажмите кнопку **OK**. Чтобы удалить подчиненного, выделите его и нажмите кнопку **Удалить**.

Поиск пользователей и групп в Active Directory

Active Directory позволяет легко найти учетные записи пользователей и групп в каталоге с помощью следующих действий:

1. В оснастке **Active Directory — пользователи и компьютеры** щелкните правой кнопкой мыши по домену или контейнеру, а затем выберите команду **Найти** (Find).
2. В окне **Поиск: Пользов., контакты и группы** (Find Users, Contacts, And Groups) список **Где** (In) содержит ранее выбранный домен или контейнер. Если нужно произвести поиск по всему каталогу, выберите из этого списка элемент **В Active Directory** (Entire Directory) или нажмите кнопку **Обзор** для выбора домена или контейнера.

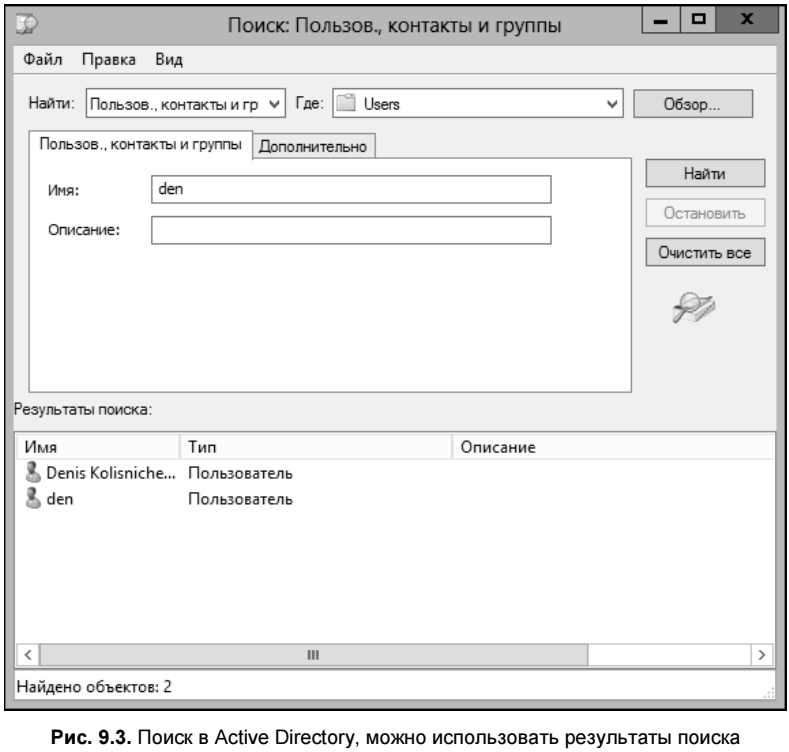


Рис. 9.3. Поиск в Active Directory, можно использовать результаты поиска для создания записей в адресной книге

3. На вкладке **Пользов., контакты и группы** (Users, Contacts, And Groups) введите имя пользователя, контакта или группы, которые нужно найти.
4. Нажмите кнопку **Найти** (Find Now) для начала поиска. Если будут найдены совпадения, будут отображены результаты поиска (рис. 9.3). В противном случае измените параметры и повторите поиск.
5. Для управления учетной записью щелкните по ней правой кнопкой мыши. Если щелкнуть по учетной записи правой кнопкой мыши и выбрать команду **Свойства**, откроется окно **Свойства**.

Также можно произвести поиск пользователей и групп, используя фильтр и функции глобального поиска утилиты Центр администрирования Active Directory. Для получения более подробной информации *см. разд. "Центр администрирования Active Directory и Windows PowerShell" главы 7*.

Настройка параметров среды пользователя

Учетные записи пользователей также обладают профилями, сценариями входа и домашними каталогами, связанными с ними. Для настройки этих необязательных параметров дважды щелкните по отображаемому имени пользователя в оснастке **Active Directory — пользователи и компьютеры**, а затем перейдите на вкладку **Профиль** (рис. 9.4).

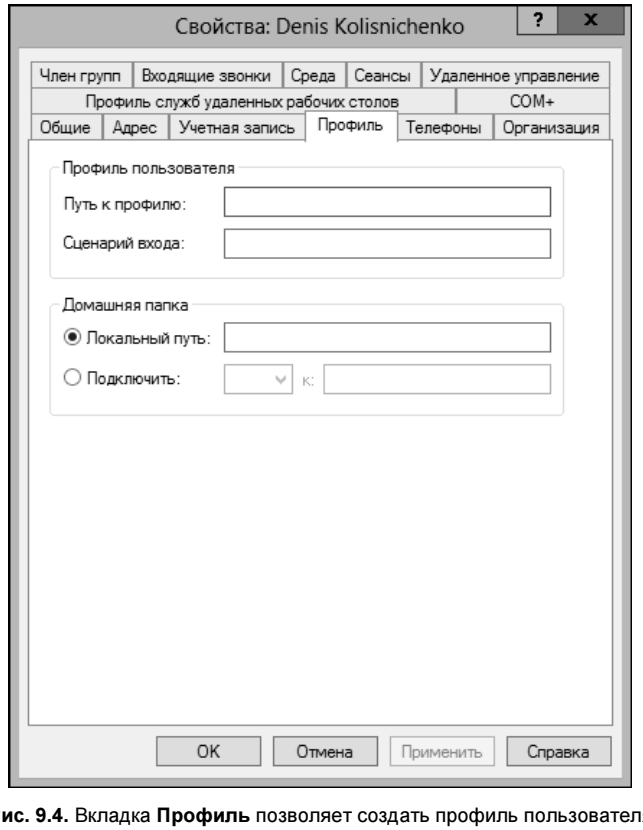


Рис. 9.4. Вкладка **Профиль** позволяет создать профиль пользователя и таким образом настроить среду пользователя

На вкладке **Профиль** (Profile) можно установить следующие параметры.

- **Путь к профилю** (Profile Path) — путь к профилю пользователя. Профили содержат параметры среды для пользователя. При каждом входе пользователя в компьютер профиль пользователя используется для определения параметров рабочего стола и Панели управления, доступности меню и приложений и т. д. Установка пути к профилю описана в *разд. "Управление профилями пользователей" далее в этой главе.*
- **Сценарий входа** (Logon Script) — путь к сценарию входа пользователя. Сценарии входа — это командные файлы, которые запускаются при входе в систему. Сценарии входа используются для выполнения команд при каждом входе пользователя в систему. Сценарии входа были рассмотрены в *главе 4*.
- **Домашняя папка** (Home Folder) — каталог, в котором пользователь должен хранить файлы. Здесь можно задать определенный каталог для файлов пользователя, это может быть как локальный каталог, так и каталог на подключенном сетевом диске. Если каталог доступен в сети, то пользователь может получить доступ к каталогу с любого компьютера сети, что является дополнительным преимуществом.

В утилите Центр администрирования Active Directory можно также настроить параметры среды пользователя на панели **Профиль** (Profile). Для настройки этих параметров дважды щелкните по отображаемому имени пользователя в утилите Центр администрирования Active Directory и в появившемся окне перейдите на панель **Профиль** (рис. 9.5).

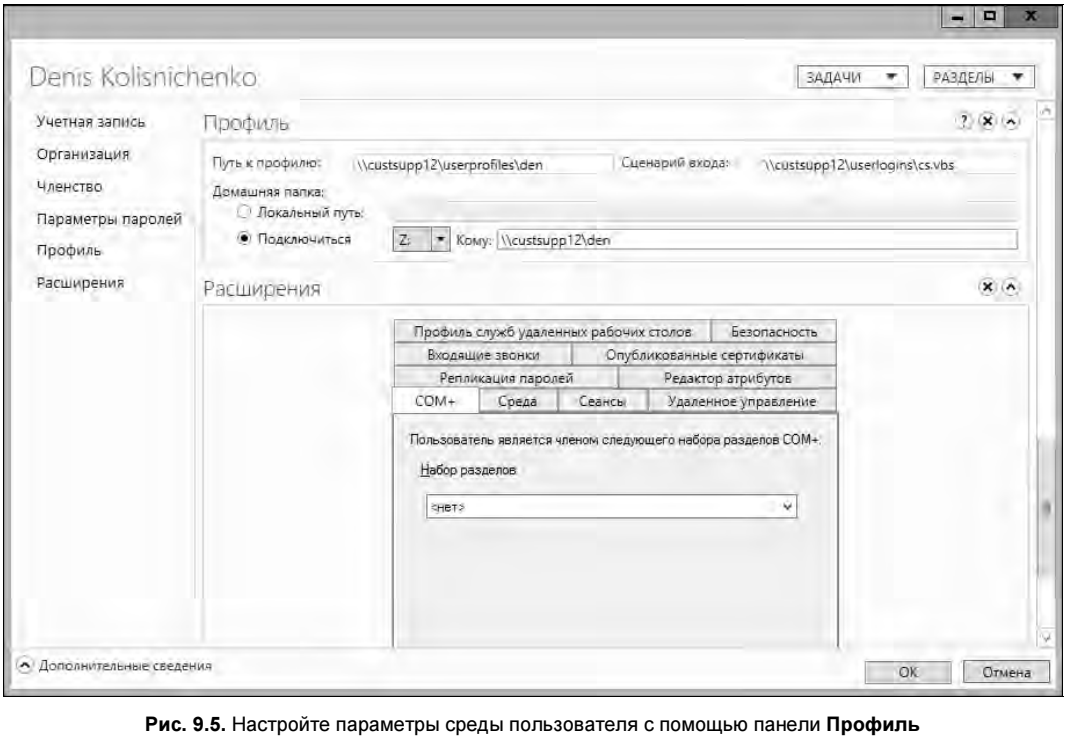


Рис. 9.5. Настройте параметры среды пользователя с помощью панели **Профиль**

Системные переменные среды

При настройке среды пользователя любому администратору пригодятся системные переменные среды, особенно они полезны при работе со сценариями входа. Используйте переменные среды для определения информации пути, которая может динамически изменяться. Чаще всего используют следующие системные переменные среды:

- `%SystemRoot%` — основной каталог операционной системы, например, C:\Windows. Используйте эту переменную на вкладке **Профиль** окна **Свойства** и в сценариях входа;
- `%UserName%` — имя учетной записи пользователя, например, wrstanek. Используйте эту переменную на вкладке **Профиль** окна **Свойства** и в сценариях входа;
- `%HomeDrive%` — буква диска с двоеточием, на котором находится домашний каталог пользователя, например, C:. Используйте эту переменную в сценариях входа;
- `%HomePath%` — полный путь к домашнему каталогу пользователя на соответствующем диске, например, \Users\Mkg\Georgej. Используйте эту переменную в сценариях входа;
- `%Processor_Architecture%` — архитектура процессора компьютера, за которым работает пользователь, например, *x*86. Используйте эту переменную в сценариях входа.

На рис. 9.6 показано, как можно использовать переменные среды при создании учетных записей пользователей. Обратите внимание, что `%UserName%` позволяет определить полную информацию пути для конкретного пользователя. Используя этот метод, можно указывать один и тот же путь для всех пользователей, но в результате каждый пользователь получит уникальные настройки.

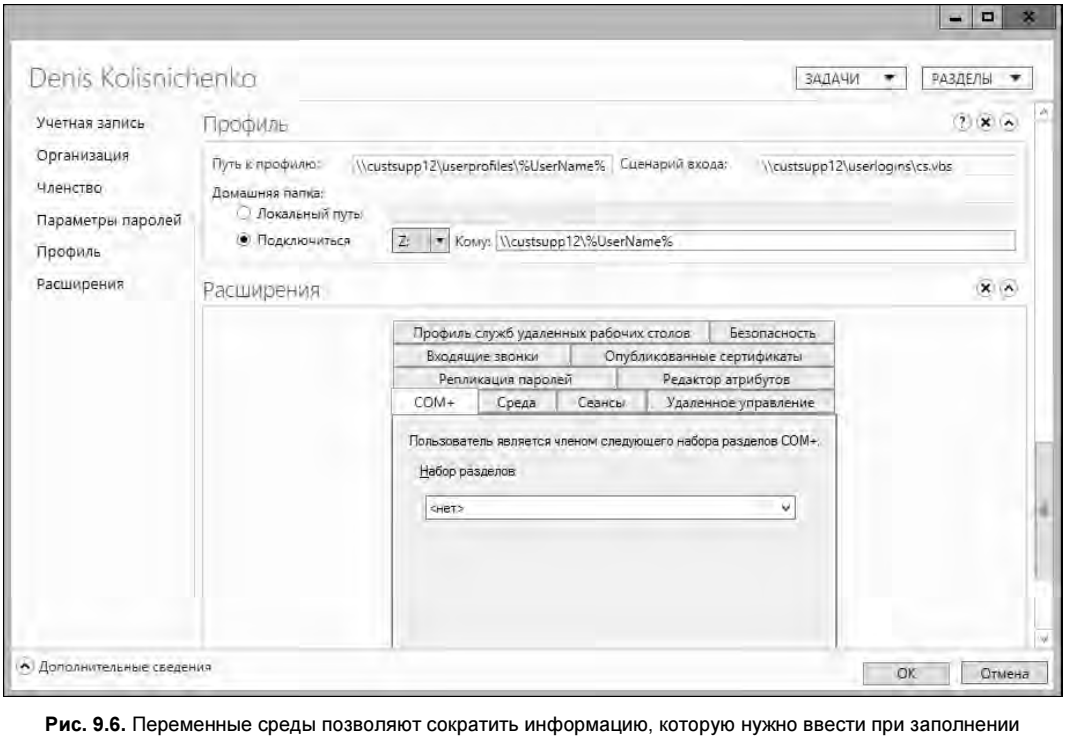


Рис. 9.6. Переменные среды позволяют сократить информацию, которую нужно ввести при заполнении вкладки **Профиль**, особенно при создании учетной записи на основании уже существующей

Сценарии входа

Команды сценария входа обрабатываются при каждом входе пользователя. Можно использовать сценарии входа для установки системного времени, путей сетевых дисков, сетевых принтеров и т. д. Хотя можно использовать сценарии входа для выполнения одноразовых команд, не нужно использовать их для установки переменных среды.

Любые настройки среды, задаваемые сценариями, не сохраняются для последующих процессов пользователей. Кроме того, нельзя использовать сценарии входа, чтобы указать автоматически запускаемые приложения. Ярлыки автоматически запускаемых программ нужно поместить в папку Startup (Автозагрузка) пользователя.

Обычно сценарии входа содержат команды Microsoft Windows. Однако сценарии входа могут быть следующими:

- сценарии PowerShell с расширением ps1 или другим корректным расширением;
- файлы Windows Script Host с расширениями bvs, js или любым другим корректным;
- командные файлы с расширением bat;
- исполняемые файлы программ с расширением exe.

Один и тот же сценарий может использоваться многими пользователями. Администратор контролирует, какие пользователи какие сценарии используют. Как подразумевает имя, пользователь получает доступ к сценариям входа при входе в свои учетные записи. Можно указать сценарий входа с помощью следующих действий:

1. Откройте окно **Свойства** пользователя в оснастке **Active Directory — пользователи и компьютеры** и перейдите на вкладку **Профиль**.
2. Введите имя сценария входа в поле **Сценарий входа** (Logon Script). Убедитесь, что указан полный путь к сценарию входа, например, \\Zeta\User_Logon\Eng.vbs

> ***Примечание***
>
> Для установки сценариев входа и выхода можно использовать другие методы. Для получения более подробной информации обратитесь к *главе 4*.

Создание сценариев входа в систему намного проще, чем можно подумать, особенно при использовании командного языка Windows. Практически любая команда, которая может быть введена в командной строке, может быть использована в сценарии входа. Чаще всего в сценариях входа устанавливаются принтеры по умолчанию и сетевые пути для пользователей. Эту информацию можно установить с помощью команды `net use`. Следующие команды `net use` определяют сетевой принтер и сетевой диск:

```
net use lpt1: \\zeta\techmain
net use G: \\gamma\corpfiles
```

Если эти команды будут в сценарии входа пользователя, пользователь получит сетевой принтер на LPT1 и сетевой диск G:. Можно создать подобные соединения в сценарии. При использовании VBScript нужно инициализировать переменные и объекты, которые планируется использовать, а затем вызвать соответствующие методы объекта `Network` для добавления соединений. Рассмотрим следующий пример:

```
Option Explicit
Dim wNetwork, printerPath
Set wNetwork = WScript.CreateObject("WScript.Network")
```

```
printerPath = "\\zeta\techmain"
wNetwork.AddWindowsPrinterConnection printerPath
wNetwork.SetDefaultPrinter printerPath
wNetwork.MapNetworkDrive "G:", "\\gamma\corpfiles"

Set wNetwork = vbEmpty
Set printerPath = vbEmpty
```

Здесь используется метод `AddWindowsPrinterConnection` для добавления соединения с принтером TechMain на компьютере Zeta, а затем применяется метод `SetDefaultPrinter` для установки этого принтера принтером по умолчанию для пользователя. Далее метод `MapNetworkDrive` вызывается для определения сетевого диска G:.

Назначение домашних каталогов

Операционная система Windows Server 2012 позволяет назначить домашний каталог для каждой учетной записи пользователя. Пользователи могут хранить и получать свои персональные файлы в этом каталоге. Большинство приложений использует домашний каталог пользователя по умолчанию при открытии и сохранении файлов, что помогает пользователю быстро найти свои ресурсы. Также домашний каталог используется командной строкой в качестве исходного текущего каталога.

Домашние каталоги могут быть расположены на локальном жестком диске пользователя или общем сетевом диске. Если домашний каталог находится на локальном диске, каталог будет доступен только с одной рабочей станции. С другой стороны, доступ к общему сетевому диску может быть получен с любого компьютера в сети, что делает среду пользователя более универсальной.

> ***Совет***
>
> Хотя пользователи могут разделять один и тот же каталог, — это плохая идея. Обычно надо предоставить каждому пользователю отдельный каталог.

Не нужно создавать домашний каталог пользователя заранее. Оснастка **Active Directory — пользователи и компьютеры** автоматически создаст его. Если будут проблемы при создании каталога, оснастка **Active Directory — пользователи и компьютеры** предоставит команды, позволяющие создать его вручную.

Для определения локального корневого каталога выполните такие действия:

1. Откройте окно **Свойства** пользователя в оснастке **Active Directory — пользователи и компьютеры**, а затем перейдите на вкладку **Профиль**.
2. Выберите переключатель **Локальный путь** (Local Path) в секции **Домашняя папка** (Home Folder), а затем введите путь к домашнему каталогу в предоставленное текстовое поле, например, C:\Home\`%UserName%`.

Чтобы указать сетевой домашний каталог, выполните такие действия:

1. Откройте окно **Свойства** пользователя в оснастке **Active Directory — пользователи и компьютеры**, а затем перейдите на вкладку **Профиль**.
2. В секции **Домашняя папка** выберите переключатель **Подключить** (Connect), затем укажите букву диска для домашнего каталога. Для однозначности используйте одну и ту же букву для всех пользователей. Также убедитесь, что выбрана буква диска, которая не

используется для других физических и виртуальных дисков. Чтобы избежать проблем, укажите букву Z в качестве буквы диска.

3. Введите полный путь к домашнему каталогу с использованием записи UNC (Universal Naming Convention), например, \\Gamma\User_Dirs\`%UserName%`. Добавьте имя сервера в путь диска, чтобы убедиться, что пользователь сможет получить доступ к каталогу с любого компьютера в сети.

> ***Примечание***
>
> Если домашний каталог не назначен, ОС Windows Server 2012 использует локальный домашний каталог по умолчанию.

Установка параметров и ограничений учетной записи

ОС Windows Server 2012 предоставляет администратору множество способов контролировать учетные записи пользователя и их доступ к сети. Администратор может определить часы входа, разрешенные рабочие станции для входа, привилегии dial-in и многое другое.

Управление часами входа

ОС Windows Server 2012 позволяет контролировать, когда пользователи могут войти в сеть. Можно сделать это путем установки разрешенных часов входа. Можно использовать ограничение часов входа для усилений безопасности и предотвращения взлома системы или вредоносной активности вне рабочего времени.

На протяжении установленных часов входа пользователи могут работать как обычно. Они могут войти в сеть и получить доступ к сетевым ресурсам. В запрещенное время пользователи не могут работать. Они не могут войти в систему или подключиться к ресурсам сети. Если пользователи вошли в систему в разрешенное время, но рабочее время вышло, что произойдет, зависит от политики учетной записи, установленной администратором. Вообще говоря, могут произойти две вещи:

- *принудительное отключение* — можно установить политику, говорящую Windows Server, что нужно принудительно отключить пользователей, когда их время входа вышло. Если эта политика установлена, удаленные пользователи будут отключены ото всех сетевых ресурсов и будет произведен их выход из системы, когда истечет разрешенное время;
- *пользователь не будет отключен* — пользователи не будут отключены от сети, когда выйдет разрешенное время. Вместо этого Windows Server просто не позволит им создавать новые сетевые соединения.

Настройка времени входа

Для настройки времени входа выполните следующие действия:

1. Откройте окно **Свойства** учетной записи пользователя. В оснастке **Active Directory — пользователи и компьютеры** перейдите на вкладку **Учетная запись** (Account), а затем нажмите кнопку **Время входа** (Logon Hours). В утилите Центр администрирования

Active Directory щелкните по ссылке **Время входа в систему** (Log On Hours) на панели **Учетная запись** (Account).

2. Теперь можно установить разрешенное и запрещенное время входа, используя окно **Время входа** (Log On Hours) (рис. 9.7). В этом окне можно включить или выключить каждый час дня или ночи:
   - разрешенные часы входа отмечаются заполненным синим прямоугольником. Можно думать об этих часах, как о включенных;
   - запрещенные часы отмечаются незаполненным прямоугольником. Можно думать об этих часах, как о выключенных.
3. Для изменения времени входа выделите время, а затем установите переключатель **Вход разрешен** (Logon Permitted) или **Вход запрещен** (Logon Denied).

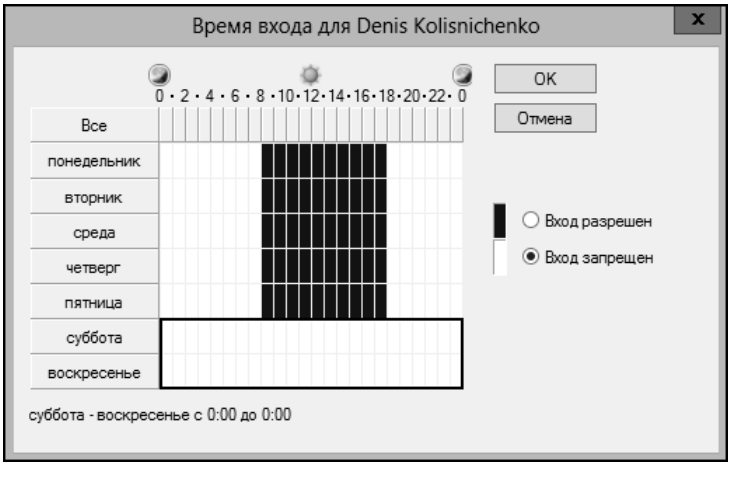


Рис. 9.7. Настройка часов входа для пользователей

В табл. 9.1 приведены опции окна **Время входа**.

Таблица 9.1. *Опции окна* ***Время входа***

Элемент	Функция
Все	Позволяет выбрать все доступные часы входа
Кнопки дней недели	Позволяют выбрать все часы определенного дня недели
Кнопки часов	Позволяют выбрать определенные часы для всех дней недели
Вход разрешен	Устанавливает разрешенные часы входа
Вход запрещен	Устанавливает запрещенные часы входа

Принудительное отключение пользователей

Для принудительного отключения пользователей, когда время входа закончилось, выполните следующие действия:

1. Откройте объект групповой политики (GPO), с которым нужно работать, как было показано в *главе 4*.

2. Откройте узел **Параметры безопасности** (Security Options), развернув дерево консоли. Разверните узлы **Конфигурация компьютера** (Computer Configuration), **Конфигурация Windows** (Windows Settings) и **Параметры безопасности** (Security Settings). В узле **Параметры безопасности** (Security Options) разверните узел **Локальные политики** (Local Policies), а затем выберите узел **Параметры безопасности** (Security Options).
3. Дважды щелкните на политике **Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы** (Network Security: Force Logoff When Logon Hours Expire). Откроется окно **Свойства** для политики.
4. Установите переключатель **Определить следующий параметр политики** (Define This Policy Setting), а затем — переключатель **Включен** (Enabled). Ограничение политики будет включено. Нажмите кнопку **OK**.

Установка разрешенных для входа рабочих станций

У Windows Server 2012 есть формальная политика, которая разрешает пользователям входить в системы локально. Эта политика определяет, может ли пользователь использовать клавиатуру компьютера и войти. По умолчанию можно использовать любую корректную учетную запись, в том числе и запись **Гость** (Guest), для локального входа в рабочую станцию.

Однако разрешение пользователям войти в любую рабочую станцию — это угроза безопасности. Если ограничивать использование рабочих станций, кто-либо, получив имя пользователя и пароль, может использовать их, чтобы войти в любую рабочую станцию в домене. Определяя список разрешенных рабочих станций, администратор уменьшает угрозу безопасности в своем домене. Теперь, мало того, что хакеры должны найти имя пользователя и пароль, они также должны найти разрешенные рабочие станции для учетной записи.

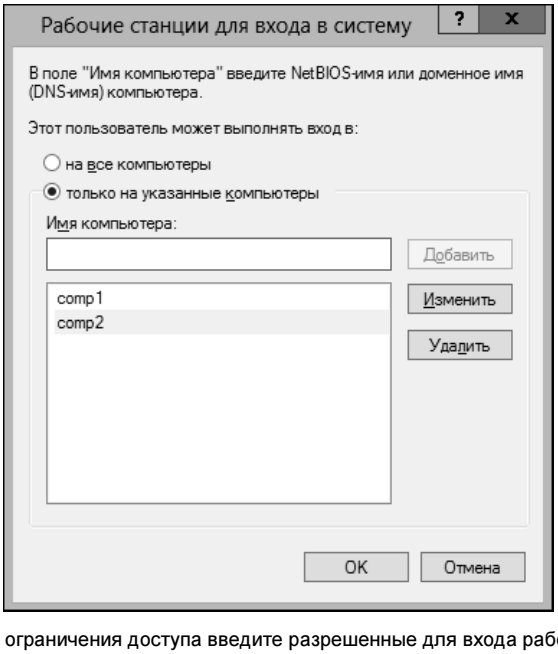


Рис. 9.8. Для ограничения доступа введите разрешенные для входа рабочие станции

Для пользователей домена можно определить разрешенные рабочие станции с помощью следующих действий:

1. Откройте окно **Свойства** пользователя. В оснастке **Active Directory — пользователи и компьютеры** перейдите на вкладку **Учетная запись** (Account), а затем нажмите кнопку **Вход на** (Log On To). В утилите Центр управления Active Directory перейдите на панель **Учетная запись** (Account) и нажмите кнопку **Вход на** (Log On To).
2. Установите переключатель **только на указанные компьютеры** (This User Can Log On To), как показано на рис. 9.8.
3. Введите имя разрешенной рабочей станции, а затем нажмите кнопку **Добавить**. Повторите эту процедуру для определения дополнительных рабочих станций.
4. В случае ошибки выберите ошибочную запись и нажмите кнопку **Удалить**.

Установка привилегий входящих звонков и VPN

Windows Server 2012 позволяет устанавливать привилегии удаленного доступа на вкладке **Входящие звонки** (Dial-In) окна **Свойства** пользователя. Эти параметры контролируют доступ для входящих звонков и виртуальных частных сетей (VPN). Привилегии удаленного доступа по умолчанию контролируются политикой Network Policy Server (NPS). Это — предпочтительный метод управления удаленным доступом. Можно явно предоставить или отклонить полномочия, установив либо переключатель **Разрешить доступ** (Allow Access), либо переключатель **Запретить доступ** (Deny Access). В любом случае, прежде чем пользователи смогут удаленно получить доступ к сети, нужно выполнить эти шаги:

1. В диспетчере серверов добавьте роль **Службы политики сети и доступа** (Network Policy And Access Services).
2. Для включений соединений удаленного доступа откройте GPO для сайта, домена или организационного подразделения, с которыми нужно работать *(см. главу 4)*. В редакторе политики разверните узел **Конфигурация пользователя\Административные шаблоны\Сеть** (User Configuration, Administrative Templates, Network). Выберите политику **Сетевые подключения** (Network Connections), а затем настройте политики сетевых подключений для сайта, домена или организационного подразделения.
3. Настройте удаленный доступ с использованием утилиты **Маршрутизация и удаленный доступ** (Routing And Remote Access). В утилите **Управление компьютером** разверните узел **Службы и приложения** (Services And Applications), а затем выберите элемент **Маршрутизация и удаленный доступ**. Настройте маршрутизацию и удаленный доступ, как необходимо.

> ***Практический совет***
>
> Необходимые двоичные файлы для установки ролей и компонентов называются *полезными нагрузками*. В Windows Server 2012 можно удалить полезные нагрузки для ролей и компонентов с помощью параметра `-Remove` командлета Uninstall-WindowsFeature. Восстановить удаленные полезные нагрузки можно командлетом Install-WindowsFeature. По умолчанию полезные нагрузки восстанавливаются через Windows Update. Используйте параметр `-Source` для восстановления полезной нагрузки из точки монтирования WIM. В следующем примере двоичные файлы NPS и RRAS восстанавливаются с помощью Windows Update:
>
> ```
> install-windowsfeature -name npas-policy-server -includemanagementtools
> install-windowsfeature -name remoteaccess -includeallsubfeature
> -includemanagementtools
> ```

После предоставления пользователю разрешения на доступ к сети удаленно, выполните следующие действия для настройки дополнительных параметров входящих звонков на вкладке **Входящие звонки** (Dial-In) окна **Свойства** учетной записи пользователя (рис. 9.9):

1. Если пользователь должен совершить входящий звонок с определенного номера телефона, установите флажок **Проверить код звонящего** (Verify Caller-ID), а затем введите номер телефона, с которого производится дозвон. Телефонная система должна поддерживать Caller ID для работы этой функции.

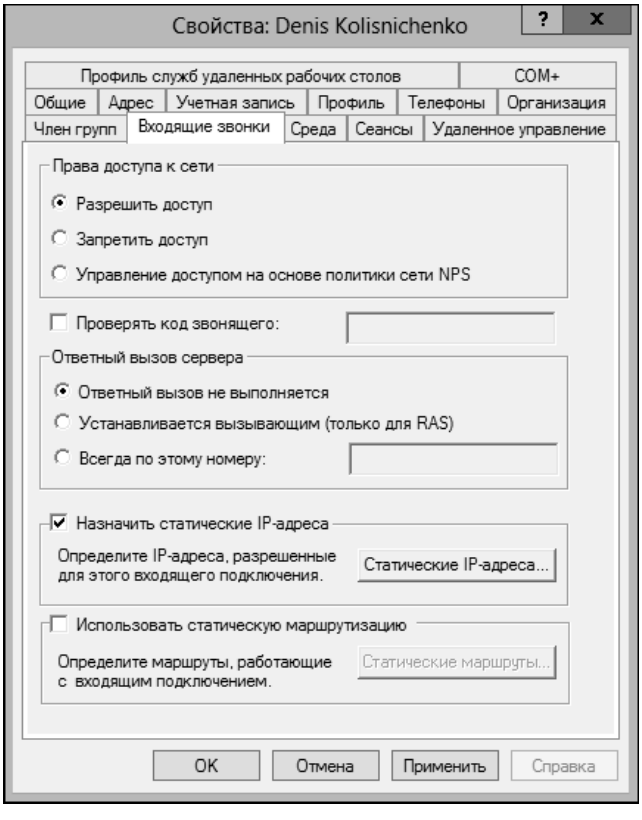


Рис. 9.9. Полномочия входящих звонков контролируют доступ к сети

Примечание

В утилите Центр управления Active Directory вкладка **Входящие звонки** (Dial-In) доступна на панели **Расширения** (Extensions). Щелкните на разделе **Расширения**, а затем выберите вкладку **Входящие звонки**.

2. Определите параметры ответного вызова (callback), используя следующие опции.
   - **Ответный вызов не выполняется** (No Callback) — позволяет пользователю непосредственно выполнить входящий звонок и остаться подключенным. Влечет дополнительные расходы со стороны пользователя.
   - **Устанавливается вызывающим (только для RAS)** (Set By Caller) — сначала пользователь дозванивается на сервер, затем сервер запрашивает у пользователя номер для обратного звонка. Как только номер введен, пользователь отключается, а сервер

перезванивает клиенту по указанному номеру и устанавливает соединения. В этом случае дополнительные расходы лягут на плечи компании.

- **Всегда по этому номеру** (Always Callback To) — позволяет предопределить номер обратного звонка из соображений безопасности. Когда пользователь позвонит на сервер, сервер автоматически наберет предустановленный номер. Как и в предыдущем случае, расходы будет оплачивать компания, но это снижает риск несанкционированного доступа к сети.

Примечание

Не нужно присваивать номера обратного вызова для пользователей, набирающих номер через коммутатор. Коммутатор не позволит пользователю должным образом соединиться с сетью. Также не нужно использовать предварительно установленные номера телефонов на многосвязных линиях, которые не будут функционировать должным образом.

Если необходимо, также можно назначить статические IP-адреса и статическую маршрутизацию для входящих звонков, нажав кнопку **Назначить статические IP-адреса** (Assign Static IP Addresses) или кнопку **Использовать статическую маршрутизацию** (Apply Static Routes) соответственно.

Установка параметров безопасности учетной записи

Вкладка/панель **Учетная запись** (Account) окна **Свойства** пользователя содержит следующие опции, призванные помочь обслуживать безопасное сетевое окружение и контролировать, как используются учетные записи пользователей.

- **Требовать смены пароля при следующем входе в систему** (User Must Change Password At Next Logon) — заставляет пользователя изменить свой пароль при очередном входе в систему.
- **Запретить смену пароля пользователем** (User Cannot Change Password) — не разрешает пользователю изменять пароль учетной записи.
- **Срок действия пароля не ограничен** (Password Never Expires) — срок действия пароля учетной записи никогда не истекает, что позволяет перезаписать нормальный срок действия пароля.

Предупреждение

Опция **Срок действия пароля не ограничен** (Password Never Expires) создает потенциальный риск безопасности в сети. Хотя можно использовать эту опцию для учетных записей администраторов, нельзя ее применять для учетных записей обычных пользователей.

- **Хранить пароль, используя обратимое шифрование** (Store Password Using Reversible Encryption) — сохраняет пароль в виде зашифрованного текста, который можно расшифровать.
- **Отключить учетную запись** (Account Is Disabled Disables) — отключает учетную запись, что предотвращает доступ пользователя в сеть и вход в систему (этот параметр есть только в оснастке **Active Directory — пользователи и компьютеры**).
- **Для интерактивного входа в сеть нужна смарт-карта** (Smart Card Is Required For Interactive Logon Requires) — требует, чтобы пользователь вошел в рабочую станцию, предоставив смарт-карту. Пользователь не может войти, указав имя пользователя и пароль с клавиатуры.

- **Учетная запись важна и не может быть делегирована** (Account Is Sensitive And Cannot Be Delegated) — определяет, что учетные данные пользователя не могут быть делегированы посредством Kerberos. Используйте этот параметр для важных учетных записей, которые должны тщательно контролироваться.
- **Использовать типы шифрования Kerberos DES для этой учетной записи** (Use Kerberos DES Encryption Types For This Account Specifies) — определяет, что учетная запись будет использовать шифрование DES (Data Encryption Standard).
- **Данная учетная запись поддерживает 128-разрядное шифрование AES** (This Account Supports Kerberos AES 128 Bit Encryption) — определяет, что учетная запись поддерживает 128-разрядное шифрование AES (Advanced Encryption Standard).
- **Данная учетная запись поддерживает 256-разрядное шифрование AES** (This Account Supports Kerberos AES 256 Bit Encryption) — определяет, что учетная запись поддерживает 128-разрядное шифрование AES.
- **Без предварительной проверки подлинности Kerberos** (Do Not Require Kerberos Preauthentication) — определяет, что учетная запись не нуждается в предварительной аутентификации Kerberos для доступа к сетевым ресурсам. Предварительная аутентификация — это часть процедуры безопасности Kerberos v5. Вход без предварительной аутентификации позволяет проверить подлинность клиентов, использующих предыдущую или нестандартную реализацию Kerberos.

> ***Практический совет***
>
> AES — один из нескольких стандартов шифрования. Другой используемый в Windows стандарт шифрования называется DES (Data Encryption Standard). Большинство компьютеров, работающих под управлением старых версий Windows, поддерживает DES.
>
> Компьютеры, работающие под управлением текущих версий Windows, поддерживают стандарт AES, предоставляющий более безопасное шифрование, чем DES. Версии AES, использующиеся в США, поддерживают как 128-битное, так и 256-битное шифрование. Версии AES, экспортируемые за пределы США, обычно поддерживают только 128-битное шифрование.

Управление профилями пользователей

Профили пользователей содержат настройки для сетевого окружения, например, конфигурацию рабочего стола и опции меню. Проблемы с профилем могут иногда препятствовать входу пользователя в систему. Например, если размер экрана в профиле не поддерживается в рабочей системе, пользователь не сможет войти корректно. Фактически пользователь может увидеть только пустой экран. Можно перезагрузить компьютер, перейти в режим VGA и затем установить режим вручную. Однако решение проблем профиля не всегда легкое, и, вполне вероятно, что придется обновить сам профиль.

ОС Windows Server 2012 предоставляет несколько способов управления профилем пользователя:

- можно назначить пути профиля в оснастке **Active Directory — пользователи и компьютеры** или в Центре администрирования Active Directory;
- можно скопировать, удалить или изменить тип существующего локального профиля с помощью утилиты **Система** (System) в Панели управления;
- можно установить системные политики, которые препятствуют тому, чтобы пользователи управляли определенными аспектами своей среды.

Локальные, перемещаемые и обязательные профили

В Windows Server 2012 у каждого пользователя есть профиль. Профили управляют функциями запуска сеанса пользователя, типами доступных программ и приложений, параметрами рабочего стола и многим другим. У каждого компьютера, с которого пользователь входит в сеть, есть копия профиля пользователя. Поскольку этот профиль сохранен на жестком диске компьютера, у пользователей, обладающих доступом к нескольким компьютерам, есть профиль на каждом компьютере. Другой компьютер в сети не может получить доступ к локально сохраненному профилю, называемому *локальным профилем*, и у этого способа есть определенные недостатки. Например, если пользователь входит в сеть с трех разных рабочий станций, у него будут три разных профиля — на каждой системе. В результате пользователь запутается, какие сетевые ресурсы доступны в данной системе.

Работа с перемещаемыми и обязательными профилями

Чтобы уменьшить беспорядок, вызванный множественными профилями, можно создать профиль, к которому могут получить доступ другие компьютеры. Этот тип профиля называют *перемещаемым* (roaming). По умолчанию, при использовании перемещаемого профиля пользователи могут получить доступ к одному и тому же профилю, независимо от того, какой компьютер они используют в пределах домена. Перемещаемые профили привязаны к серверу и хранятся только на Windows Server. Когда пользователь с перемещаемым профилем входит в систему, профиль загружается и создается локальная копия на компьютере пользователя. Когда пользователь выходит из системы, изменения в профиле обновляются и на локальном компьютере, и на сервере.

> ***Практический совет***
>
> Если организация использует зашифрованную файловую систему (Encrypted File System, EFS), то для повышения безопасности доступа к файлам использование перемещаемых профилей становится чрезвычайно важным для пользователей, которые входят в сеть с разных компьютеров. Это важно, потому что сертификаты шифрования хранятся в профилях пользователей, сертификат шифрования необходим для доступа и работы с зашифрованными файлами пользователя. Если пользователь зашифровал файлы и у него нет перемещаемого профиля, пользователь не сможет работать с этими зашифрованными файлами на другом компьютере (за исключением применения службы Digital Identity Management Service, DIMS).

Администратор может управлять профилями пользователей или позволить пользователям управлять собственными профилями. Одна из причин самостоятельного управления профилями — у всех пользователей будет общая конфигурация сети, которая может сократить количество связанных со средой проблем.

Профили, контролируемые администраторами, называются *обязательными*. Пользователи, у которых есть обязательный профиль, могут произвести только переходные изменения в среде. Любые изменения, которые пользователи вносят в окружение, не сохраняются, при следующем входе в систему, и пользователи вернутся к исходному профилю. Идея заключается в том, что если пользователи не могут изменить сетевое окружение, они не смогут внести изменения, которые станут причиной проблемы. Основной недостаток обязательных профилей в том, что пользователь может войти в систему, только если доступен его профиль. Если по каким-то причинам сервер, хранящий профиль, недоступен и недоступен кэшированный профиль, пользователь не сможет войти в систему. Если сервер недоступен, но доступен кэшированный профиль, пользователь получит предупреждающее сообщение, но будет зарегистрирован в локальной системе с учетом кэшированного профиля.

Практический совет

Если у пользователя обязательный профиль, временный профиль (пользователь зарегистрирован по учетной записи **Гость**) или системный профиль, Windows 8 и Windows Server 2012 по умолчанию блокируют развертывание пакетов приложений. Чтобы разрешить развертывание приложений при использовании одного из этих специальных профилей, можно включить политику **Разрешить операции развертывания для особых профилей** (Allow Deployment Operation In Special Profiles) в узле **Конфигурация компьютера\Политики\ Административные шаблоны\ Компоненты Windows\Развертывание пакета приложений** (Computer Configuration\Policies\Administrative Templates\Windows Components\App Package Deployment).

Ограничение перемещаемых профилей

Обычно пользователи могут получить доступ к своему перемещаемому профилю, независимо от того, какой компьютер они используют в домене. Операционные системы Windows 8 и Windows Server 2012 позволяют изменить это поведение путем указания, с каких компьютеров пользователь может получить доступ к перемещаемому профилю и перенаправленным папкам. Это можно сделать посредством назначения некоторых компьютеров основными и настройки политики домена для ограничения загрузки профилей, перенаправленных папок на основных компьютерах.

Основной компьютер — компьютер, который был специально назначен как разрешенный для использования с перенаправленными данными путем редактирования расширенных свойств пользователя или группы в Active Directory и указанием имен разрешенных компьютеров для свойства msDS-PrimaryComputer. Включите на основном компьютере ограничение для перемещаемых профилей, с помощью политики **Загружать перемещаемые профили только на основные компьютеры** (Download Roaming Profiles On Primary Computers Only) в узле **Конфигурация компьютера\Политики\Административные шаблоны\Система\Профили пользователей** (Computer Configuration\Policies\Administrative Templates\System\User Profiles). Также на основных компьютерах можно включить ограничение для перенаправленных папок посредством политики **Перенаправление папки только на основных компьютерах** (Redirect Folders On Primary Computers Only) в узле **Конфигурация компьютера\Политики\Административные шаблоны\Система\Перенаправление папок** (Computer Configuration\Policies\Administrative Templates\System\Folder Redirection).

Цель этих политик — защитить персональные и корпоративные данные, когда пользователи входят в компьютеры, отличающиеся от тех, которые они регулярно используют для работы. Безопасность данных улучшается, если мы не загружаем и не кэшируем эти данные на компьютерах, на которых обычно пользователь не работает. Чтобы установить свойство msDS-PrimaryComputer для пользователя или группы, выполните следующие действия:

1. В Центре администрирования Active Directory откройте окно **Свойства** для пользователя или группы, а затем перейдите на панель **Расширения**. В оснастке **Active Directory — пользователи и компьютеры** убедитесь, что в меню **Вид** (View) выбрана опция **Дополнительные компоненты** (Advanced Features), а затем откройте окно **Свойства** пользователя или группы.
2. На вкладке **Редактор атрибутов** (Attribute Editor) пролистайте список атрибутов. Найдите и выделите атрибут msDS-PrimaryComputer и нажмите кнопку **Изменить** (Edit).
3. В окне **Редактор многозначных строк** (Multi-Valued String Editor) введите имя первого основного компьютера и нажмите кнопку **Добавить**. Повторите этот процесс для всех основных компьютеров. Нажмите кнопку **OK** дважды.

Создание локальных профилей

Профили пользователей хранятся либо в каталоге по умолчанию, либо в каталоге, который задан текстовым полем **Путь к профилю** (Profile Path) в диалоговом окне **Свойства** (на вкладке **Профиль**) пользователя. Для Windows 7 каталог по умолчанию выглядит так: *%SystemDrive%*\Users\%UserName%\. Ключевая часть профиля — файл Ntuser.dat, который можно найти в этом каталоге, например, C:\Users\wrstanek\Ntuser.dat. Если изменить расположение по умолчанию, у пользователя будет локальный профиль.

Создание перемещаемых профилей

Перемещаемые профили хранятся на Windows Server. Когда пользователи входят на разные компьютеры и используют EFS, они нуждаются в перемещаемом профиле, чтобы убедиться, что сертификаты, необходимые для чтения и работы с зашифрованными файлами, доступны на всех компьютерах, а не только на их основных компьютерах.

Если нужно, чтобы у пользователя был перемещаемый профиль, установите каталог на сервере, где будут храниться профили. Для этого выполните следующие действия:

1. Создайте общий каталог на сервере под управлением Windows Server и убедитесь, что группа **Все** (Everyone) имеет как минимум доступ **Изменение** (Change) и **Чтение** (Read).
2. В оснастке **Active Directory — пользователи и компьютеры** или в Центре администрирования Active Directory откройте окно **Свойства** пользователя и перейдите на вкладку **Профиль**. Введите путь к общему каталогу в поле **Путь к профилю**. Путь должен быть указан в виде *сервер**папка_профиля*. Например, \\Zeta\\User_Profiles\Georgej, где Zeta — это имя сервера, User_profiles — общий каталог, а Georgej — имя пользователя. Перемещаемый профиль будет сохранен в файле Ntuser.dat назначенного каталога, например, \\Zeta\\User_Profiles\Georgej\Ntuser.dat.

   Примечание

   Обычно не нужно создавать каталог профилей. Этот каталог создается автоматически при входе пользователя, а NTFS-разрешения устанавливаются, как только пользователь получает доступ. Можно выбрать несколько учетных записей пользователей для одновременного редактирования. Один из способов — удерживать нажатой клавишу <Shift> или <Ctrl> при выборе имен пользователей. После этого щелкните правой кнопкой мыши на именах пользователей и выберите команду **Свойства**. Теперь можно отредактировать свойства для всех выбранных пользователей. Убедитесь, что используете переменную среды `%UserName%` в пути профиля, например, \\Zeta\User_Profiles\`%UserName%`.

3. В качестве дополнительного шага можно создать профиль для пользователя или скопировать существующий профиль в каталог профиля пользователя. Если не создать актуальный профиль для пользователя, при следующем входе в систему он будет использовать локальный профиль по умолчанию. Любые изменения, которые пользователь вносит в этот профиль, будут сохранены при выходе из системы. В следующий раз, когда пользователь войдет в систему, у него будет персональный профиль.

Создание обязательных профилей

Обязательные профили хранятся на серверах под управлением Windows Server. Если нужно чтобы у пользователя был обязательный профиль, определите профиль так:

1. Выполните действия 1 и 2 в предыдущем *разд. "Создание перемещаемых профилей"*.
2. Создайте обязательный профиль, переименовав файл Ntuser.dat в `%UserName%`\Ntuser.man. При следующем входе в систему у пользователя будет обязательный профиль.

Примечание

Файл Ntuser.dat содержит настройки реестра для пользователя. При изменении расширения файла на Ntuser.man операционная система Windows Server создает обязательный профиль.

Использование утилиты *Система* для управления локальными профилями

Для управления локальными профилями нужно зарегистрироваться на компьютере пользователя. Затем можно использовать утилиту **Система** (System) в Панели управления для управления локальными профилями. Чтобы просмотреть информацию о текущем профиле, перейдите в раздел **Система и безопасность** (System and Security) в Панели управления и запустите утилиту **Система**. На странице **Система** (System) в Панели управления щелкните по ссылке **Дополнительные параметры системы** (Advanced System Settings). В окне **Свойства системы** (System Properties) в области **Профили пользователей** (User Profiles) нажмите кнопку **Параметры** (Settings).

Как показано на рис. 9.10, окно **Профили пользователей** (User Profiles) отображает информацию о профилях, сохраненных на локальном компьютере. Эта информация поможет в управлении профилями. Список профилей содержит следующую информацию:

- **Имя** (Name) — имя локального профиля, генерируется автоматически, содержит имя домена или компьютера, а также имя учетной записи пользователя. Например, имя ADATUM\Wrstanek означает, что домен называется adatum, а имя учетной записи пользователя — wrstanek;

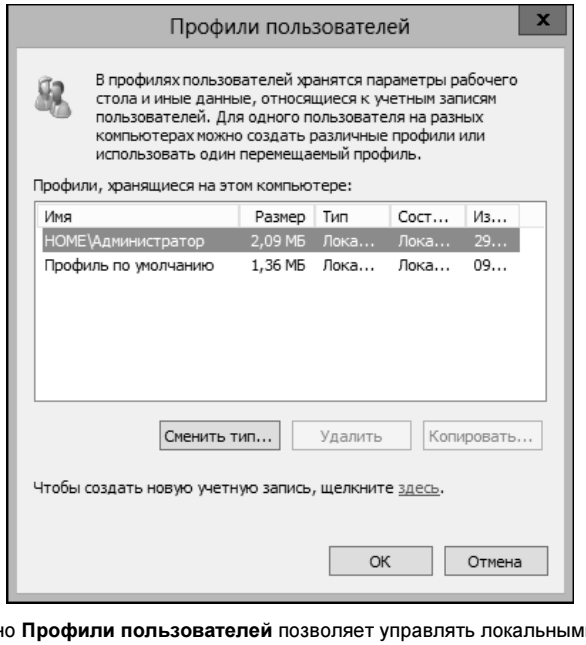


Рис. 9.10. Окно **Профили пользователей** позволяет управлять локальными профилями

Примечание

Если удаляется учетная запись, но не удаляется связанный с ней профиль, учетная запись будет помечена как **Учетная запись удалена** (Account Deleted) или **Учетная запись неиз-**

вестна (Account Unknown). Не волнуйтесь — профиль все еще доступен для копирования (в случае необходимости), в этом же окне его можно удалить (рис. 9.10).

- **Размер** (Size) — размер профиля. Обычно, чем больше профиль, тем больше изменений пользователь внес в среду;
- **Тип** (Type) — тип профиля, может быть локальным или перемещаемым;
- **Состояние** (Status) — текущее состояние профиля, например, находится ли профиль в локальном кэше;
- **Изменение** (Modified) — дата последнего изменения профиля.

Создание профиля вручную

Иногда нужно создать профиль вручную. Для этого войдите в учетную запись пользователя, внесите необходимые изменения и выйдите. Такой метод занимает много времени. Лучше всего создать базовую учетную запись пользователя, настроить ее окружение, а затем использовать ее в качестве основы для других учетных записей.

Копирование существующего профиля в новую учетную запись пользователя

Если есть базовая учетная запись пользователя или учетная запись, которую планируется использовать подобным образом, можно скопировать существующий профиль в новую учетную запись пользователя. Для этого выполните следующие действия в утилите **Система** Панели управления:

1. Запустите утилиту **Система** из Панели управления. На странице **Система** щелкните по ссылке **Дополнительные параметры системы**. В окне **Свойства** системы нажмите кнопку **Параметры** в области **Профили пользователей**.
2. Из списка **Профили, хранящиеся на этом компьютере** (Profiles Stored On This Computer) выберите профиль, который нужно скопировать (см. рис. 9.10).
3. Скопируйте профиль в новую учетную запись, нажав кнопку **Копировать** (Copy To). В окне **Копирование профиля** (Copy Profile To) введите путь к каталогу профиля новой учетной записи пользователя (рис. 9.11). Например, если нужно создать профиль для georgej, введите \\Zeta\User_Profiles\Georgej.

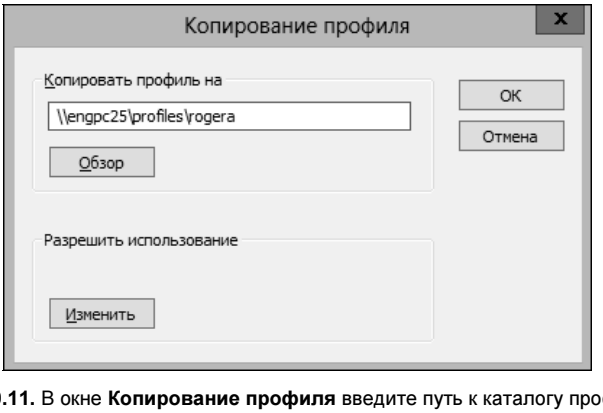


Рис. 9.11. В окне **Копирование профиля** введите путь к каталогу профиля и назначьте разрешения для пользователя

4. Теперь нужно назначить пользователю разрешения для доступа к профилю. В области **Разрешить использование** (Permitted To Use) нажмите кнопку **Изменить** (Change), а затем используйте окно **Выбор: "Пользователь" или "Группа"** (Select User Or Group) для предоставления доступа к новой учетной записи пользователя.
5. Нажмите кнопку **OK** для закрытия окна **Копирование профиля**. Windows скопирует профиль в новое место.

> ***Совет***
> Если знаете имя пользователя или группы, которое нужно использовать, можно сэкономить время, просто указав их в поле **Введите имена выбираемых объектов** (Name).

Копирование или восстановление профиля

В рабочей группе, где каждый компьютер управляется отдельно, часто приходится копировать локальный профиль пользователя с одного компьютера на другой. Копирование профиля позволяет пользователям обслуживать настройки среды, когда они используют разные компьютеры. Конечно, в домене Windows Server можно использовать перемещаемый профиль для создания одного профиля, который может быть доступен с любого компьютера в домене. Проблема в том, что иногда нужно скопировать существующий локальный профиль, чтобы заменить перемещаемый профиль пользователя (когда перемещаемый профиль поврежден), или необходимо скопировать существующий локальный профиль, чтобы создать перемещаемый профиль в другом домене.

Для копирования профиля в новое место выполните следующие действия:

1. Войдите в компьютер пользователя и запустите утилиту **Система**. На странице **Система** щелкните по ссылке **Дополнительные параметры системы**. В окне **Свойства системы** нажмите кнопку **Параметры** в области **Профили пользователей**.
2. Из списка **Профили, хранящиеся на этом компьютере** выберите профиль, который нужно скопировать.
3. Скопируйте профиль в новое место: нажмите кнопку **Копировать**, а в окне **Копирование профиля** укажите путь к новому каталогу профиля. Например, если создаете профиль для janew, можно ввести \\Gamma\User_Profiles\Janew.
4. Для предоставления пользователю доступа к профилю нажмите кнопку **Изменить**. Затем в окне **Выбор: "Пользователь" или "Группа"** предоставьте доступ к соответствующей учетной записи пользователя.
5. Когда закончите, нажмите кнопку **OK** для закрытия окна **Копирование профиля**. ОС Windows скопирует профиль в новое место.

Удаление локального профиля и назначение нового

Доступ к профилям осуществляется, когда пользователь заходит в компьютер. ОС Windows Server использует локальные профили для всех пользователей, у которых нет перемещаемых профилей. Обычно локальные профили также используются, если у локального профиля более свежая дата изменения, чем у перемещаемого профиля пользователя. Поэтому иногда нужно удалить локальный профиль пользователя. Например, если локальный профиль пользователя поврежден, можно удалить его и присвоить новый. Имейте в виду, что при удалении локального профиля, который больше нигде в домене не сохранен, невозможно будет восстановить исходные настройки среды пользователя.

Для удаления локального профиля пользователя выполните следующие действия:

1. Войдите на компьютер пользователя, используя учетную запись с правами администратора, а затем запустите утилиту **Система**.
2. На странице **Система** щелкните по ссылке **Дополнительные параметры системы**. В окне **Свойства системы** нажмите кнопку **Параметры** в области **Профили пользователей**.
3. В появившемся окне выберите профиль, который нужно удалить, и нажмите кнопку **Удалить** (Delete). Для подтверждения удаления нажмите кнопку **Да** (Yes) в появившемся диалоговом окне.

> ***Примечание***
>
> Нельзя удалить профиль, который в данный момент используется. Если пользователь зарегистрирован в локальной системе (на компьютере, с которого удаляется профиль), нужно, чтобы пользователь вышел из системы до удаления профиля. В некоторых случаях Windows Server помечает профили как используемые, хотя на самом деле это не так. Это обычно результат изменения среды для пользователя, которое не было правильно применено. Чтобы исправить это, нужно перезагрузить компьютер.

При следующем входе пользователя Windows Server сделает одну из двух вещей. Операционная система либо предоставит пользователю локальный профиль по умолчанию, либо получит перемещаемый профиль пользователя, сохраненный на другом компьютере. Чтобы предотвратить использование любого из этих профилей, необходимо назначить пользователю новый профиль. Чтобы сделать это, выполните одно из следующих действий:

- скопируйте существующий профиль в каталог профиля пользователя (копирование профилей было рассмотрено *ранее в этой главе*);
- обновите настройки профиля для пользователя в оснастке **Active Directory — пользователи и компьютеры**. Установите путь к профилю, как было показано в *разд. "Создание перемещаемых профилей" ранее в этой главе*.

Изменение типа профиля

При работе с перемещаемыми профилями утилита **Система** позволяет изменить тип профиля на компьютере пользователя. Чтобы сделать это, выберите профиль и затем нажмите кнопку **Сменить тип** (Change Type). Опции в появившемся окне позволяют сделать следующее.

- **Изменить перемещаемый профиль на локальный** (Change a roaming profile to a local profile) — если нужно, чтобы пользователь всегда работал с локальным профилем на этом компьютере, укажите, что профиль предназначен для локального использования. Все изменения в этом профиле будут сделаны локально, и исходный перемещаемый профиль останется неизменным.
- **Изменить локальный профиль (который был изначально определен как перемещаемый) на перемещаемый** (Change a local profile (that was defined originally as a roaming profile) to a roaming profile) — пользователь будет использовать исходный перемещаемый профиль при следующем входе. Windows Server будет обрабатывать профиль как любой другой перемещаемый, т. е. любые изменения в локальном профиле будут скопированы в перемещаемый профиль.

> ***Примечание***
>
> Если эти параметры недоступны, исходный профиль пользователя определен локально.

Обновление учетных записей пользователя и группы

Центр администрирования Active Directory и оснастка **Active Directory — пользователи и компьютеры** — утилиты, использующиеся для обновления учетных записей пользователя домена или группы. Если необходимо обновить учетную запись локального пользователя или группы, примените утилиту **Локальные пользователи и группы**.

При работе с Active Directory часть нужно получить список учетных записей и потом что-то с ними сделать. Например, можно вывести все учетные записи пользователей в организации и затем отключить учетные записи пользователей, которые уже больше не работают в компании. Для выполнения этой задачи выполните следующие действия:

1. В оснастке **Active Directory — пользователи и компьютеры** щелкните правой кнопкой мыши по имени домена и выберите команду **Найти** (Find).
2. В списке **Найти** (Find) выберите элемент **Пользовательский поиск** (Custom Search). Окно поиска будет обновлено и отобразит вкладку **Пользовательский поиск (**Custom Search).
3. В списке **Где** (In) выберите область поиска. Для поиска по всему предприятию выберите **В Active Directory** (Entire Directory).
4. На вкладке **Пользовательский поиск** (Custom Search) нажмите кнопку **Поле** (Field) для отображения меню. Выберите **Пользователь** (User), а затем **Имя входа (пред-Windows 2000)** (Logon Name (Pre-Windows 2000)).

   Совет

   Убедитесь, что выбрана опция **Имя входа (пред-Windows 2000)** (Logon Name (Pre–Windows 2000)). Не используйте просто **Имя входа** (Logon Name). Учетная запись не всегда имеет имя входа, но у нее всегда есть имя входа для версий ОС, предшествовавших Windows 2000.

5. В списке **Условие** (Condition) выберите **присутствует** и затем нажмите кнопку **Добавить**. Для подтверждения своих намерений нажмите кнопку **Да**.
6. Нажмите кнопку **Найти** (Find Now). Оснастка сформирует список всех пользователей в выбранной области.
7. Теперь можно работать с учетными записями по отдельности или с несколькими сразу. Один из способов непоследовательно выбрать несколько ресурсов — нажать и удерживать клавишу <Ctrl>, а затем с помощью мыши отмечать каждый объект, который нужно выбрать. Выбрать ресурсы последовательно можно с помощью клавиши <Shift>, нажмите и удерживайте ее, потом щелкните мышью на первом объекте, а затем — на последнем.
8. Щелкните правой кнопкой мыши по имени пользователя и выберите действие из контекстного меню, например **Отключить учетную запись** (Disable Account).

   Совет

   Можно выполнять следующие действия сразу над несколькими учетными записями: **Добавить в группу** (Add To Group), **Включить учетную запись** (Enable Account)**, Отключить учетную запись** (Disable Account), **Удалить** (Delete)**, Переместить** (Move) и **Отправить почту** (Send Mail). Выбрав команду **Свойства**, можно отредактировать свойства нескольких учетных записей сразу.

Используйте подобную процедуру для получения списка всех компьютеров, групп или других ресурсов Active Directory. Для получения списка компьютеров откройте вкладку **Пользовательский поиск** (Custom Search), из меню **Поле** (Field) выберите **Компьютер | Имя компьютера (пред-Windows 2000)** (Computer | Computer Name (Pre-Windows 2000)). Для получения групп из меню **Поле** (Field) нужно выбрать команду **Группа** (Group), а затем — **Имя группы (пред-Windows 2000)** (Group Name (Pre-Windows 2000)).

В следующих разделах мы поговорим о других методах, позволяющих обновлять (переименовывать, копировать, удалять и включать) учетные записи, изменять и сбрасывать пароли. Также мы поговорим о решении проблем с входом в учетную запись.

Переименование учетных записей пользователя и группы

При переименовании учетной записи пользователя ей просто назначается новая метка. Как было упомянуто в *главе 8*, имена пользователей просто облегчают управление и использование учетных записей. Но за кулисами Windows Server использует идентификаторы безопасности (Security ID, SID) для идентификации, отслеживания и управления учетными записями независимо от имен пользователя. SID — это уникальные идентификаторы, генерируемые при создании учетных записей.

Поскольку SID отображаются внутренне в имена учетных записей, не нужно изменять привилегии или разрешения для переименованных учетных записей. ОС Windows Server просто отобразит SID в новое имя учетной записи.

Одна из наиболее частых причин изменения имени учетной записи пользователя — смена фамилии. Например, если Светлана Иванова (svetai) вышла замуж, она может захотеть изменить свое имя пользователя на Светлана Петрова (svetap). При изменении имени пользователя с svetai на svetap все соответствующие привилегии и полномочия сразу отразят смену имени.

Чтобы упростить процесс переименования учетных записей пользователей, оснастка **Active Directory — пользователи и компьютеры** предоставляет диалоговое окно **Переименование пользователя** (Rename User), которое можно использовать для изменения имени учетной записи пользователя и всех связанных компонентов имени. В настоящее время это окно отсутствует в оснастке Центр администрирования Active Directory, поэтому для переименования пользователя нужно открыть окно **Свойства** пользователя и изменить значения соответствующих текстовых полей.

Для переименования учетной записи выполните следующие действия:

1. Найдите в оснастке **Active Directory — пользователи и компьютеры** учетную запись, которую нужно переименовать.
2. Щелкните правой кнопкой мыши по имени пользователя и выберите команду **Переименовать** (Rename). Оснастка подсветит редактируемую учетную запись. Нажмите клавишу <Backspace> или <Delete>, чтобы стереть существующее имя, а затем нажмите клавишу <Enter> для открытия окна **Переименование пользователя** (Rename User) (рис. 9.12).
3. Внесите необходимые изменения в информацию об имени пользователя и затем нажмите кнопку **OK**. Если пользователь вошел, будет показано предупреждение, что пользователь должен сначала выйти, а затем снова войти для использования нового имени учетной записи.

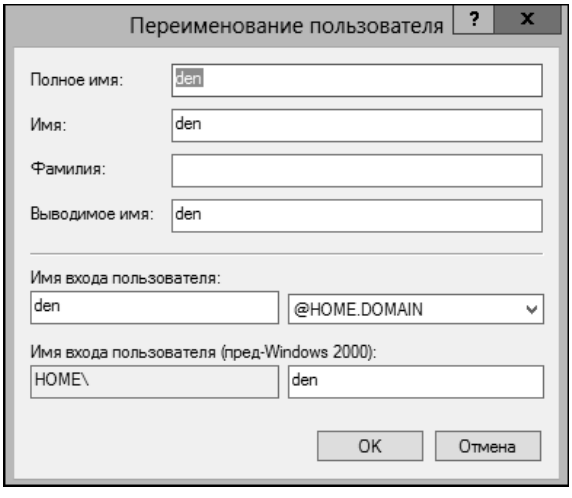


Рис. 9.12. Полное переименование учетной записи

4. Учетная запись будет переименована, а SID для разрешений доступа останется тем же. Однако нужно еще модифицировать другие данные в окне **Свойства** пользователя:
   - **Путь к профилю** (User Profile Path) — измените путь к профилю в оснастке **Active Directory — пользователи и компьютеры** и переименуйте соответствующий каталог на диске;
   - **Сценарий входа** (Logon Script Name) — если используете индивидуальные сценарии входа для каждого пользователя, измените имя сценария в оснастке **Active Directory — пользователи и компьютеры** и переименуйте соответствующий сценарий на диске;
   - **Домашняя папка** (Home Directory) — измените путь к домашней папке в оснастке **Active Directory — пользователи и компьютеры** и переименуйте соответствующий каталог на диске.

   Примечание

   Изменение имени каталога для учетной записи во время работы пользователя может вызвать проблемы. Нужно обновить эту информацию вне рабочего времени или попросить пользователя выйти и войти снова через несколько минут. Обычно можно написать простой Windows-сценарий, осуществляющий эти задачи автоматически.

Копирование учетных записей пользователя домена

Создание учетных записей пользователей домена с нуля может быть весьма утомительным занятием. Вместо того чтобы каждый раз создавать новую учетную запись, можно использовать существующую учетную запись в качестве начальной точки. На данный момент эта возможность отсутствует в оснастке Центр администрирования Active Directory. Чтобы сделать это в оснастке **Active Directory — пользователи и компьютеры**, выполните следующие действия:

1. Щелкните правой кнопкой мыши на учетной записи, которую нужно скопировать, и нажмите кнопку **Копировать** (Copy). Откроется окно **Копировать объект — Пользователь** (Copy Object — User).

2. Создайте учетную запись, как и любую другую учетную запись пользователя домена, а затем обновите свойства учетной записи.

Как можно было бы ожидать, при создании копии учетной записи оснастка **Active Directory — пользователи и компьютеры** сохраняет не всю информацию из существующей учетной записи. Вместо этого оснастка пытается сохранить только необходимую информацию и отбрасывает сведения, которые нужно обновить. Следующие свойства будут сохранены:

- город, область, почтовый индекс, страна — свойства с вкладки **Адрес** (Address);
- отдел и компания — свойства с вкладки **Организация** (Organization);
- параметры учетной записи, установленные в блоке **Параметры учетной записи** (Account Options) на вкладке **Учетная запись** (Account);
- время входа и разрешенные рабочие станции;
- срок действия учетной записи;
- членство в группах;
- настройки профиля;
- привилегии входящих звонков.

> ***Примечание***
>
> Если использовались переменные среды для определения настроек профиля в исходной учетной записи, переменные окружения, как правило, используются и для копии учетной записи. Например, если исходная учетная запись использовала переменную `%UserName%`, то и копия учетной записи будет также использовать эту переменную.

Импорт и экспорт учетных записей

Операционная система Windows Server 2012 содержит утилиту командной строки CSVDE (Comma-Separated Value Directory Exchange), которая применяется для импорта и экспорта объектов Active Directory. Для операций импорта CSVDE использует файл в формате CSV (текст, разделенный запятыми) в качестве источника импорта.

Запустить CSVDE можно со следующими параметрами:

- `-i` — включает режим импорта (по умолчанию используется режим экспорта);
- `-f` *`имя_файла`* — устанавливает источник для операции импорта и результирующий файл для операции экспорта;
- `-s` *`имя_сервера`* — устанавливает сервер, используемый для импорта и экспорта;
- `-v` — включает подробный режим.

Для операций импорта первая строка файла-источника определяет список атрибутов LDAP (Lightweight Directory Access Protocol) для каждого конкретного объекта. Каждая строка данных предоставляет подробности по определенному объекту импорта и должна содержать точно перечисленные атрибуты. Пример:

```
DN,objectClass,sAMAccoutName,sn,givenName,userPrincipalName "CN=William
Stanek,OU=Eng,DC=cpandl,DC=com",user,williams,William,Stanek, williams@cpandl.com
```

При условии, что файл источника импорта называется newusers.csv, можно импортировать его в Active Directory командой:

```
csvde -i newusers.csv
```

При операциях CVSDE записывает экспортируемые объекты в файл, разделяя их запятыми. Можно запустить CSVDE со следующими параметрами:

- `-d` *`RootDN`* — устанавливает начальную точку для экспорта, например, `-d "OU=Sales, DC=domain,DC=local"`. Это текущий контекст имен по умолчанию;
- `-l` *`список`* — предоставляет разделенный запятыми список атрибутов вывода;
- `-r` *`фильтр`* — устанавливает поисковый фильтр LDAP, например, `-r "(objectClass=user)"`;
- `-m` — настраивает вывод для SAM (Security Accounts Manager), а не для Active Directory.

Чтобы экспортировать текущий контекст имен (домен по умолчанию), можно ввести следующую команду в командной строке:

```
csvde -f newusers.csv
```

Однако в результате будет создан очень большой файл. В большинстве случаев нужно указать как минимум *`RootDN`* и фильтр объектов, например:

```
csvde -f newusers.csv -d "OU=Service,DC=cpandl,DC=com" -r "(objectClass=user)"
```

Удаление учетных записей пользователя и группы

При удалении учетной записи она удаляется безвозвратно. Удалив учетную запись, нельзя создать новую с таким же именем, чтобы получить такие же разрешения. Это происходит, потому что SID новой учетной записи не совпадает с SID старой учетной записи.

Поскольку удаление встроенных учетных записей может иметь далеко идущие последствия для домена, операционная система Windows Server 2012 не позволяет удалять встроенные учетные записи пользователей или учетные записи группы. Можно удалить учетные записи других типов, выбрав их и нажав клавишу <Delete> или же щелкнув на записи правой кнопкой мыши и выбрав команду **Удалить** (Delete). Для подтверждения намерения следует нажать кнопку **Да**.

В оснастке **Active Directory — пользователи и компьютеры** можно выбрать несколько объектов одним из двух способов:

- для выбора нескольких имен пользователей нажмите и удерживайте клавишу <Ctrl>, а затем щелкните на каждой учетной записи, которую нужно выбрать;
- можно выбрать диапазон учетных записей с помощью клавиши <Shift>: нажмите и удерживайте ее, потом щелкните на первой учетной записи, а затем — на последней учетной записи диапазона.

> ***Примечание***
>
> При удалении учетной записи пользователя Windows Server 2012 не удаляет профиль пользователя, его личные файлы и домашний каталог. Если необходимо удалить эти файлы и каталоги, нужно сделать это вручную. Задача довольно рутинная, поэтому нужно написать сценарий, который автоматизирует описанные процедуры. Однако не забудьте сделать резервную копию файлов или данных перед удалением.

Изменение и сброс паролей

Администратору часто приходится изменять или сбрасывать пароли пользователей. Данная ситуация может произойти, когда пользователь забудет пароль или закончится срок его действия.

Для изменения или сброса пароля выполните следующие действия:

1. Откройте оснастку **Active Directory — пользователи и компьютеры**, Центр администрирования Active Directory или утилиту **Локальные пользователи и группы** (в зависимости от типа учетной записи).
2. Щелкните правой кнопкой мыши на учетной записи и выберите команду **Сбросить пароль** (Reset Password) или **Смена пароля** (Set Password).
3. Введите новый пароль пользователя и подтвердите его. Пароль должен соответствовать политике сложности пароля для компьютера или домена.
4. Параметр **Требовать смены пароля при следующем входе в систему** (Must Change Password At Next Logon) заставит пользователя изменить его пароль при следующем входе в систему. Если не нужно, чтобы пользователь изменял свой пароль, выключите этот параметр.
5. Параметр **Разблокировать учетную запись пользователя** (Account Lockout Status On This Domain Controller) позволяет разблокировать заблокированную учетную запись. Если учетная запись заблокирована, включите этот параметр и нажмите кнопку **OK**.

Включение учетных записей пользователя

Учетные записи пользователей могут оказаться отключенными по нескольким причинам. Если пользователь забыл свой пароль и пытается подобрать его, он может превысить число неудачных попыток входа. Другой администратор может отключить учетную запись, пока пользователь был в отпуске, или же срок действия учетной записи может истечь. В следующем разделе будет описано, что делать, если учетная запись отключена, заблокирована или срок ее действия истек.

Учетная запись отключена

Оснастка **Active Directory — пользователи и компьютеры** и Центр администрирования Active Directory помечают отключенные учетные записи стрелкой черного цвета, направленной вниз, в левом нижнем углу значка учетной записи в списке учетных записей. Когда учетная запись отключена, можно включить ее с помощью следующих действий:

1. Откройте оснастку **Active Directory — пользователи и компьютеры**, Центр администрирования Active Directory или утилиту **Локальные пользователи и группы**.
2. Щелкните правой кнопкой мыши по имени учетной записи пользователя, выберите соответствующую команду, ее название зависит от используемой утилиты, например **Включить** (Enable) или **Включить учетную запись** (Enable Account).

> ***Совет***
>
> Чтобы быстро найти отключенные учетные записи в текущем домене, в командной строке введите команду `dsquery user -disabled`.

Можно выбрать несколько учетных записей одновременно, а затем щелкнуть на выделении правой кнопкой мыши и использовать команды контекстного меню для их включения или отключения. В оснастке **Active Directory — пользователи и компьютеры** можно включить все выбранные учетные записи с помощью команды **Включить учетную запись** (Enable Account) или отключить командой **Отключить учетную запись** (Disable Account). В оснастке Центр администрирования Active Directory можно включить все учетные записи,

используя команду **Включить все** (Enable All), а отключить — командой **Отключить все** (Disable All).

Учетная запись заблокирована

Для разблокировки учетной записи выполните следующие действия:

1. Откройте оснастку **Active Directory — пользователи и компьютеры**, Центр администрирования Active Directory или **Локальные пользователи и группы** (Local Users And Groups).
2. Дважды щелкните на учетной записи и установите флажок **Разблокировать учетную запись** (Unlock Account). В оснастке **Active Directory — пользователи и компьютеры** этот флажок находится на вкладке **Учетная запись** (Account).

В Центре администрирования Active Directory можно разблокировать несколько учетных записей одновременно. Просто выделите заблокированные учетные записи и выберите команду **Разблокировать все** (Unlock All) из контекстного меню.

> ***Примечание***
>
> Если у пользователей часто блокируются учетные записи, рекомендуется пересмотреть политику учетной записи для домена. Нужно увеличить число попыток входа в систему и уменьшить продолжительность блокировки. Для более подробной информации обратитесь к *главе 8*.

Срок действия учетной записи истек

Срок действия есть только у учетных записей домена (у локальных учетных записей пользователей нет срока действия). Когда срок действия истекает, нужно выполнить следующие действия:

1. Откройте оснастку **Active Directory — пользователи и компьютеры** или Центр администрирования Active Directory.
2. Дважды щелкните по имени учетной записи пользователя. Откройте вкладку/панель **Учетная запись** (Account).
3. В области **Срок действия учетной записи** (Account Expires) нажмите стрелку вниз возле поля **Истекает** (End Of). В оснастке **Active Directory — пользователи и компьютеры** будет отображен календарь, позволяющий установить новую дату окончания учетной записи. В Центре администрирования Active Directory введите дату в предложенном формате.

Управление несколькими учетными записями

Оснастку **Active Directory — пользователи и компьютеры** можно использовать для изменения свойств сразу нескольких учетных записей. Любые изменения свойств будут применены сразу ко всем выбранным учетным записям. Выделите учетные записи и щелкните на выделении правой кнопкой мыши, появится меню со следующими командами:

- **Добавить в группу** (Add To A Group) — отобразит окно **Выбор: "Группы"** (Select Group), в котором можно назначить группы, членами которых должны быть выбранные пользователи;
- **Отключить учетную запись** (Disable Account) — отключает все выбранные учетные записи;

- **Включить учетную запись** (Enable Account) — включает все выбранные учетные записи;
- **Переместить** (Move) — перемещает выбранные учетные записи в новый контейнер или организационное подразделение;
- **Вырезать** (Cut) — перемещает выбранные учетные записи в новый контейнер или организационное подразделение, после выбора этой команды нужно перейти в другой контейнер и выбрать команду **Вставить** (Paste);
- **Удалить** (Delete) — удаляет выбранные учетные записи из каталога;
- **Свойства** — позволяет настроить ограниченный набор свойств для нескольких учетных записей.

В оснастке Центр администрирования Active Directory параметры подобны: **Добавить в группу** (Add To Group), **Отключить все** (Disable All), **Включить все** (Enable All), **Разблокировать все** (Unlock All), **Переместить** (Move), **Удалить** (Delete) и **Свойства**.

Команду **Свойства** мы уже рассматривали. Как показано на рис. 9.13, интерфейс окна **Свойства множественных элементов** (Properties For Multiple Items) отличается от интерфейса окна **Свойства** для одного пользователя.

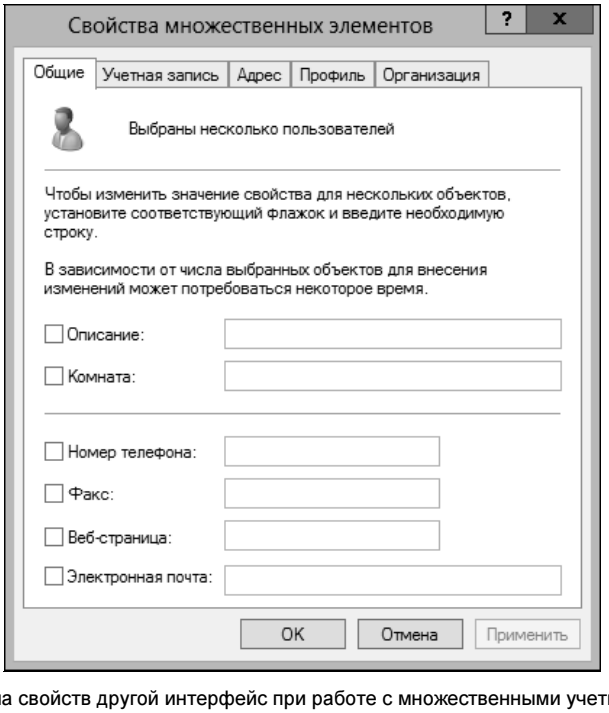


Рис. 9.13. У окна свойств другой интерфейс при работе с множественными учетными записями

Примечание

Примеры, показанные здесь и в следующих разделах, приводятся на базе оснастки **Active Directory — пользователи и компьютеры**. Методы управления аналогичны и для Центра администрирования Active Directory.

Нужно отметить следующую разницу:

- поля, позволяющие устанавливать имя и пароль учетной записи, больше недоступны. Однако можно установить доменное имя DNS (суффикс UPN, User Principal Name), часы

входа, ограничения компьютеров, параметры учетной записи, срок действия учетной записи и профили;

- необходимо выбрать свойства, с которыми нужно работать, установив флажки свойств. После этого значение, введенное в текстовое поле, будет применено ко всем выбранным учетным записям.

Установка профилей для нескольких учетных записей

Установить параметры профиля для нескольких учетных записей сразу можно на вкладке **Профиль**. Одна из причин работы с несколькими учетными записями в оснастке **Active Directory — пользователи и компьютеры** заключается в том, что можно установить все их профили окружения, используя один интерфейс. Чтобы сделать это, используйте переменную среды `%UserName%`, позволяющую назначить пути и имена файлов, которые базируются на отдельных именах пользователей. Например, если назначить имя входного сценария как `%UserName%.cmd`, Windows заменит это значение именем пользователя для каждого управляемого вами пользователя. Пользователям с именами bobs, janew и ericl будут назначены следующие сценарии входа: bobs.cmd, janew.cmd и ericl.cmd.

На рис. 9.14 показан пример установки информации среды профиля для нескольких учетных записей. Заметьте, что переменная `%UserName%` используется для назначения пути профиля, сценария входа пользователя и домашней папки.

Хотя можно назначить всем пользователям уникальные имена файлов и путей, иногда пользователи должны разделять эту информацию. Например, если используются обязательные профили для пользователей, можно назначить определенный путь профиля, а не создавать их динамически.

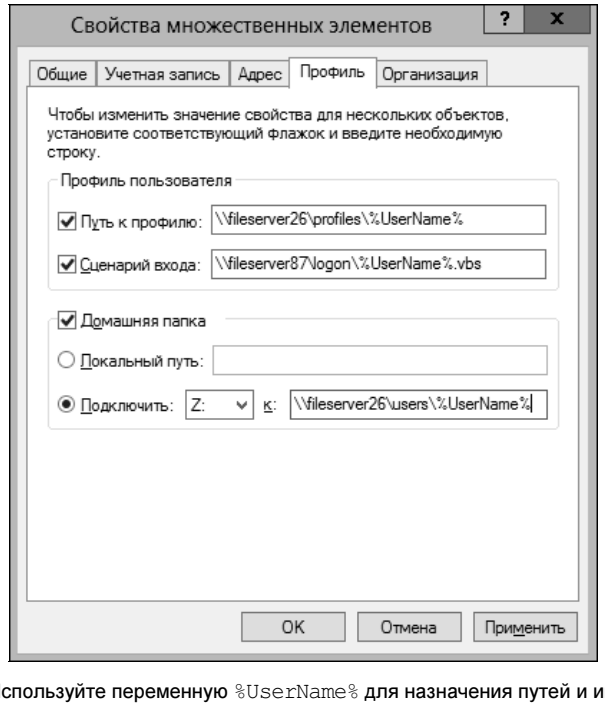


Рис. 9.14. Используйте переменную `%UserName%` для назначения путей и имен файлов на основании имен отдельных пользователей

Установка часов входа для нескольких учетных записей

При выборе нескольких учетных записей в оснастке **Active Directory — пользователи и компьютеры** можно управлять их часами входа коллективно. Чтобы сделать это, выполните следующие действия:

1. Выберите учетные записи, с которыми нужно работать в оснастке **Active Directory — пользователи и компьютеры**.
2. Щелкните правой кнопкой мыши на выделенных учетных записях и выберите команду **Свойства**. В окне **Свойства множественных элементов** (Properties For Multiple Items) перейдите на вкладку **Учетная запись** (Account).
3. Установите флажок **Время входа** (Logon Hours) и нажмите кнопку **Время входа** (Logon Hours). Как устанавливать часы входа, мы уже знаем *(см. разд. "Управление часами входа" ранее в этой главе)*.

> ***Примечание***
>
> Оснастка **Active Directory — пользователи и компьютеры** не показывает ранее установленные часы входа для выбранных учетных записей и не предупреждает, если часы входа для учетных записей отличаются.

Установка разрешенных для входа рабочих станций для множественных учетных записей

Можно установить разрешенные для входа рабочие станции для нескольких учетных записей с помощью окна **Рабочие станции для входа в систему** (Logon Workstations). Чтобы открыть это окно, выполните следующие действия:

1. Выберите учетные записи, с которыми можно работать, в оснастке **Active Directory — пользователи и компьютеры**.
2. Щелкните правой кнопкой мыши по выделенным учетным записям и выберите команду **Свойства**. В окне **Свойства множественных элементов** перейдите на вкладку **Учетная запись**.
3. Установите флажок **Ограничения компьютера** (Computer Restrictions) и нажмите кнопку **Вход на** (Log On To).
4. Если нужно разрешить пользователям входить с любой рабочей станции, выберите переключатель **На все компьютеры** (All Computers). Если нужно указать, с каких рабочих станций пользователям разрешено входить, выберите **Только на указанные компьютеры** (The Following Computers), а затем введите имена рабочих станций. После нажатия кнопки **OK** эти настройки будут применены ко всем выбранным учетным записям пользователей.

Установка свойств входа, пароля и срока действия для множественных учетных записей

Учетные записи пользователей обладают многими параметрами, позволяющими контролировать вход, пароли и срок действия учетной записи. Все эти параметры можно установить на вкладке **Учетная запись** окна **Свойства множественных элементов**. При работе

с множественными учетными записями для включения необходимой опции установите соответствующий ей флажок в крайнем левом столбце[1]. После этого есть два варианта:

- включить опцию, выбрав ее флажок. Например, если работаете с опцией **Срок действия пароля не ограничен** (Password Never Expires), установка флажка означает, что срок действия пароля не будет ограничен для всех выбранных учетных записей после нажатия кнопки **OK**;
- не устанавливать опцию, для чего нужно сбросить флажок. Например, при работе с опцией **Отключить учетную запись** (Account Is Disabled) после нажатия кнопки **OK** выбранные учетные записи будут включены.

Если нужно установить срок действия для выбранных учетных записей, установите флажок **Срок действия учетной записи** (Account Expires) и потом выберите подходящую дату окончания. Параметр **Никогда** (Never) удаляет любые ранее установленные ограничения срока действия. Параметр **Истекает** (End Of) позволяет установить определенную дату окончания срока действия.

Решение проблем с входом в систему

Ранее были представлены способы отключения учетной записи. В оснастке **Active Directory — пользователи и компьютеры** отключенные учетные записи помечаются черной стрелкой, направленной вниз, в правом нижнем углу значка учетной записи. Для включения учетной записи щелкните на ней правой кнопкой мыши и выберите команду **Включить учетную запись** (Enable Account).

Можно также произвести поиск всех отключенных учетных записей в домене с помощью команды `dsquery user -disabled` в командной строке. Для включения отключенной учетной записи из командной строки введите команду `dsmod user UserDN -disabled no`.

Заблокированную политикой блокировки учетную запись пользователя нельзя использовать для входа, пока не выйдет время блокировки или администратор не сбросит учетную запись. Если продолжительность блокировки учетной записи не определена, единственный способ разблокировать учетную запись заключается в ее сбросе, что и было показано ранее.

Операционная система Windows Server 2012 может записывать удачные и неудачные попытки входа. После включения аудита неудачных попыток входа неудачные попытки входа заносятся в журнал безопасности контроллера домена. Политики аудита для GPO сайта, домена или организационного подразделения находятся в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита** (Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy).

Когда пользователь входит в сеть с использованием своей учетной записи домена, учетные данные учетной записи проверяются контроллером домена. По умолчанию пользователи могут войти в систему посредством своих учетных записей пользователей домена, даже если произошел сбой сети или ни один контроллер домена, способный аутентифицировать вход в систему пользователя, не доступен.

---

[1] В области **Параметры учетной записи** будут два флажка. Крайний левый позволяет отметить опции, которые нужно переустановить для множественных учетных записей. Второй флажок, который находится ближе к названию параметра, используется для установки значения параметра. Если флажок установлен, то и параметр включен, и наоборот. — *Прим. пер.*

Для этого нужно, чтобы пользователь ранее входил в компьютер и его учетные данные были кэшированы. Если учетные данные не были ранее кэшированы, сеть недоступна или недоступен контроллер домена, пользователю не удастся войти в систему. Каждый компьютер в домене может кэшировать до 10 учетных данных по умолчанию.

Когда домен работает в режиме Windows 2000 или Windows Server 2003, сбой аутентификации может произойти, если системное время рядового компьютера отличается от системного времени контроллера домена входа больше, чем разрешено в политике **Политика Kerberos: Максимальная погрешность синхронизации часов компьютера** (Kerberos Policy: Maximum Tolerance For Computer Clock Synchronization). Максимальная погрешность по умолчанию равна 5 минутам для рядовых компьютеров.

Кроме этих типичных причин отключения учетной записи некоторые параметры системы могут также вызывать проблемы доступа. В частности, нужно обратить внимание на следующее.

- **Пользователь получает сообщение о том, что он не может войти интерактивно.** Право интерактивного входа не установлено для пользователя или для группы, членом которой является пользователь. Пользователь может попытаться войти в сервер или контроллер домена. Если это так, имейте в виду, что право интерактивного входа применяется ко всем контроллерам домена. В противном случае это правило применяется только к единственной рабочей станции. Если у пользователя, как предполагается, есть доступ к локальной системе, настройте право **Локальный вход** (Logon Locally) в систему, как было показано в *главе 8*.
- **Пользователь получает сообщение, что не может войти в систему**. Если имя пользователя и пароль уже проверены, можно попробовать проверить тип учетной записи. Пользователь может попытаться получить доступ к домену, используя локальную учетную запись. Если проблема не в этом, в сети может быть недоступен глобальный каталог, и это означает, что войти в домен могут только пользователи с полномочиями администратора.
- **У пользователя есть обязательный профиль, и компьютер, хранящий профиль, недоступен.** Если у пользователя обязательный профиль, компьютер, хранящий профиль, должен быть доступен во время входа в систему. Если компьютер выключен или недоступен по другой причине, пользователи с обязательными профилями не смогут войти в систему *(см. разд. "Локальные, перемещаемые и обязательные профили" ранее в этой главе)*.
- **Пользователь получает сообщение о том, что система настроена для предотвращения входа с рабочей станции.** Пользователь пытается получить доступ с рабочей станции, которая не определена как разрешенная рабочая станция. Если пользователь должен иметь доступ к этой рабочей станции, измените настройки входа в систему, как было показано в *разд. "Установка разрешенных для входа рабочих станций" ранее в этой главе*.

Просмотр и установка разрешений Active Directory

Учетные записи пользователя, группы и компьютера представлены в Active Directory как объекты. У объектов Active Directory есть стандартные и расширенные разрешения безопасности, которые могут предоставить или запретить доступ к объектам.

Разрешения для объектов Active Directory не столь прямые, как другие разрешения. У различных типов объектов могут быть наборы полномочий, которые являются специфическими для объекта определенного типа. У них также могут быть общие разрешения, которые являются специфическими для контейнера, в котором они определены.

Можно просмотреть и установить стандартные права доступа для объектов, выполнив следующие действия:

1. Откройте оснастку **Active Directory — пользователи и компьютеры** и включите отображения дополнительных параметров, выбрав команду **Дополнительные компоненты** (Advanced features) из меню **Вид** (View). Далее щелкните правой кнопкой мыши на учетной записи пользователя, группы или компьютера, с которой нужно работать, и выберите команду **Свойства**.
2. В окне **Свойства** перейдите на вкладку **Безопасность** (Security). Будет отображен список групп и пользователей (рис. 9.15), которым были назначены разрешения для выбранного объекта. Если разрешения недоступны, это означает, что они наследуются из родительского объекта.
3. Пользователи или группы с разрешениями доступа приводятся в списке **Группы или пользователи** (Group or user names).

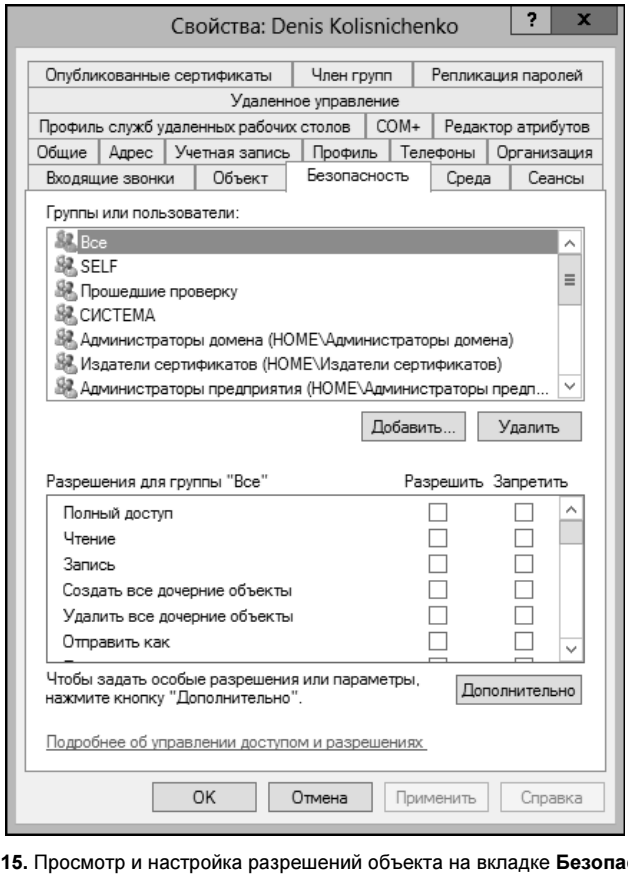


Рис. 9.15. Просмотр и настройка разрешений объекта на вкладке **Безопасность**

Можно изменить разрешения для этих пользователей или групп так:

- выберите пользователя или группу, которые нужно изменить;
- предоставьте или запретите разрешения в списке **Разрешения для** (Permissions for);
- если наследованные разрешения недоступны, переопределите разрешения полномочия, выбрав противоположные значения.

4. Чтобы установить разрешения доступа для дополнительных пользователей, компьютеров или групп, нажмите кнопку **Добавить**. В окне **Выбор: "Пользователи", "Компьютеры", "Учетные записи" или "Группы"** (Select Users, Computers, Service Accounts, or Groups) добавьте пользователей, компьютеры или группы.
5. В списке **Группы или пользователи** выберите пользователя, компьютер или группу, которые нужно настроить. Нажмите кнопку **Проверить имена**, а затем — кнопку **OK**. В области **Разрешения** с помощью флажков предоставьте или запретите разрешения. Повторите этот шаг для других пользователей, компьютеров или групп.
6. Нажмите кнопку **OK**, когда все будет готово.

> ***Осторожно!***
>
> Только администраторы с глубоким пониманием Active Directory и разрешений Active Directory могут изменять разрешения объекта. Некорректная установка разрешений объекта может вызвать проблемы, которые будет очень сложно отследить.

Для просмотра и установки расширенных разрешений безопасности выполните следующие действия:

1. Откройте оснастку **Active Directory — пользователи и компьютеры** и включите отображения дополнительных параметров, выбрав команду **Дополнительные компоненты** в меню **Вид**. Далее щелкните правой кнопкой мыши на учетной записи пользователя, группы или компьютера, с которыми нужно работать, и выберите команду **Свойства**.
2. В окне **Свойства** перейдите на вкладку **Безопасность** и нажмите кнопку **Дополнительно** (Advanced). Будет отображен список отдельных разрешений для ранее выбранного объекта. Колонка **Унаследовано от** (Inherited) позволяет узнать, от какого родительского объекта были унаследованы разрешения.
3. Для просмотра и установки отдельных разрешений, связанных с записью разрешения, выберите запись, а затем нажмите кнопку **Изменить**. Можно изменить расширенные разрешения для выбранного пользователя или группы путем предоставления или запрещения разрешений доступа в списке **Разрешения**. Когда наследованные разрешения недоступны, переопределите их, выбрав противоположные значения.
4. Нажмите кнопку **OK** дважды.

часть III

Администрирование данных Windows Server 2012

ГЛАВА 10

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 установлены 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 11* мы поговорим о настройке томов и RAID-массивов для обеспечения отказоустойчивости.

Управление ролью *Файловые службы*

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. В более ранних версиях операционной системы Microsoft Windows Server все серверы устанавливались с базовыми файловыми службами.

В случае с Windows Server 2012 нужно специально настроить сервер в качестве файлового сервера, добавив роль **Файловые службы** (File Services) и настроив эту роль использовать надлежащие службы роли.

В табл. 10.1 предоставлен обзор служб роли, связанных с ролью **Файловые службы**. При установке роли **Файловые службы** может понадобиться 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.

Если двоичные файлы утилит были удалены, нужно установить утилиты из определенного источника, как было показано в *главе 2*.

Таблица 10.1. *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, хранящиеся 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) 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
Файловый сервер (File Server)	Позволяет управлять совместно используемыми файлами, к которым пользователи могут получить доступ по всей сети

Таблица 10.1 *(окончание)*

Служба роли	Описание
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

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

1. В окне диспетчер серверов в меню **Управление** выберите команду **Добавить роли и компоненты** 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**.
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 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 жесткий диск (virtual hard disk, VHD). Если роли и компоненты добавляются на VHD, нажмите кнопку **Обзор**, 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.

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

Примечание

Краткое описание каждой службы роли приведено в табл. 10.1. Чтобы разрешить взаимодействие с UNIX, выберите **Сервер для NFS** (Server for NFS).

5. На странице **Выбор компонентов** (Features) выберите один или несколько компонентов для установки. Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, будет отображено дополнительное диалоговое окно. Нажмите кнопку **Добавить компоненты** для закрытия этого окна и установки требуемых компонентов на сервер. По окончанию выбора компонентов нажмите кнопку **Далее**.
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.
7. 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.

Практический совет

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**. Например, если образ Windows смонтирован и доступен на локальном сервере *(см. разд. "Основные компоненты диспетчера серверов и двоичные файлы" главы 2)*, можно ввести альтернативный путь в виде c:\mountdir\windows\winsxs. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer20120\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2-12\install.wim:4.

8. 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 щелкните по ссылке, предназначенной для повторного открытия мастера.
9. 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** уже установлена на сервере и необходимо установить дополнительные службы для файлового сервера, 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 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 улучшения надежности и производительности необходимо заставить работать вместе набор дисков. ОС Windows Server 2012 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 используются для хранения данных. Объем записанных на диск данных зависит от его размера и от того, используется ли сжатие. ОС Windows Server 2012 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 *дисками 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 байтов).

ОС Windows Server 2012 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 как 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 так же 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. Например, у Maxtor Atlas 15K II максимальная устойчивая скорость передачи данных равна 98 Мбайт/с. У Seagate Cheetah 15K.4 максимальная устойчивая скорость равна 96 Мбайт/с. У обеих моделей MTTF равен 1,4 млн часов. 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. Средняя скорость длительной передачи — наиболее важный фактор. У Seagate Barracuda 7200 SATA II скорость вращения 7200 об/мин, а средняя скорость длительной передачи — 58 Мбайт/с. Со средним временем поиска в 8,5 мс и MTTF 1 млн часов диск выделяется среди других дисков SATA II со скоростью 7200 об/мин. Однако у большинства дисков SCSI Ultra320 производительность выше, особенно в многопользовательских операциях чтения/записи.

> ***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 частота 800 Мбит/с. В случае с SATA максимальная частота передачи данных обычно около 150 Мбайт/с или 300 Мбит/с. При использовании PATA/IDE максимальная частота передачи данных обычно около 100 Мбайт/с.

Температура — другой важный фактор, на который нужно обратить внимание при выборе диска, но его принимают во внимание немного администраторов. 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 Maxtor Atlas 15K II и Seagate Cheetah 15K.4 температура отказа составляет 70° C и выше (как и в случае с большинством других дисков).

Операционная система Windows Server 2012 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 будет использовать аппаратное шифрование с BitLocker, если это возможно. Другие средства защиты, доступные в Windows Server 2012, 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.

На дисках используются разделы двух типов: главная загрузочная запись (Master Boot Record, MBR) и таблица разделов GUID (GUID partition table, GPT). MBR содержит таблицу

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

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.

При использовании 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. GPT рекомендуется использовать для дисков, больших 2 Тбайт на *x*86 и *x*64 или на любых дисках, установленных в компьютер на базе 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.

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 поддерживает следующие файловые системы:

- FAT;
- FAT32;
- exFAT;
- NTFS;
- ReFS.

В случае с FAT число бит, 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 битов. 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 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, ко-

торый был в FAT32. Файловая система exFAT поддерживает размеры кластера до 128 Кбайт для томов до 256 Тбайт.

У томов NTFS совсем другая структура и 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 поддерживает пространства хранения, помните об этом при форматировании тома на файловых серверах. Для получения дополнительной информации о пространствах хранения обратитесь к *главе 11*.

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).

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

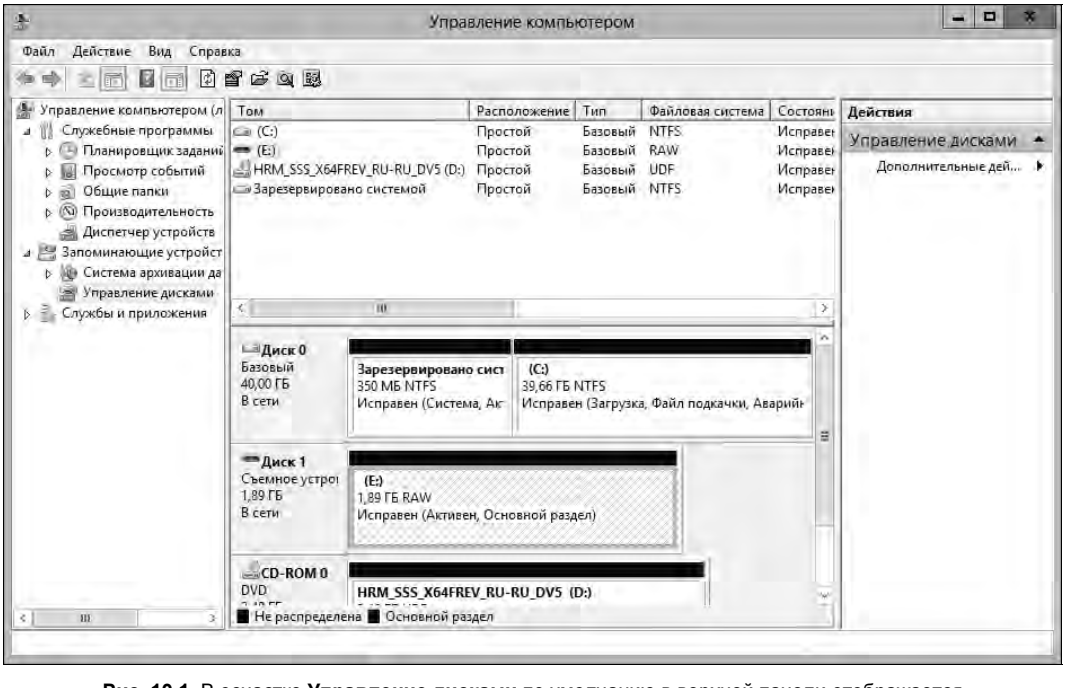


Рис. 10.1. В оснастке **Управление дисками** по умолчанию в верхней панели отображается сводка по всем дискам, а нижняя панель предоставляет обзор этих же дисков

ОС Windows Server 2012 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.

- **Динамический** — расширенный тип жесткого диска (фиксированный) для Windows Server 2012, который можно обновлять без необходимости перезапуска системы (в большинстве случаев). Динамические диски делятся на тома.
- **Сменный** — 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 они используют 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. 10.2 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.

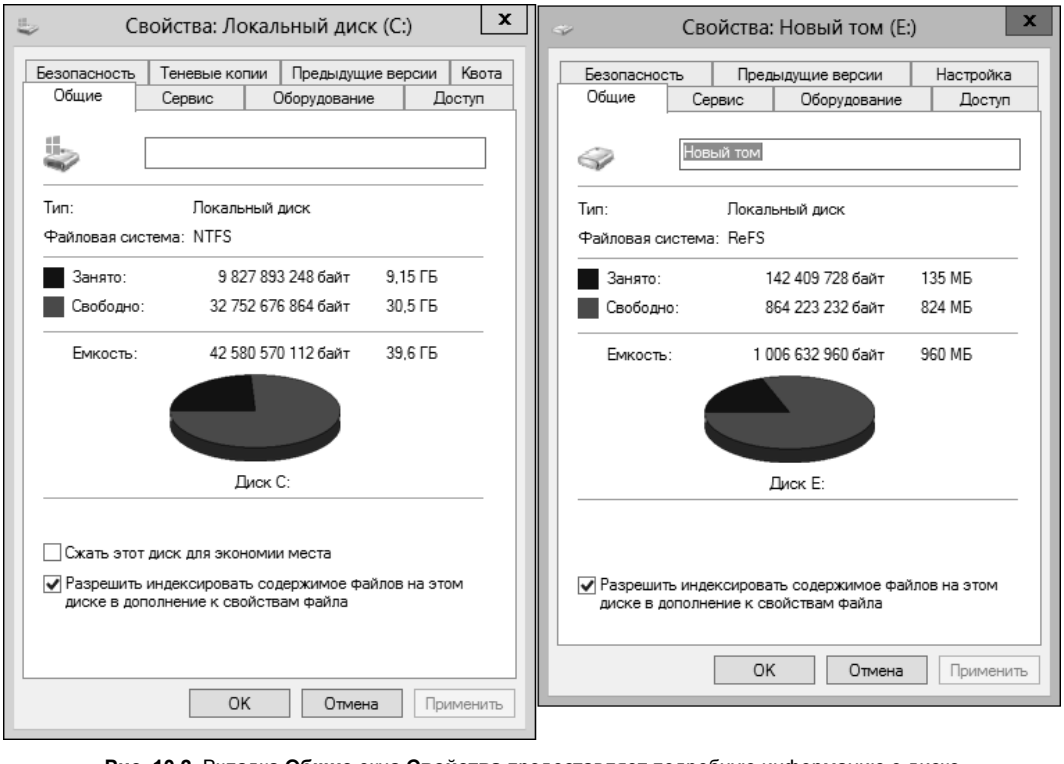


Рис. 10.2. Вкладка **Общие** окна **Свойства** предоставляет подробную информацию о диске

Если настроено удаленное управление через диспетчер серверов и MMC, как было показано в *главе 2*, 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.

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 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 медленнее, 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 Мбит/с (S400), 800 Мбит/с (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:

1. Щелкните правой кнопкой мыши по сменному носителю и выберите команду **Открыть** (Open) или **Проводник** (Explore), чтобы исследовать содержимое диска в Проводнике.
2. 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.
3. 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 11)*.

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 одновременных 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, разрешается 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 такие 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 запишет дисковую подпись на диски и инициализирует диски 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.

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. 10.2 представлены общие значения состояния.

Таблица 10.2. *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
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

Таблица 10.2 *(окончание)*

Состояние	Описание	Резолюция
Вне сети (Offline)	Диск недоступен и может быть поврежден или временно недоступен. Если имя диска изменено на **Отсутствует** (Missing), диск больше 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 **Рективировать 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
Неопознан (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 использовать этот диск на компьютере, поэтому попытайтесь использовать другой диск
Не проинициализирован (Not Initialized)	У диска нет верной подписи. Это состояние может отображать диск с не-Windows файловой системой	Если диск относится к другой операционной системе, ничего не делайте. Этот диск нельзя использовать на компьютере. Для подготовки диска с целью использования в Windows Server 2012 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 поддерживает базовые, дисковые и виртуальные конфигурации дисков. В этом разделе обсуждаются техники работы с диском каждого типа конфигурации.

> ***Примечание***
>
> Невозможно использовать динамические диски на портативных компьютерах или со сменными носителями.

Использование базовых и динамических дисков

Обычно разделы диска Windows Server 2012 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 диски 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 доступны следующие действия:

- форматировать разделы и помечать их как активные;
- создавать и удалять первичные и расширенные разделы;
- создавать и удалять логические диски на расширенных разделах.

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.

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.

> ***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

Базовые диски разработаны для использования с предыдущими версиями Windows. Динамические диски позволят получить все преимущества последних функций Windows. Только компьютеры, работающие под управлением Windows 2000 и более поздних версий Windows, могут использовать динамические диски. Однако динамические диски могут использоваться и с другими операционными системами, например, в UNIX. Чтобы сделать это, необходимо создать отдельный том для не-Windows операционной системы. На портативных компьютерах использовать динамические диски невозможно.

Операционная система Windows Server 2012 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. Только компьютеры под управлением Windows 2000 и более поздних версий могут использовать динамические диски.

В случае с MBR-дисками также нужно убедиться, 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.

- Должно 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 Windows Server 2012.

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 используется — **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. При преобразовании составного, чередующегося, зеркалируемого или RAID 5 тома убедитесь, что выбраны все базовые диски в этом наборе. Необходимо конвертировать набор дисков вместе. Нажмите кнопку **OK** для продолжения. Будет отображено окно **Диски для преобразования** (Disks To Convert).
3. Окно **Диски для преобразования** показывает 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.

4. 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.
5. 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 статусом **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 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 эти действия:

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 нажмите 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. Дополнительно, 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 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. 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 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 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 соз-

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

дать 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**.
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**.

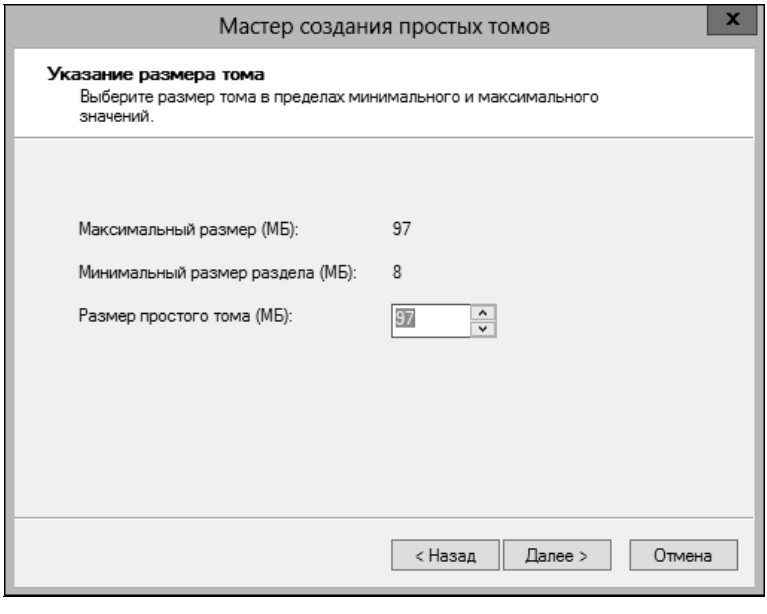


Рис. 10.3. Установите размер тома на странице **Указание размера тома**

3. На странице **Назначение буквы диска или пути (**Assign Drive Letter Or Path) (рис. 10.4) 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 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 11)*.

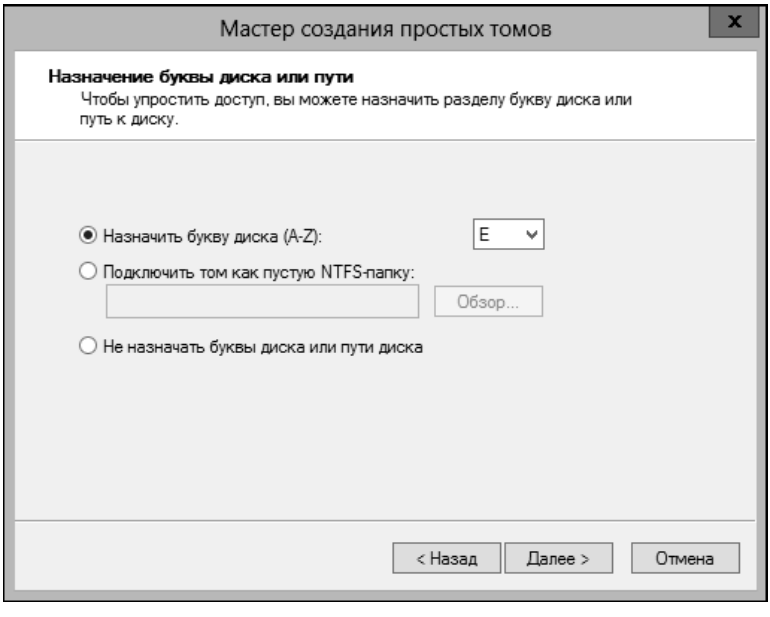


Рис. 10.4. На странице **Назначение буквы диска или пути** можно назначить указатель диска или сделать это позже

4. На странице **Форматирование раздела** (Format Partition) (рис. 10.5) определите, будет ли отформатирован том. Если это необходимо сделать, выберите **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. Об-

ратите 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, 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. Встроенное сжатие доступно только для файловой системы NTFS (и не поддерживается FAT, FAT32, exFAT и ReFS). При использовании NTFS сжатие будет 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**.

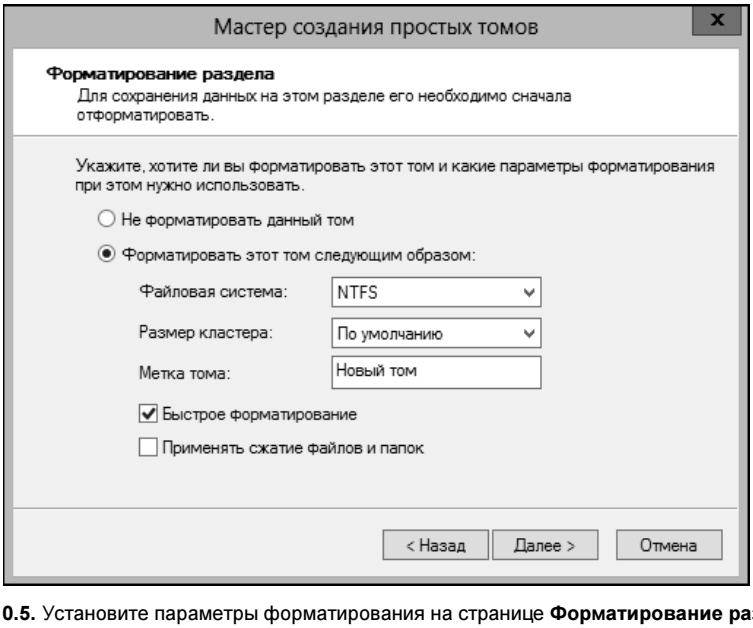


Рис. 10.5. Установите параметры форматирования на странице **Форматирование раздела**

Форматирование разделов

Форматирование делит файловую систему на разделы и удаляет все существующие данные. Здесь идет речь о высокоуровневом форматировании, создающем структуру файловой сис-

темы, 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. 10.6.

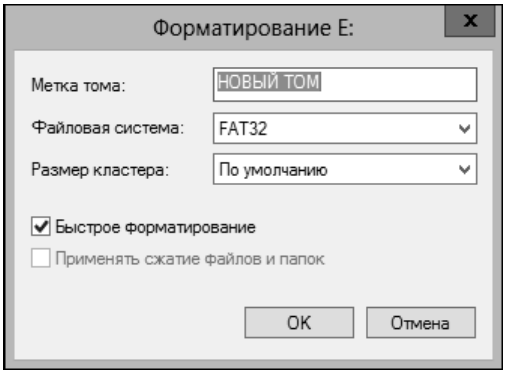


Рис. 10.6. Окно **Форматирование** позволяет выбрать файловую систему и установить метку диска

Параметры форматирования:

- **Метка тома** (Volume Label) — текстовая метка для раздела. Эта метка — имя тома раздела;
- **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, 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 в файловую систему NTFS Windows Server 2012 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. Обратите внимание, что Проводник отмечает имена сжатых ресурсов синим цветом.

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 автоматически расшифрует их, а затем выполнит сжатие. Аналогично, при попытке зашифровать сжатые данные Windows Server 2012 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 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 файлов 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.

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 13*. 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 шифрова-

ния 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 атрибут **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 назначаются агентами восстановления для автономных рабочих станций.

С помощью групповой политики можно просмотреть, назначить и удалить агентов восстановления. Чтобы сделать это, выполните следующие действия:

1. Откройте групповую политику локального компьютера, сайта, домена или организационного подразделения. Более подробная информация об этом была приведена в *главе 4*.
2. Откройте 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 открыт 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 использовать 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 использовать опубликованный сертификат этого пользователя. Если нужно использовать файл сертификата, нажмите кнопку **Обзор папок**. В окне **Открытие** (Open) выберите файл сертификата, который нужно использовать.

   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 11

Настройка томов и RAID-массивов

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 автору этой книги нужно выбрать между двумя методами управления, он сначала обращается к традиционному методу, а затем — к методу на основе стандартов. В этой главе сначала будут рассмотрены традиционные методы создания массива томов, а потом методы — стандартизированные. 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 используются 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 создать 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

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 поддерживает три уровня программного RAID: 0, 1 и 5. RAID-массивы реализуются как зеркальные, чередующиеся и чередующиеся с контролем четности.

Массивы томов и RAID-массивы создаются на динамических дисках, которые доступны только в Windows 2000 и более поздних версиях. Однако компьютеры под управлением ранних версий Windows смогут получить доступ к таким дискам по сети, как и к любому другому сетевому диску.

Создание и управление томами осуществляется так же, как и 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 чинить том, но нельзя создавать новые тома.

Понимание базовых томов

В оснастке **Управление дисками** тома разных типов помечаются цветом аналогично разделам. На рис. 11.1 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.

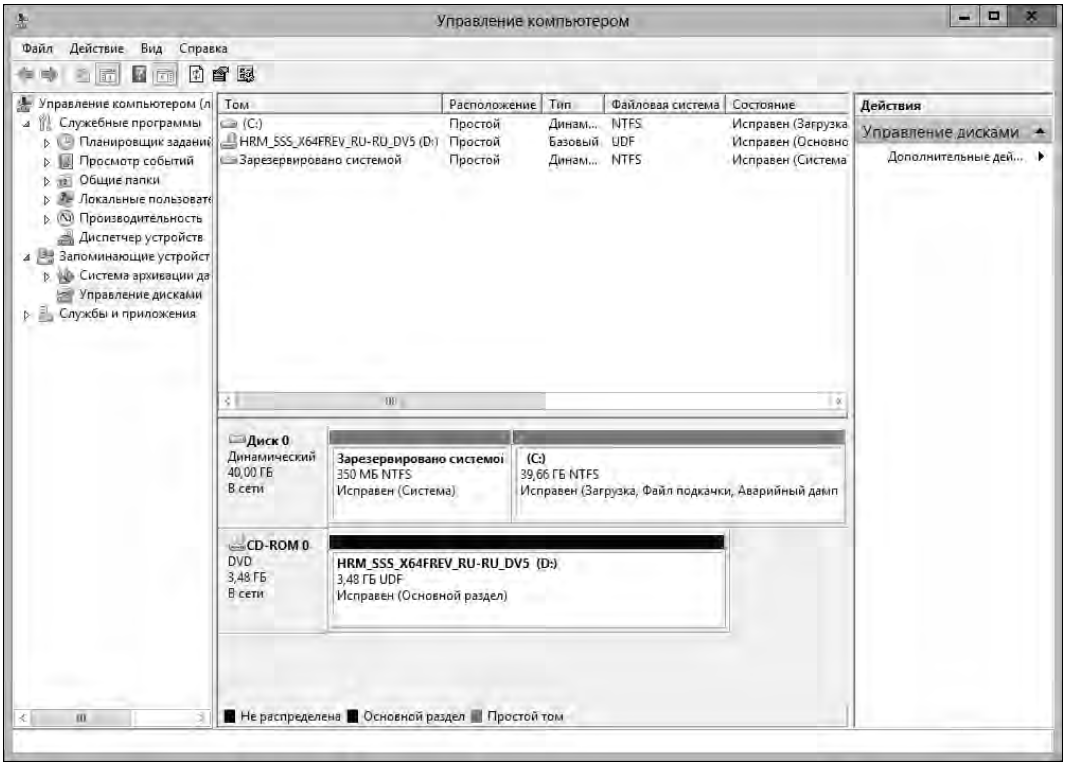


Рис. 11.1. Окно **Управление компьютером** отображает тома как разделы

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. 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 на томе C, а Windows 8 на томе D.

С томами можно сделать следующее:

- назначать буквы и пути дисков, как будет описано в *разд. "Назначение букв и путей дисков" далее в этой главе*;
- создавать любое количество томов на диске — столько, на сколько хватит свободного пространства;
- создавать тома, состоящие из двух или более дисков, если необходимо, настроить толерантность отказа;
- расширить тома до полной емкости тома;
- назначить активный, системный и загрузочный тома, как было описано в *главе 10*.

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 заполняет, 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 используемую 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. 11.1 приведены значения состояния динамических дисков.

Таблица 11.1. *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** (Reactivate Volume). 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
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

Таблица 11.1 *(окончание)*

Состояние	Описание	Решение
Исправен (Под угрозой) (Healthy (At Risk))	Windows обнаружила проблемы чтения или записи на физическом диске, на котором расположен динамический том. Состояние появляется, когда Windows обнаружила 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. 11.2) выберите диски, которые должны быть частью тома, а также укажите размер сегментов тома на этих дисках.

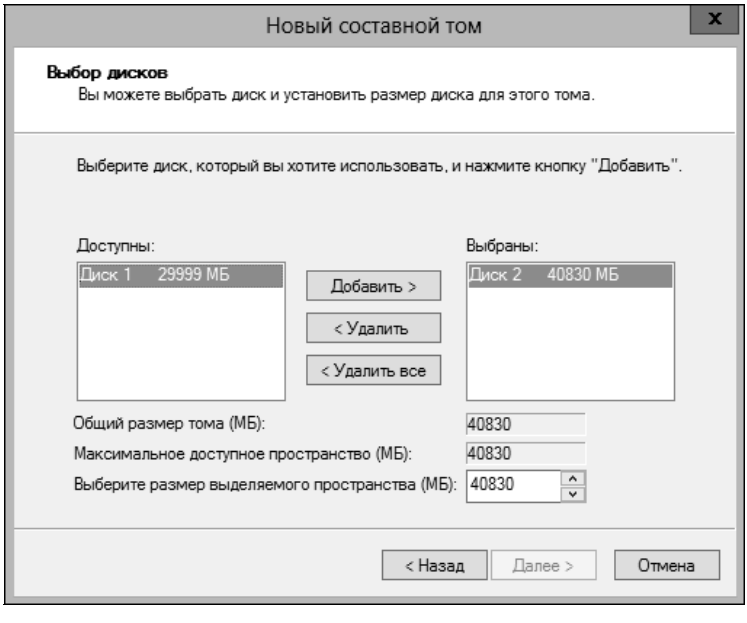


Рис. 11.2. На странице **Выбор дисков** выберите диски, которые должны быть частью тома

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 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.

Общий размер тома (МБ) (Total Volume Size In Megabytes) показывает общее дисковое пространство, которое будет использовано для тома. Нажмите кнопку **Далее**.

> ***Совет***
>
> Хоты 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 определенное 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, 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 10*.
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.

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 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. 11.2 предоставлен краткий обзор поддерживаемых уровней RAID. Поддержка осуществляется полностью программно.

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 кон-

трольной суммы для каждого блока данных, записанного на диск. Эта контрольная сумма используется для восстановления данных в случае отказа.

Таблица 11.2. *Уровни RAID, поддерживаемые Windows Server 2012*

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

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

Операционная система Windows Server 2012 поддерживает зеркалирование диска, чередование диска 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 диска

Уровень RAID 0 — это чередование диска. При чередовании диска два или более томов каждый на отдельном диске настраиваются как чередующийся набор. Данные, записывае-

мые 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 13*.

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

При создании чередующихся наборов нужно использовать тома приблизительно одинакового размера. 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.

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

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 используется метод, называемый *дублированием дисков*. На рис. 11.3 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.

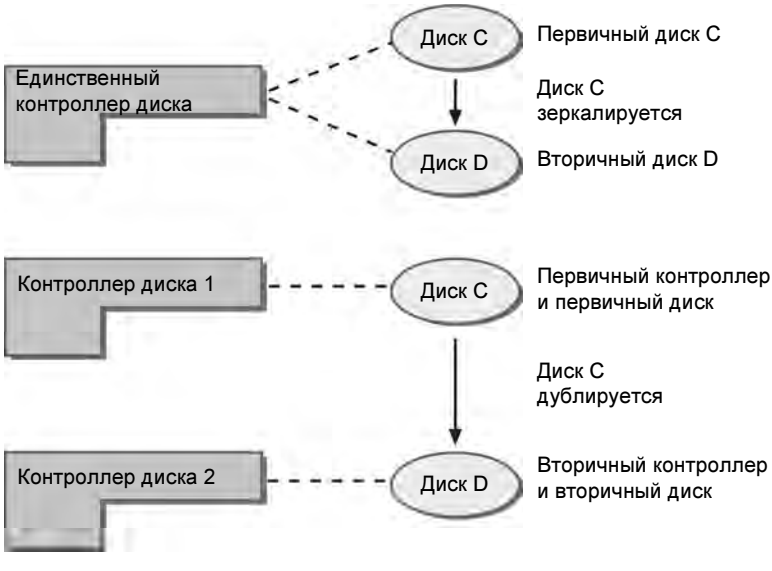


Рис. 11.3. Хотя зеркалирование диска обычно использует единственный контроллер для создания отказоустойчивого набора данных, дедупликация использует два разных контроллера

Если один из дисков набора откажет, операции с диском могут быть продолжены. Здесь, когда пользователи читают и записывают данные, 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.*

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).

Чтобы в оснастке **Управление дисками** зеркально отразить существующий том, выполните следующие действия:

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. 11.4) выберите расположение для зеркала, а затем нажмите кнопку **Добавить зеркальный том** (Add Mirror). ОС Windows Server 2012 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.

Реализация RAID 5: чередование диска с контролем четности

Уровень RAID 5 — это чередование диска 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, по сути, является улучшенной версией RAID-1 с ключевым добавлением отказоустойчивости. Отказоустойчивость гарантирует, что отказ одного диска не приведет к отказу всего набора. Вместо отказа набор продолжает функционировать с оставшимися томами в наборе.

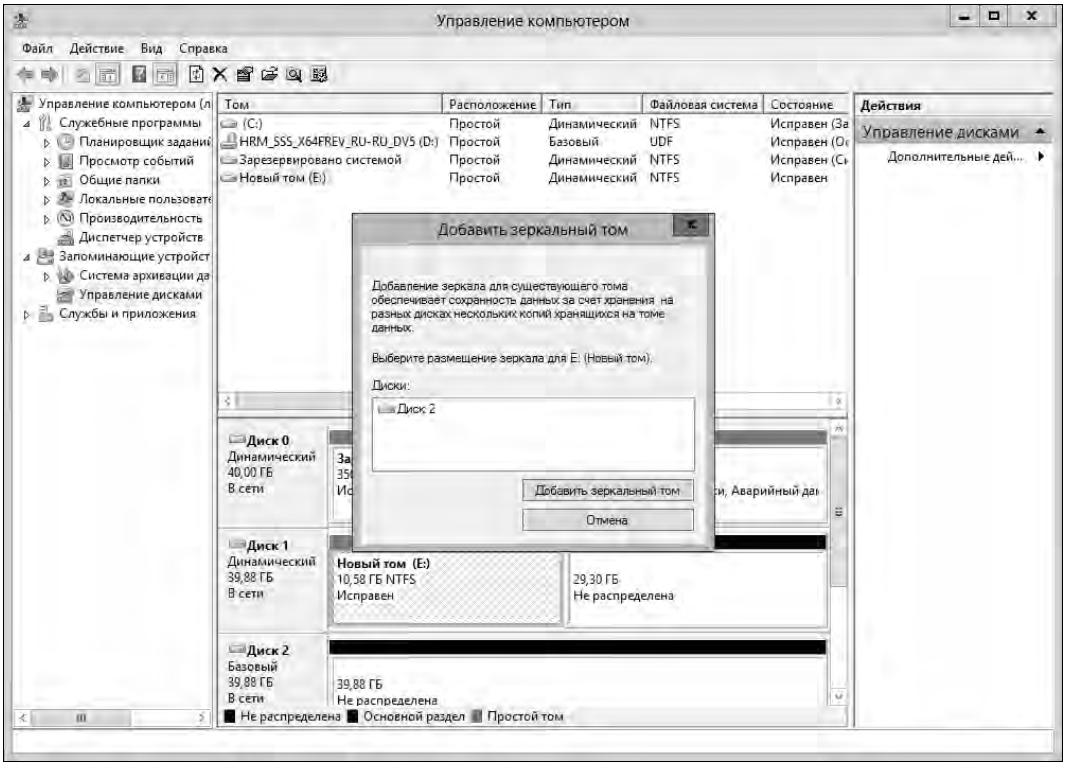


Рис. 11.4. Выберите расположение зеркала

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 разобьет зеркало, создав два независимых тома.

Ресинхронизация и восстановление зеркального набора

Операционная система Windows Server 2012 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 **Отка-**

завшая избыточность. Меры по ликвидации последствий, которые можно предпринять, зависят от состояния отказавшего тома:

1. 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).
2. 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**.
3. 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.
4. 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 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 — 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 **Реактиви-**

ровать 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 отказавший регион 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

Для использования стандартизированного хранилища нужно добавить компонент **Стандартизированное управление хранилищами Windows** (Windows Standards-Based Storage Management) на серверы. Если сервер настроен с ролью **Файловые службы и службы хранилища** (File Services And Storage), **Стандартизированное управление хранилищами Windows** добавляет компоненты и обновляет диспетчер серверов опциями для работы со стандартизированными томами. Возможно, также нужно сделать следующее:

- 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. 11.5 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) — используется 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.
- **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.

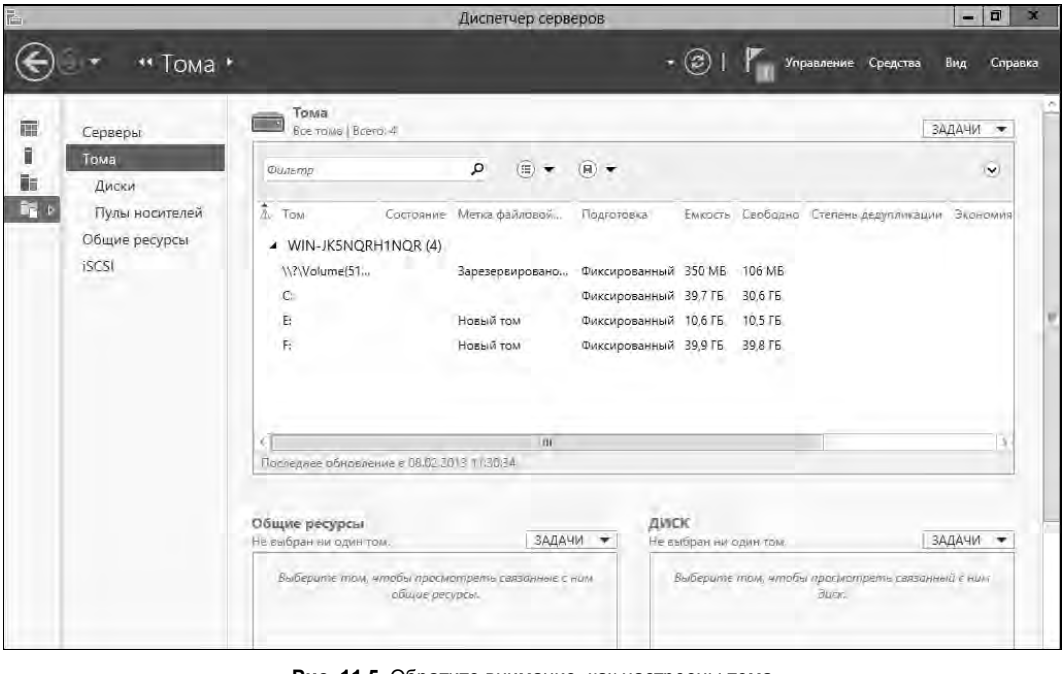


Рис. 11.5. Обратите внимание, как настроены тома

Как показано на рис. 11.6, 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.

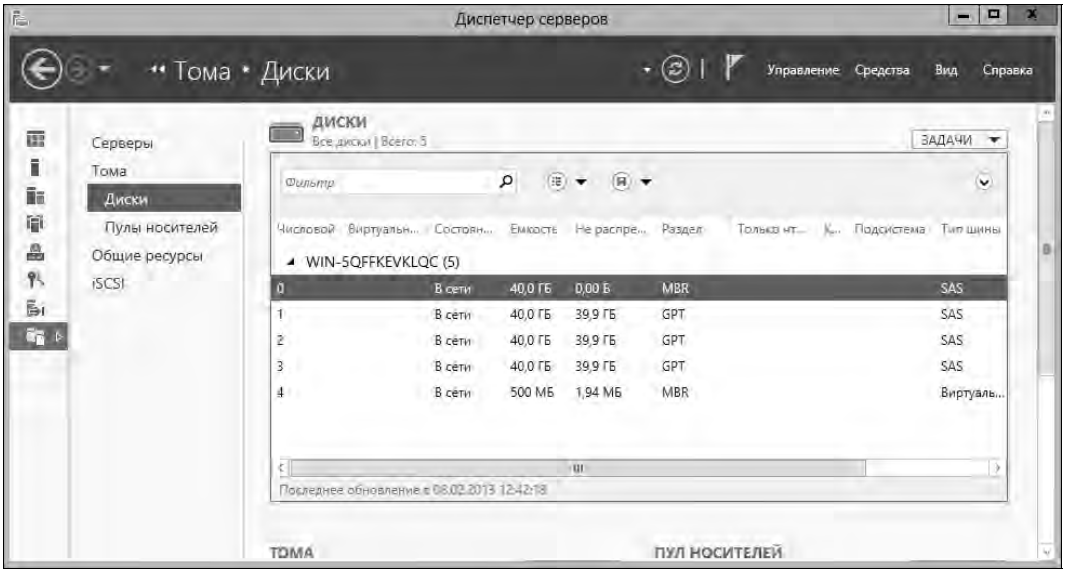


Рис. 11.6. Выводит все доступные диски и сообщает, сколько нераспределенного пространства доступно

Создание 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. 11.7, 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.

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.

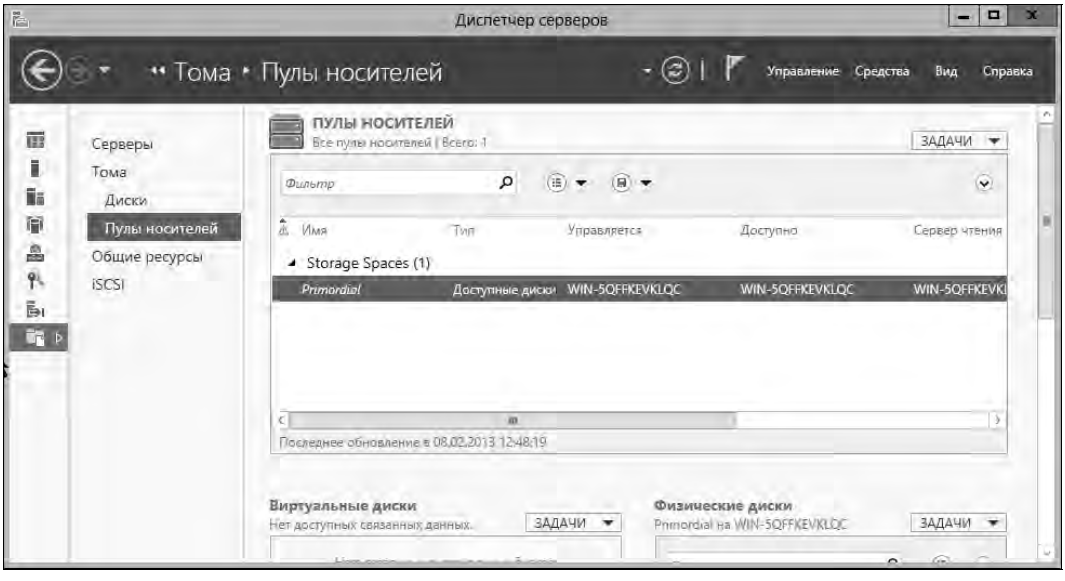


Рис. 11.7. Создание и управление пулами

Создание пространства хранилища

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 Storage Spaces или подсистему, связанную с присоединенным хранилищем.

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 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 использования 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 показывает 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.

Создание виртуального диска в пространстве хранилища

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 зеркаль-

но 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. 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**.
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**.
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 нужно 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**.

Управление существующими разделами и дисками

Оснастка **Управление дисками** предоставляет множество способов управления существующими разделами и дисками. Можно назначать буквы дисками, удалять разделы, устанавливать активный раздел и т. д. Дополнительно ОС Windows Server 2012 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. 11.8. 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**.

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

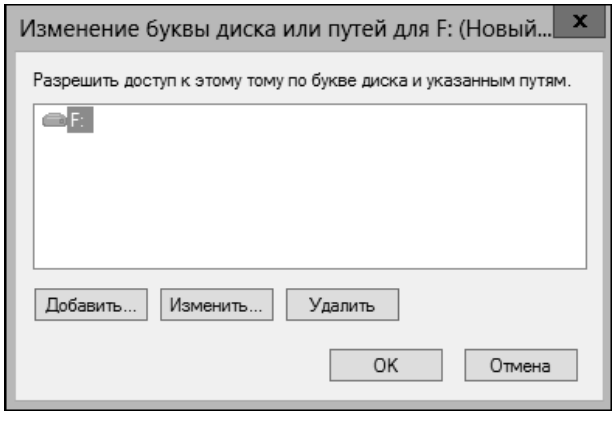


Рис. 11.8. Можете изменить букву диска и путь в окне **Изменение буквы диска или путей**

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, 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 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 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 со-

храняется, и данные не будут потеряны. Помните, однако, что в Windows Server 2012 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 ввести метку, если она 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 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 требу-

ет 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 диски. 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 резервируемого 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 при преобразовании 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 неиспользуемое место в файле будет зарезервировано для будущего использования MFT.

Изменение размера раздела и тома

Операционная система Windows Server 2012 не использует загрузчик Ntldr и файл Boot.ini для загрузки операционной системы. Вместо этого у Windows Server 2012 есть предустановочная среда, в которой используется 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 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. 11.9) 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;

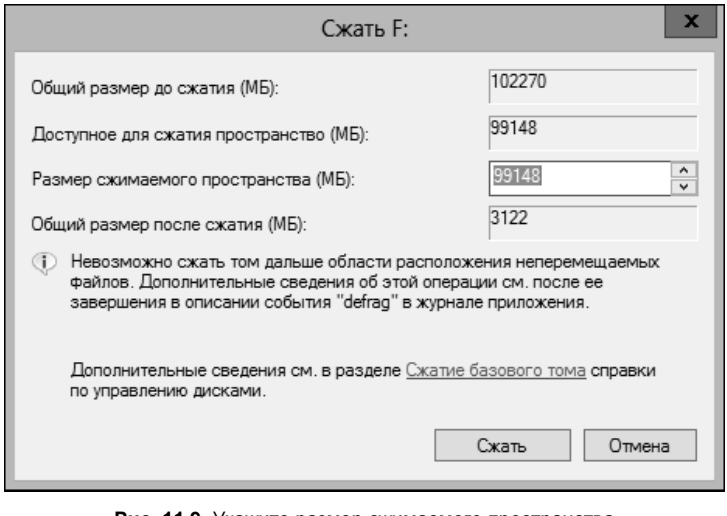


Рис. 11.9. Укажите размер сжимаемого пространства

   - **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.

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 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 ChkDsk для исправления ошибок и противоречий в NTFS-томах на диске. Поскольку этот процесс может разрушить доступность Windows-систем, ОС Windows Server 2012 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 том случае, если будет получено уведомление от операционной системы, что проблема не может быть исправлена автоматически. Если произойдет такая ошибка, Windows Server 2012 уведомит о проблеме и предоставит возможные решения.

У самовосстановления NTFS есть много преимуществ по сравнению с ChkDsk.

- ChkDsk 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). Несмотря на то, что ChkDsk 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 ограничена. Например, утилита не может восстановить поврежденные данные в файлах, которые, возможно, структурно не повреждены.

Как часть автоматизированного обслуживания, Windows Server 2012 выполняет превентивное сканирование томов NTFS. Как и с другим автоматизированным обслуживанием,

Windows сканирует диски, запуская утилиту **Проверка диска** в 3:00, 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 **Проверка диска** 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 3:00, если компьютер работает от сети питания и операционная система неактивна. В противном случае Windows, обслуживание будет запущено в следующий раз, когда компьютер работает от сети питания и операционная система простаивает. 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.

Проверка дисков вручную

В Windows Server 2012 утилита **Проверка диска** осуществляет расширенное сканирование и восстановление диска автоматически, вместо проверки вручную, как в предыдущих версиях Windows. Здесь, при использовании утилиты **Проверка диска** 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 ChkDsk с FAT, FAT32 или exFAT Windows Server 2012 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.

Можно запустить утилиту **Проверка диска** 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, ChkDsk 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 ChkDsk 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 ChkDsk:

- *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.

Интерактивный запуск проверки дисков

Можно запустить утилиту **Проверка диска** 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. 11.10.

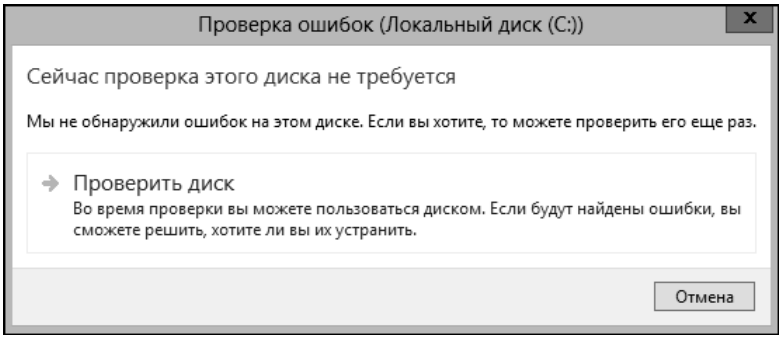


Рис. 11.10. Используйте утилиту **Проверка диска** для проверки диска на наличие ошибок и устранения ошибок, если они будут найдены

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.

> ***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 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. 11.11) проанализирует диск, чтобы определить, нуждается ли он в дефрагментации. Если это так, программа порекомендует дефрагментировать диск.

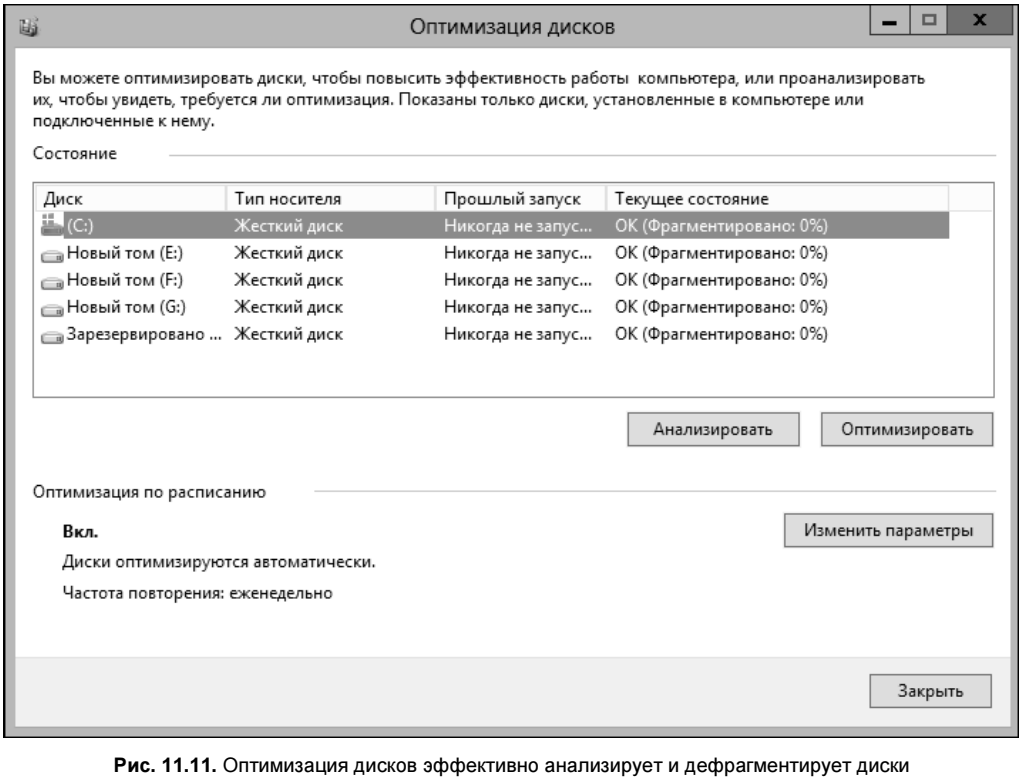


Рис. 11.11. Оптимизация дисков эффективно анализирует и дефрагментирует диски

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 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. 11.12. Для отмены автоматической дефрагментации сбросьте флажок **Выполнять по расписанию (рекомендуется)** (Run On A Schedule). Для включения автоматической дефрагментации, наоборот, установите этот флажок.

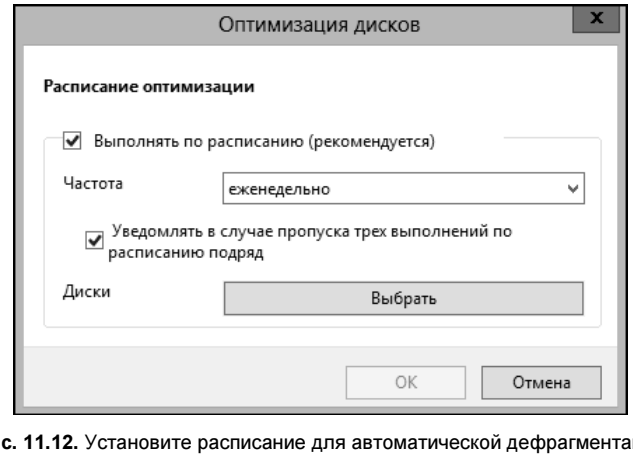


Рис. 11.12. Установите расписание для автоматической дефрагментации

4. Частота дефрагментации по умолчанию установлена так, как показано на рис. 11.12. 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).

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 12

Общий доступ к данным, безопасность и аудит

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. Операционные системы Windows 8 и Windows Server 2012 поддерживают SMB версии 3.0 и содержат SMB-клиента, совместимого с версией 3.0. SMB 3.0 содержит много улучшений, положительно влияющих на производительность, особенно при использовании кластеризируемых файловых серверов. Основное улучшение — сквозное шифрование данных SMB, которое избавляет от использования протокола IPsec, специальных аппаратных средств или акселераторов глобальной сети (WAN) для защиты данных от прослушивания. Шифрование SMB может быть включено индивидуально для каждого общего ресурса.

При использовании SMB Windows Server 2012 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 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 добавляет новые слои безопасности с помощью комплексной проверки подлинности, технологии идентификации на основе требований и политик централизованного доступа. В Windows 8 и Windows Server 2012 можно назначить идентификацию на основе требований к ресурсам файла и папки на томах NTFS и ReFS. В Windows Server 2012 пользователям доступ к ресурсам файла и папки предоставляется непосредственно с помощью разрешений доступа и разрешений общего доступа или косвенно с помощью 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. Операционные системы Windows 8 и Windows Server 2012 поддерживают SMB 3.0 (они используют клиент SMB 3.0).

Практический совет

Хотя ReFS обеспечивает высоконадежную файловую систему, имейте в виду, что ReFS не поддерживает теневые копии. Поэтому, если создаете общие ресурсы на томах ReFS, пользователи не смогут вернуться к предыдущим версиям файлов и папок, сохраненных в этих общих ресурсах.

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).

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 разрешит 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 может использовать 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. 12.1, 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.

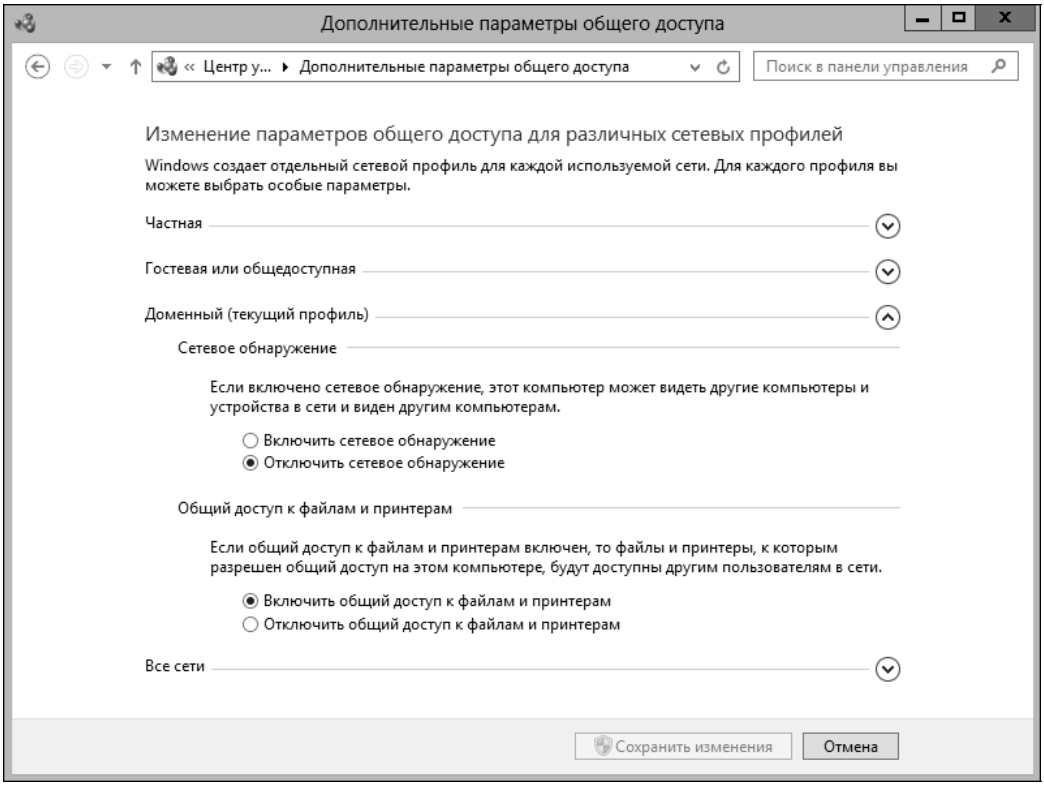


Рис. 12.1. Центр управления сетями и общим доступом показывает текущую конфигурацию

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 предотвращать внешний доступ;
   - **Отключить общий доступ** (Turn off public folder sharing) — отключает общий доступ, предотвращая 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.

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 суффиком $) 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. 12.2).

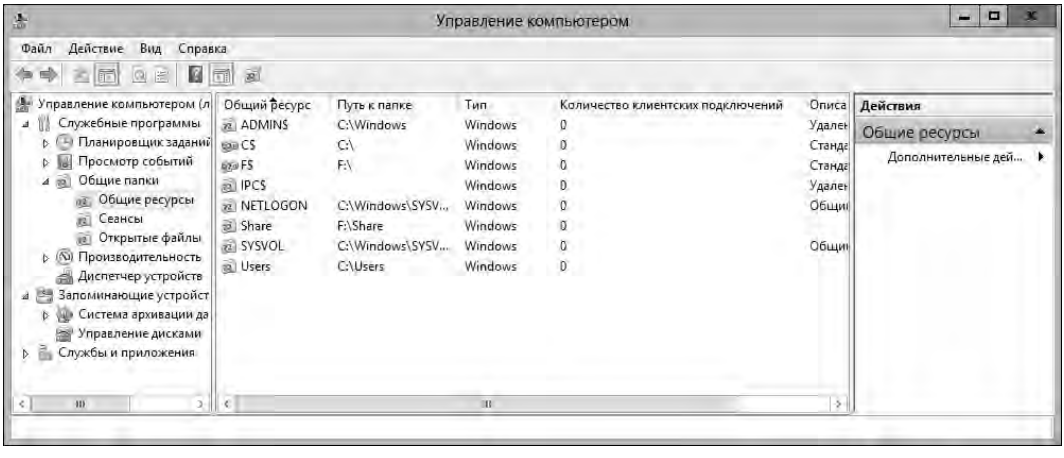


Рис. 12.2. Доступные общие ресурсы выводятся в узле **Общие ресурсы**

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;
   - **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. 12.3). 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.

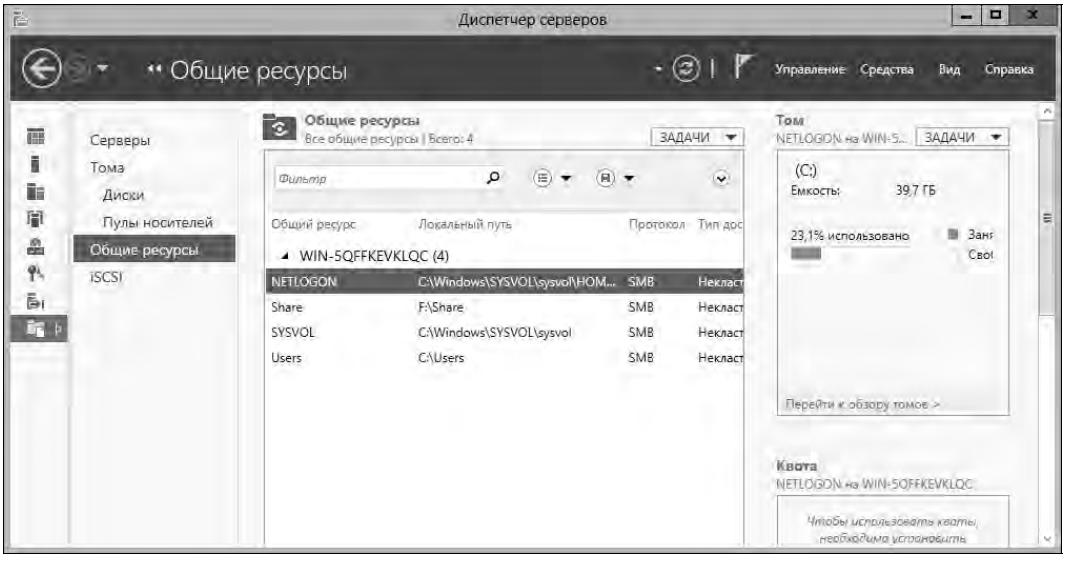


Рис. 12.3. Выберите **Общие ресурсы** на главной панели (слева) для просмотра всех доступных общих ресурсов

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 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**. Нажмите 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. 12.4). Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальны для каждой системы.

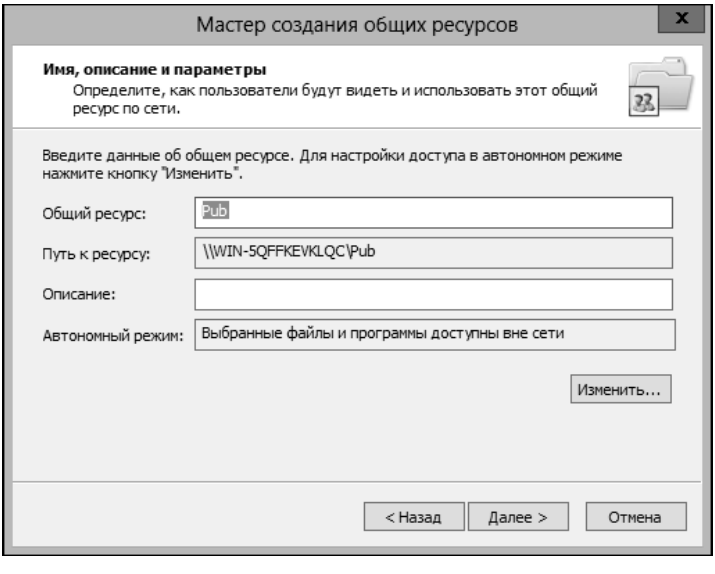


Рис. 12.4. Используйте мастер создания общих ресурсов для настройки параметров общего ресурса, включая имя, описание и параметры автономного режима

> ***Совет***
>
> Если нужно скрыть общий ресурс от пользователей (это означает, что они не увидят ресурс, когда они 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 **Файловые службы и 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 серверных 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. 12.5). Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальными для каждой систем.

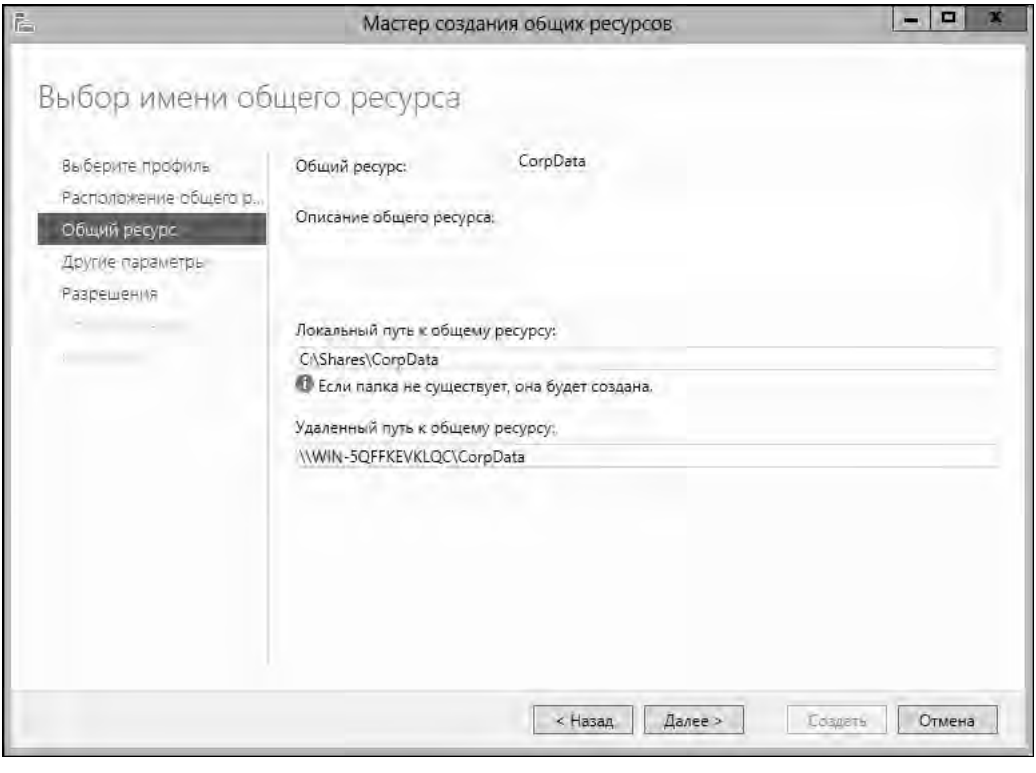


Рис. 12.5. Установите имя и описание общего ресурса

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**.
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" далее в этой главе*.
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 шаблон квоты, который уже создан. Подробно этот процесс будет описан в *разд. "Управление шаблонами дисковых квот" далее в этой главе*.
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. 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.
2. Щелкните правой кнопкой мыши на общем ресурсе, с которым нужно работать, и выберите команду **Свойства**.
3. В окне **Свойства** (рис. 12.6) есть несколько панелей с параметрами. Можно развернуть панели по одной или выбрать опцию **Показать все** (Show All), чтобы просмотреть все панели за один раз.

Рис. 12.6. Измените параметры общего ресурса, используя предоставленные опции

4. 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 подпапкок;
  - 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 8*.

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. 12.7. Теперь можно просмотреть список пользователей и групп, у которых есть доступ к этому ресурсу, а также тип предоставленного им доступа.

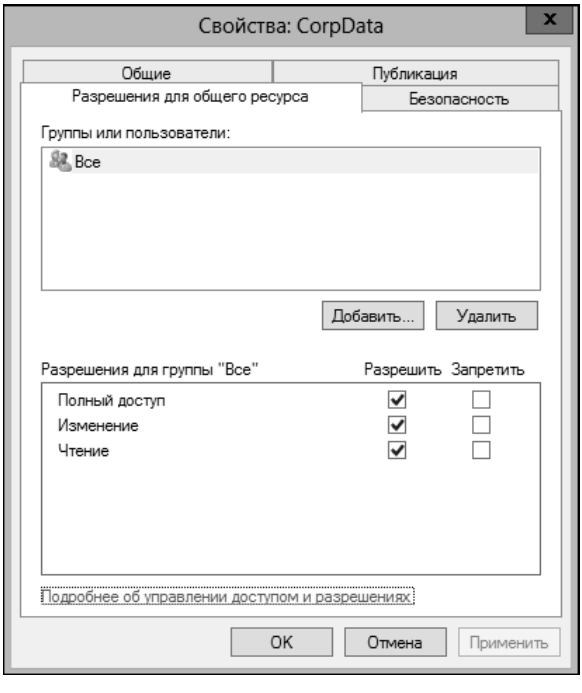


Рис. 12.7. Вкладка **Разрешения для общего ресурса** показывает, какие пользователи и группы обладают доступом к общему ресурсу и какой тип доступа им предоставлен

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 для** (Permissions for);
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. 12.8).

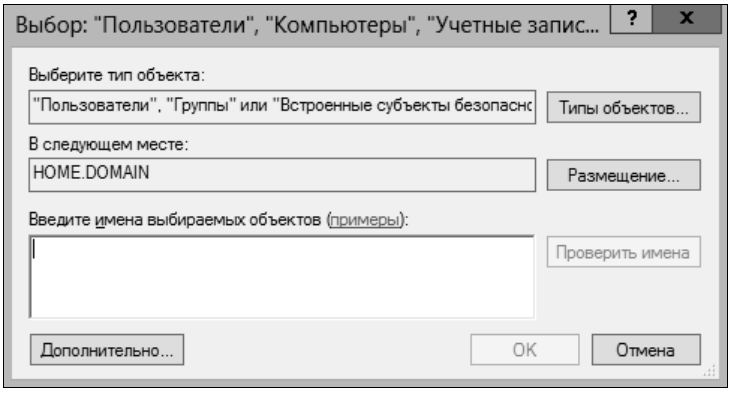


Рис. 12.8. Добавьте пользователей и группы в общий ресурс

6. Введите имя пользователя, компьютера или группы в текущем домене, а затем нажмите кнопку **Проверить имена**. 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** и выберите другое место;
   - если найдено несколько совпадений, выберите имя или имена, которые должны использоваться, и затем нажмите кнопку **OK**. Чтобы присвоить полномочия другим 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. разд. "Разрешения файла и папки" далее в этой главе*.

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. 12.9.

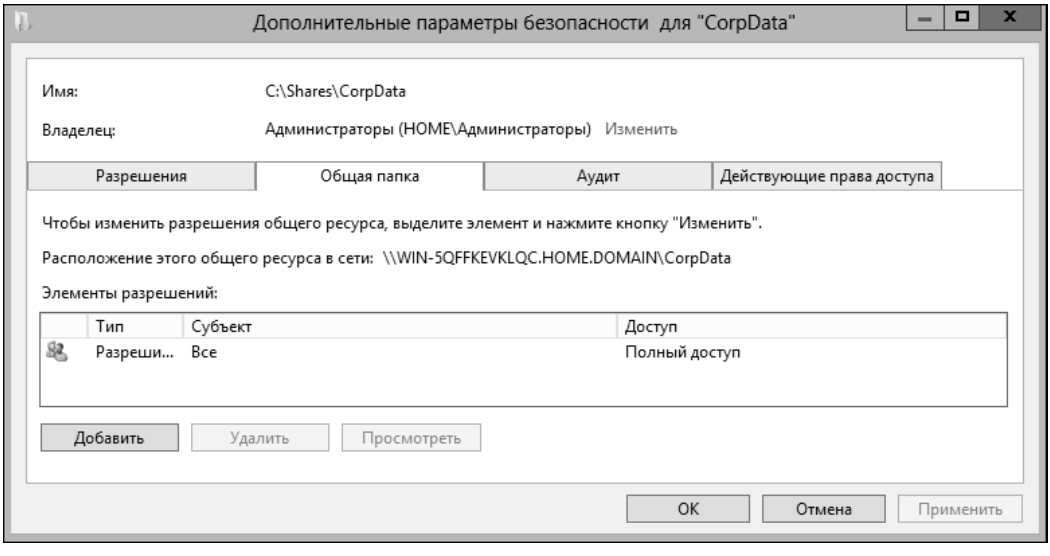


Рис. 12.9. Вкладка **Общая папка** показывает, какие пользователи и группы имеют доступ к ресурсу и какой тип доступа им назначен

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 нажмите кнопку **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. 12.10).
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**.

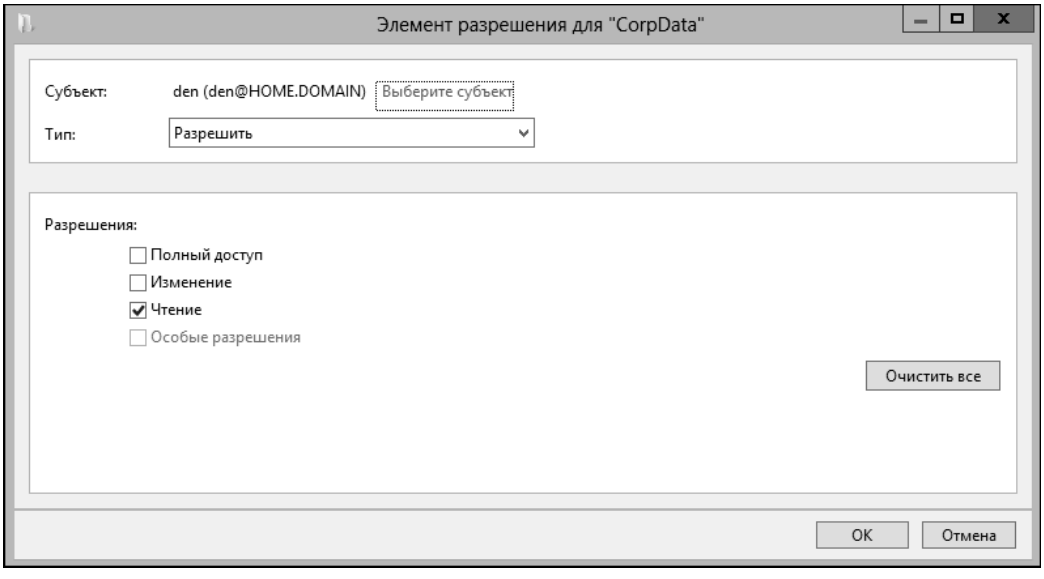


Рис. 12.10. Добавление разрешений для определенной учетной записи пользователя или группы

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), чтобы указать, 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" далее в этой главе.*

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. 12.1 перечислены специальные ресурсы и указано их использование.

Таблица 12.1. *Особые общие ресурсы, используемые в Windows Server 2012*

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. Для подключения к специальному ресурсу выполните эти действия:

1. Откройте Проводник, перейдите на панель **Компьютер** (Computer).
2. Нажмите кнопку **Подключить сетевой диск** (Map Network Drive) на панели **Компьютер**. Откроется окно **Подключение сетевого диска** (Map Network Drive) (рис. 12.11).

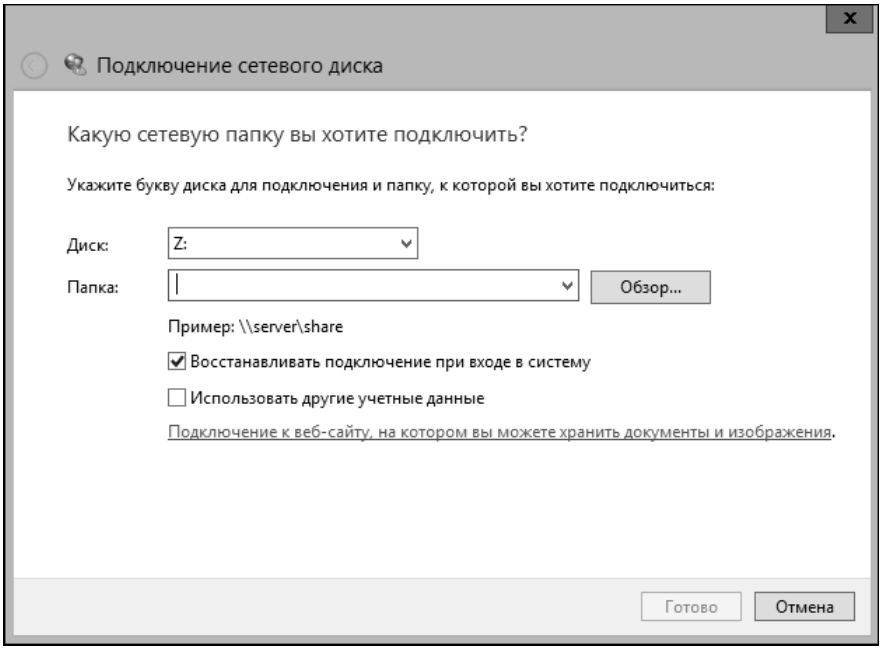


Рис. 12.11. Подключитесь к особым ресурсам, используя окно **Подключение сетевого диска**

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. Независимо от того, кто подклю-

чился к ресурсу — пользователь или компьютер, Windows Server 2012 выводит соединение в узле **Сеансы** (Sessions).

Для просмотра соединений к общим ресурсам введите команду `net session` в командной строке или выполните 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.

Управление сеансами и общими ресурсами

Управление сеансами и общими ресурсами — общая административная задача. Перед завершением работы сервера или приложения, запущенного на сервере, нужно отключить пользователей от общих ресурсов. Также нужно 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 \\computername /delete` в командной строке или 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. 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.

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).

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.

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.

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 компьютеров** 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 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 10*, 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, OS X и UNIX, позволяя пользователям передавать файлы между операционными системами Windows Server 2012, 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. 12.12.

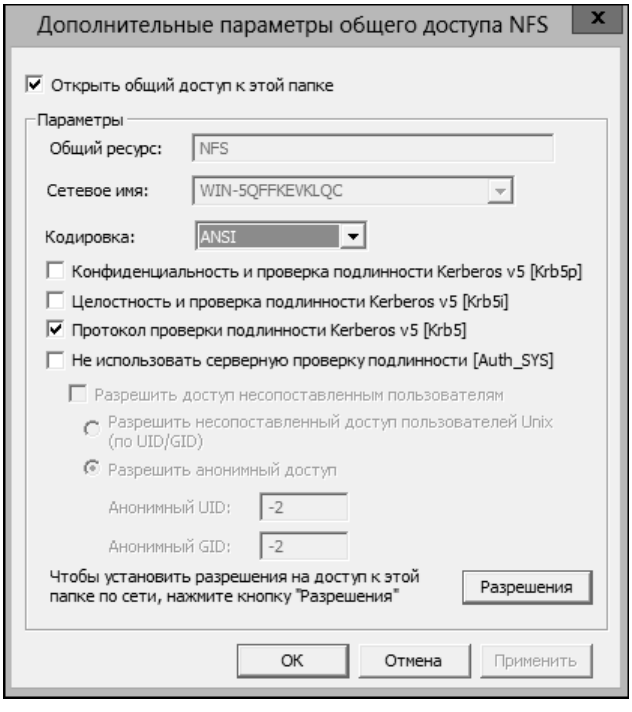


Рис. 12.12. Можно использовать общий доступ NFS для обмена файлами между Windows и UNIX-компьютерами

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).
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,

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 вечера. 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 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.
3. Щелкните правой кнопкой мыши на узле **Управление дисками** и выберите команду меню **Все задачи | Настроить теневые копии** (All tasks | Configure shadow copies).

---

[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.*

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. 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. На вкладке **Предыдущие версии** 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 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 операционной 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 **Теневые копии**. 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. 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 подключение к сетевому диску осуществляется путем его сопоставления буквы диска общему ресурсу с использованием команды `NET USE`:

```
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`.

Если клиентский компьютер работает под управлением Windows 8, 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

Для отключения сетевого диска 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).

Управление объектами, владением и наследованием

Операционная система Windows Server 2012 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. 12.2.

Таблица 12.2. *Объекты Windows Server 2012*

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

дительского 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 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:

1. Отредактируйте разрешения родительского объекта.
2. Остановите наследование разрешений из родительского объекта и затем назначьте разрешения дочернему объекту.
3. 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, 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 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 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. 12.3. 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 12.3. *Разрешения файла и папки, используемые в Windows Server 2012*

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

Таблица 12.3 *(окончание)*

Разрешение	Значение для папок	Значение для файлов
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 — это 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. 12.4 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.

В табл. 12.5 показаны 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 12.4. *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				
Удаление (Delete)	Да	Да			
Чтение разрешений (Read Permissions)	Да	Да	Да	Да	Да
Смена разрешений (Change Permissions)	Да				
Смена владельца (Take Ownership)	Да				

Таблица 12.5. *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		

Таблица 12.5 *(окончание)*

Особые разрешения	Базовые разрешения					
	Полный доступ	**Изменение**	**Чтение и выполнение**	**Список содержимого папки**	**Чтение**	**Запись**
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
Удаление подпапок и файлов (Delete Subfolders And Files)	Да					
Удаление (Delete)	Да	Да				
Чтение разрешений (Read Permissions)	Да	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. 12.13).

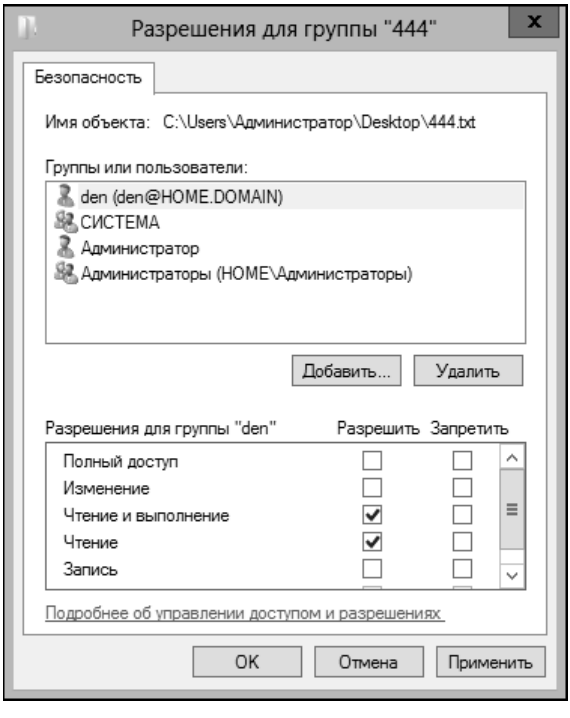


Рис. 12.13. Настройка базовых разрешений для файла или папки на вкладке **Безопасность**

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;
   - 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 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** щелкните правой кнопкой мыши на папке и выберите команду **Свойства**. Откроется одноименное окно.
2. Выберите на левой панели элемент **Разрешения**, будут отображены текущие разрешения общего ресурса и NTFS-разрешения на основной панели.
3. Нажмите кнопку **Настройка разрешения** для открытия окна **Дополнительные параметры безопасности** с активной вкладкой **Разрешения**.
4. 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. 12.14). Основные отличия — отображаются индивидуальные наборы разрешений,

указано, наследованы ли разрешения и от кого, а также перечислены ресурсы, к которым применены разрешения.

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.

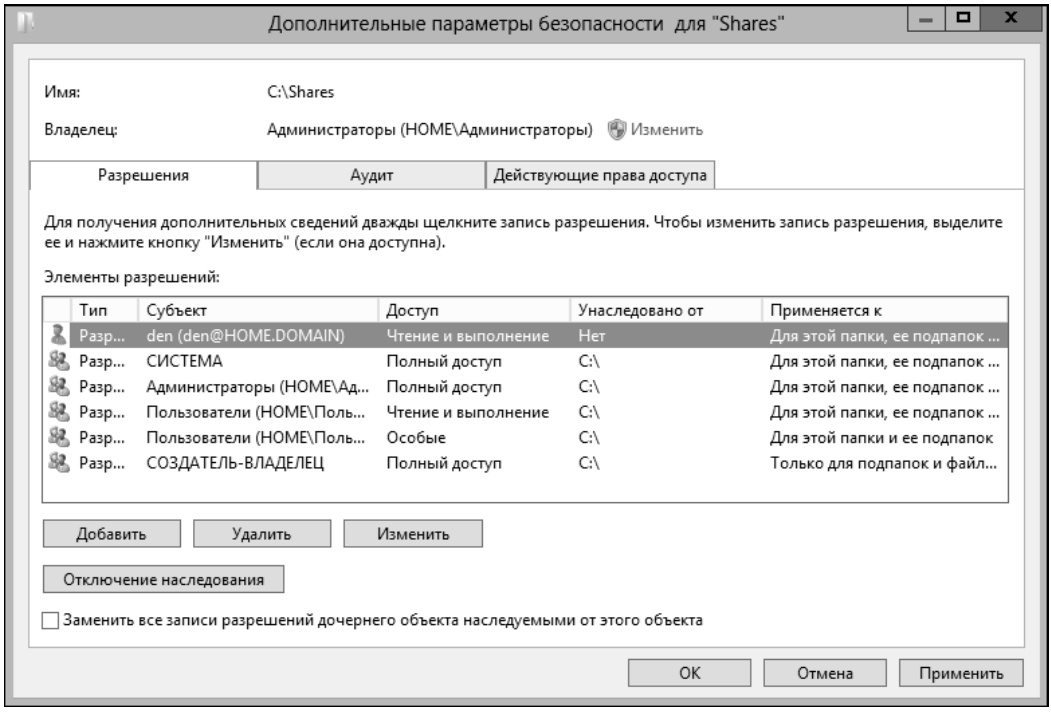


Рис. 12.14. Настройте особые разрешения для файлов и папок

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. 12.15).

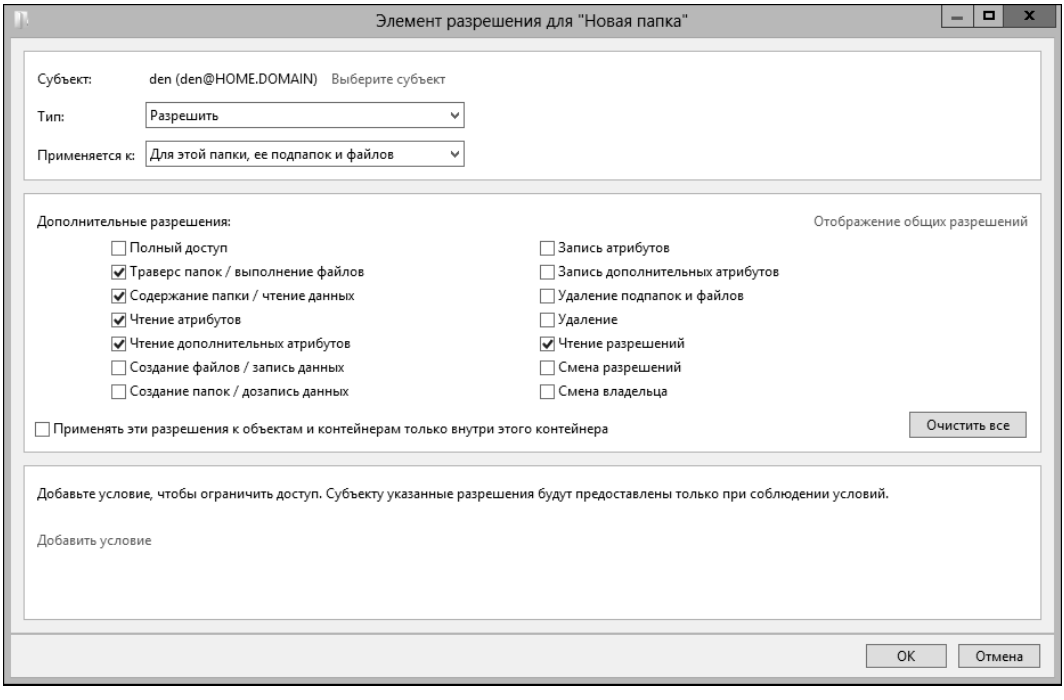


Рис. 12.15. Настройте особые разрешения, которые должны быть разрешены или запрещены

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;

- **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 выберите **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. Компьютеры 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 и Windows Server 2012, 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** щелкните правой кнопкой мыши на папке и выберите команду **Свойства** для отображения одноименного окна.
2. На панели слева выберите элемент **Разрешения**, на основной панели будут отображены разрешения общего ресурса и NTFS-разрешения.
3. Нажмите кнопку **Настройка разрешений**, чтобы открыть окно **Дополнительные параметры безопасности** с активной вкладкой **Разрешения**.
4. 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. 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. 12.16) 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).

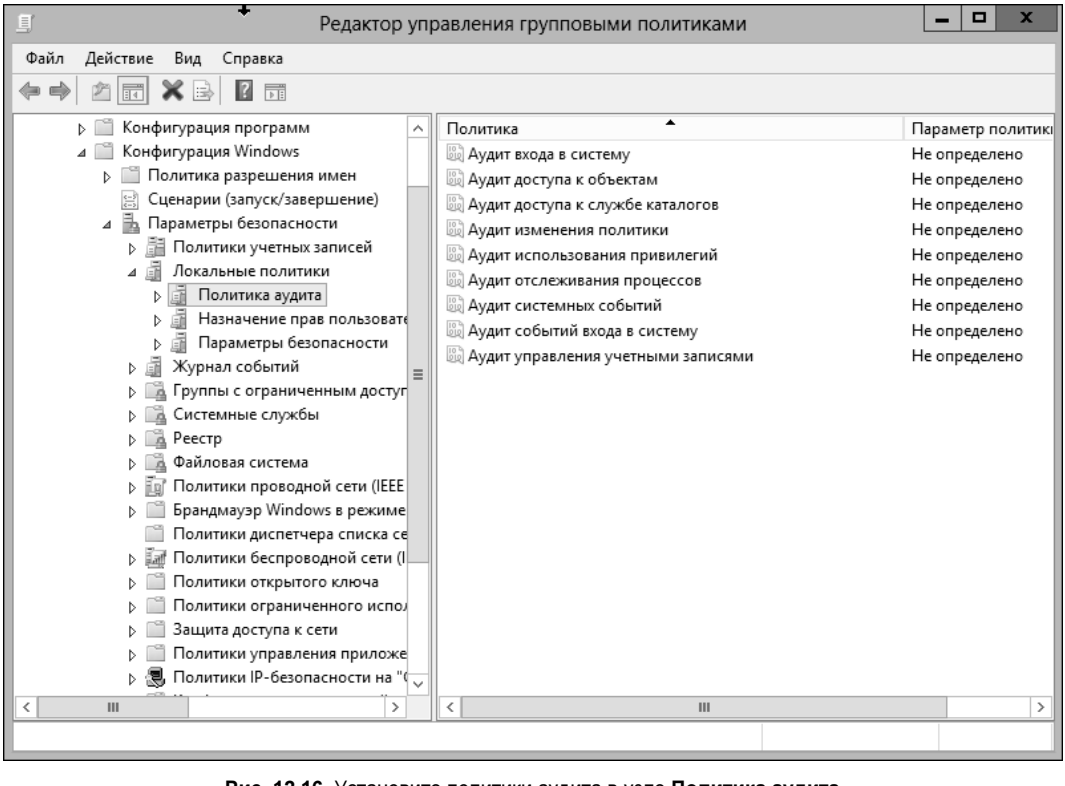


Рис. 12.16. Установите политики аудита в узле **Политика аудита**

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 Tracks) — отслеживает все события, связанные с управлением учетными записями средствами ос-

настки **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. 12.17).

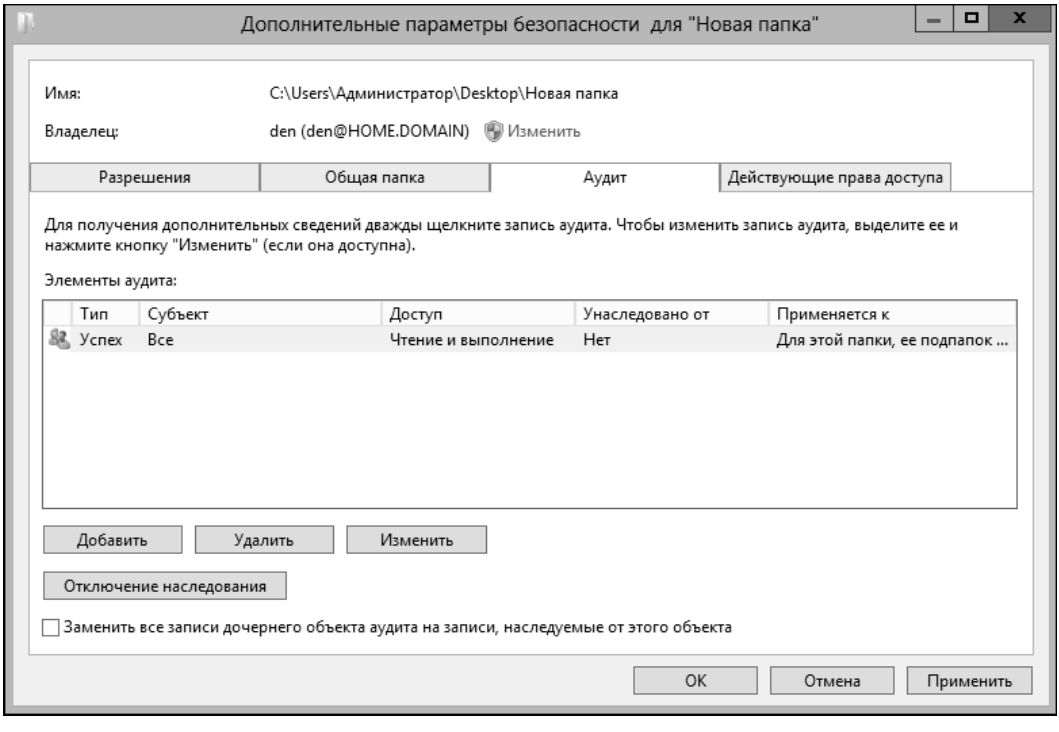


Рис. 12.17. Настройка политик аудита для отдельных файлов или папок на вкладке **Аудит**

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. 12.4 и 12.5) 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). В окне **Разрешения** нажмите кнопку **Дополнительно**. В окне **Дополнительные параметры безопасности** перейдите на вкладку **Аудит**.
3. Нажмите кнопку **Добавить** для отображения окна **Элемент аудита**. Щелкните по ссылке **Выберите субъект** для отображения окна **Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"**.
4. В этом окне введите **Все** (Everyone) и нажмите кнопку **Проверить имена**, а затем нажмите кнопку **OK**.
5. В окне **Элемент аудита** отображаются только базовые разрешения. Щелкните по ссылке **Отображения дополнительных разрешений**, чтобы отобразить особые разрешения.
6. Используйте список **Применяется к**, чтобы указать, как будет применяться элемент аудита.
7. 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.
8. 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 поддерживает два взаимоисключающих типа дисковых квот.

- *Дисковые квоты файловой системы NTFS* поддерживаются всеми выпусками Windows Server 2012 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 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.

Понимание дисковых квот файловой системы NTFS или как используются квоты

Администраторы используют дисковые квоты файловой системы NTFS для управления использованием дискового пространства для 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 установить 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 размещение 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 локальной системной группы **Администраторы**. 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 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 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 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 правила и применять их поочередно к каждому тому, которым 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. 12.6 представлены доступные политики.

Таблица 12.6. *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

Таблица 12.6 *(окончание)*

Имя политики	Описание
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. 12.18) установите переключатель **Включено**.
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 пользователи, 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**.

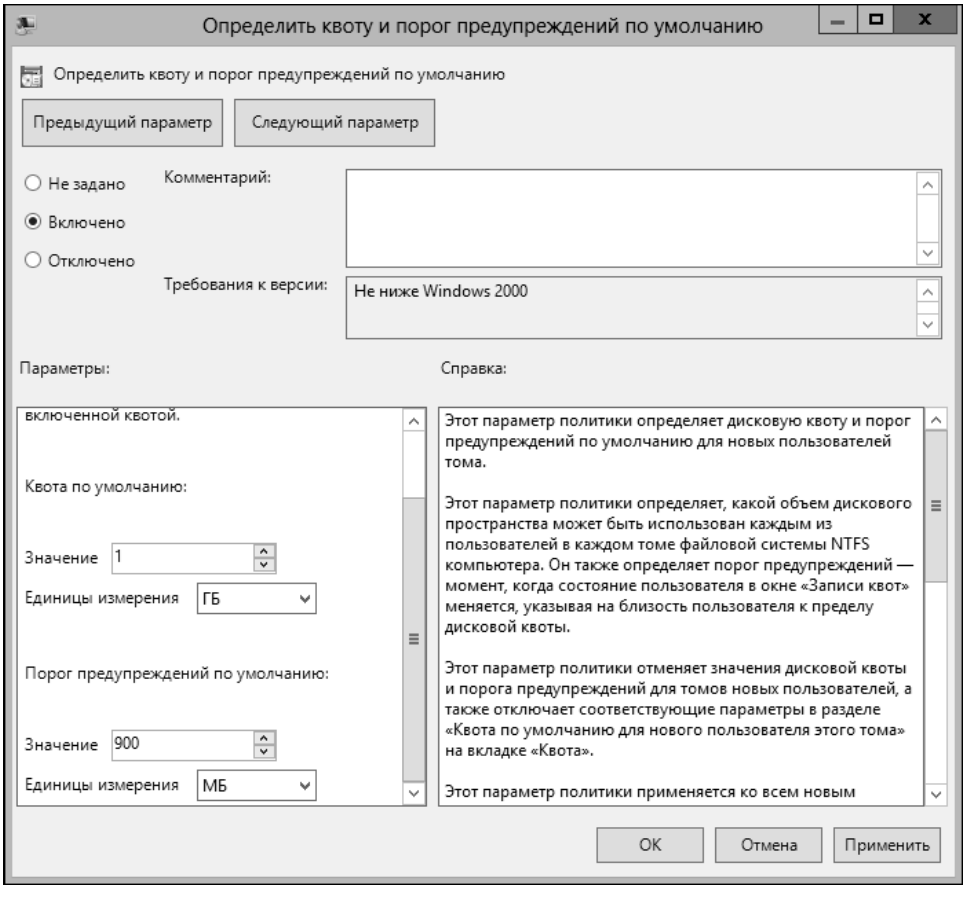


Рис. 12.18. Установите квоту и порог предупреждения

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, если они превысили 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. 12.19). Если квоты уже включены через групповую политику, эти параметры будут недоступны, и их нельзя изменить. Вместо этого нужно модифицировать параметры через групповую политику.

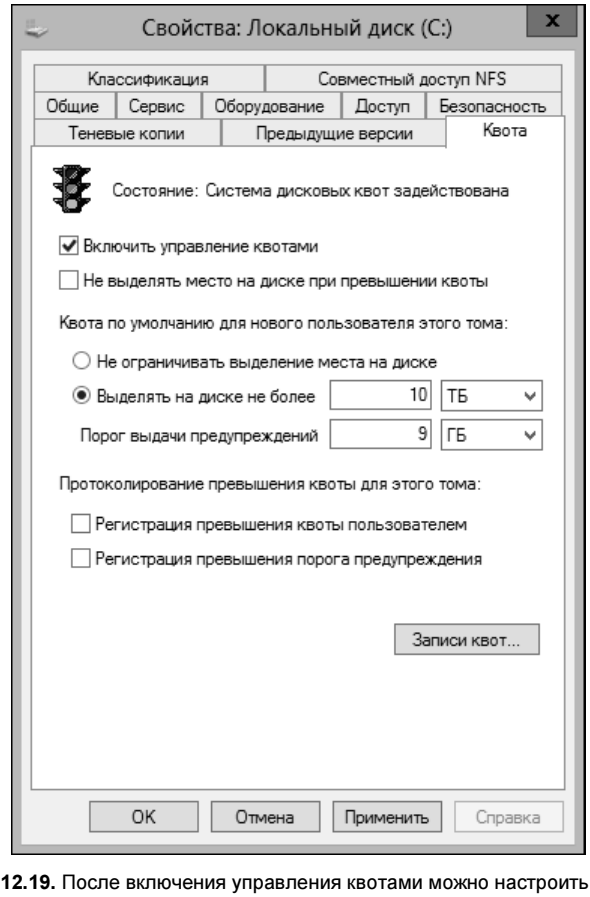


Рис. 12.19. После включения управления квотами можно настроить квоту и порог выдачи предупреждений

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 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. Автор книги 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. 12.20). Есть две опции. Можно удалить все ограничения квот для этого поль-

зователя, 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**.

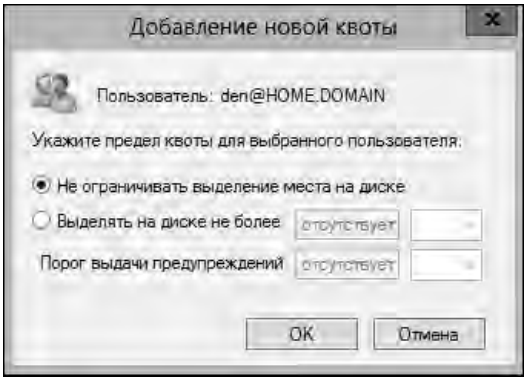


Рис. 12.20. В окне **Добавление новой квоты** можно настроить квоту для пользователя и порог выдачи предупреждения или удалить ограничения квоты вообще

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, используйте 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 — этот 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 выбора ко всем записям квот установите флажок **Применить ко всем записям квот** (Do this for all quota entries), а затем нажмите кнопку **Да** или **Нет**.

---

[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.*

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 **OK**. Когда увидите запрос, еще раз нажмите кнопку **OK**.

Использование, настройка и управление квотами диспетчера ресурсов

Операционная система Windows Server 2012 поддерживает расширенную систему управления квотами, называемую *дисковыми квотами диспетчера ресурсов* (Resource Manager disk quotas). Используя 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 обоих 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 использовать квоты диспетчера ресурсов.

Понимание дисковых квот диспетчера ресурсов

При работе с Windows Server 2012 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, представлены в табл. 12.7. 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 12.7. *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. 12.7 было представлено общее описание имеющихся шаблонов. В табл. 12.8 перечислены переменные, которые могут быть использованы для автоматического создания сообщений и событий.

Таблица 12.8. *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. 12.21).
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**.
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 ка-

ких 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.

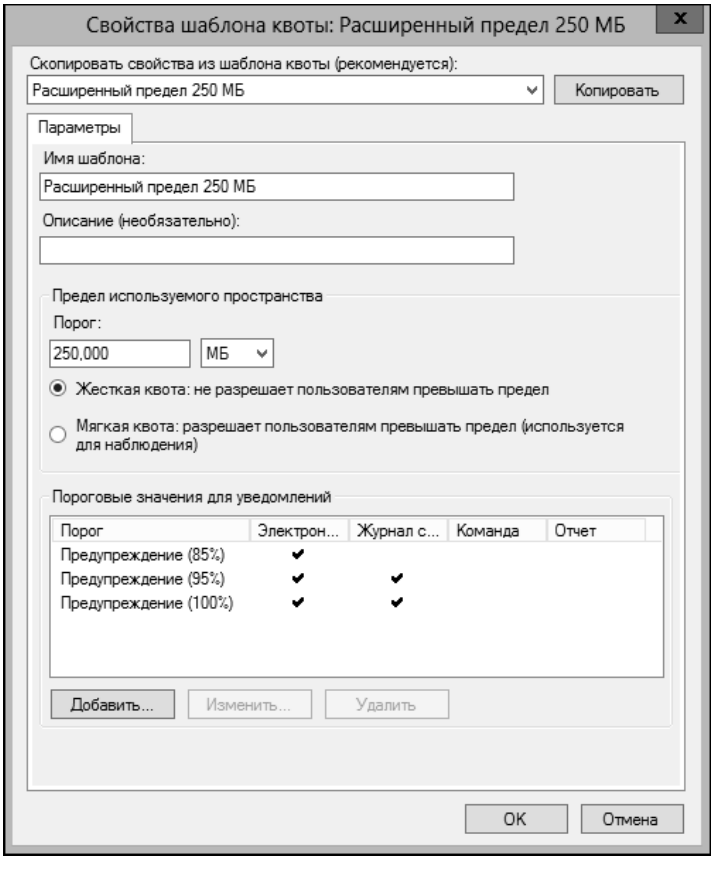


Рис. 12.21. Используйте свойства квоты для настройки предела, типа квоты и порогов уведомления

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) и

введите содержимое письма уведомления в поля **Тема** (Subject) и **Текст сообщения** (Message body).

В табл. 12.8 приведены доступные переменные 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. 12.8 приведены доступные переменные и их значения.
7. 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 по умолчанию, и они могут также быть отправлены назначенным администраторам. Используйте переменную `[Admin Email]`, чтобы указать администраторов по умолчанию, ранее указанных в глобальных параметрах.
8. Повторите действия 5—7 для определения дополнительных порогов уведомлений.
9. 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 13

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, чтобы 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 запланировать 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 быть один рабочий день, с другим — два рабочих дня. 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, что означает, что любое отключение сервера, вероятно, приведет к потере данных всего рабочего дня. RTO показывает, сколько фактически займет процедура восстановления и зависит от объема данных, который 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, чтобы определить, должен ли тот или иной файл или каталог быть заархивирован. Если атрибут включен, файл или каталог будет помещен в резервную копию. Могут осуществляться следующие основные типы резервных копий:

- **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, что сообщает, что в следующий раз файл нуждается 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. 13.1. 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 13.1. *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 Microsoft 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 заключается в периодическом перемещении дисков во внешнее хранилище.

Выбор утилиты для резервного копирования

Для использования в Windows Server 2012 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 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.
- **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 данные 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 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. Однако нельзя установить графические компоненты этих утилит при установке основных серверных компонентов (Server Core) Windows Server 2012. 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.

> ***Практический совет***
>
> При использовании утилиты **Система архивации данных Windows Server** с Microsoft Exchange Server 2010 можно использовать только полную резервную копию. Запуск утилит командной строки системы архивации данных для Exchange Server 2012 также не поддерживается. Для получения более подробной информации обратитесь к *главе 13* книги "Microsoft Exchange Server 2010 Administrator's Pocket Consultant"[1].

Введение в *Систему архивации данных Windows Server*

Для запуска утилиты **Системы архивации данных Windows Server** выберите соответствующую опцию из меню **Средства** в диспетчере серверов. 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. 13.1) 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).

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

[1] William R. Stanek. Microsoft Exchange Server 2010: Administrator's Pocket Consultant. — Microsoft Press, 2010.

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.

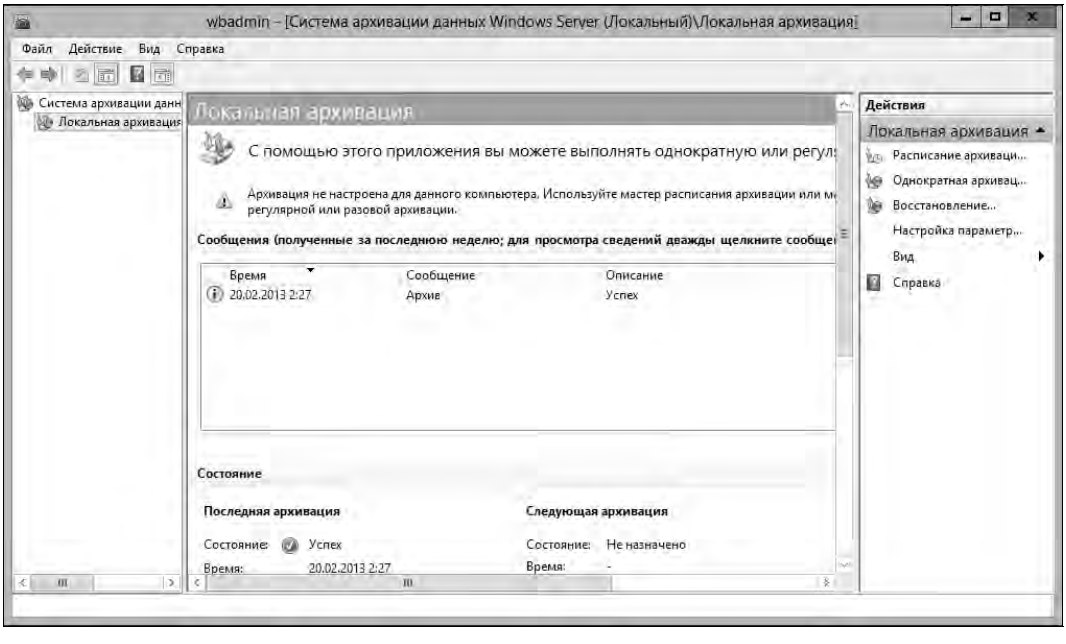


Рис. 13.1. Система архивации данных Windows Server предоставляет дружественный интерфейс для резервного копирования и восстановления

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 проис-

ходит 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 будет выполнено резервное копирование (полное или добавочное), 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. 13.2.

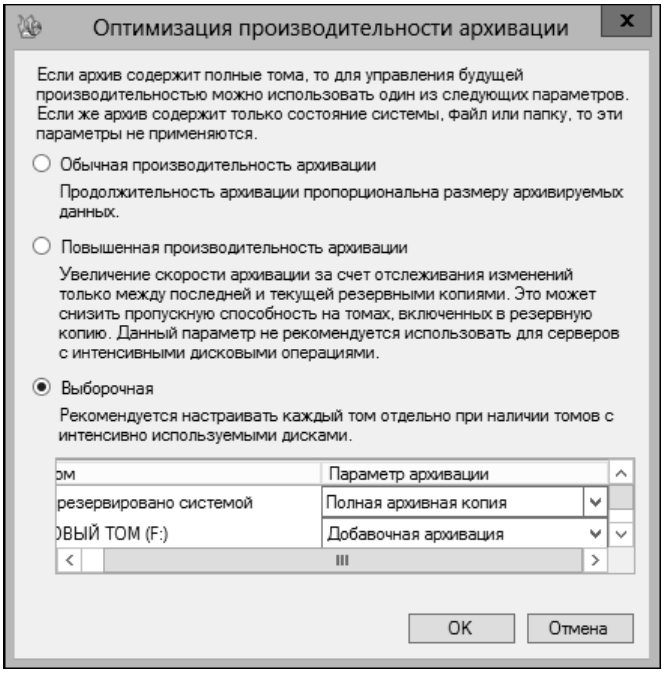


Рис. 13.2. Настройка параметров резервного копирования

2. Выберите одну из следующих опций и нажмите кнопку **OK**:
   - **Обычная производительность архивации** (Choose normal backup performance) для осуществления полного резервного копирования всех присоединенных дисков;
   - **Повышенная производительность архивации** (Choose 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. 13.2.

Таблица 13.2. *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 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

Таблица 13.2 *(окончание)*

Команда	Описание
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 запланирован-

ных 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 приложениями).** Выполняет резервное копирование всех томов с данными приложений, что позволяет полностью восстановить сервер, 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 с помощью 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 на 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. 13.3. Это место, необходимое для архивации данных сервера, приложений и состояния системы. Для архивации всех томов на сервере выберите опцию **Весь сервер** и нажмите кнопку **Далее**. Чтобы выбрать тома для архивации, установите переключатель **Настраиваемый** (Custom) и нажмите кнопку **Далее**.

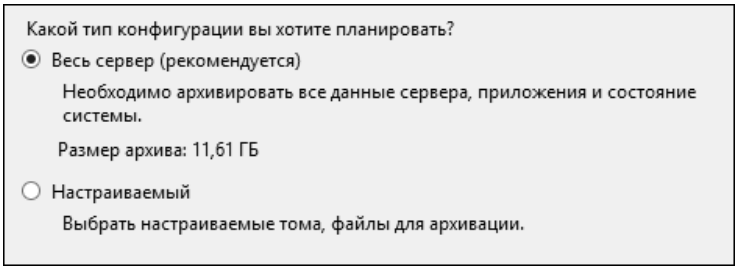


Рис. 13.3. Обратите внимание на размер резервной копии

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 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. 13.4, можно выбрать тома, которые нужно добавить в резервную копию. Если необходимо полностью восстановить систему, выберите опцию **Восстановление исходного состояния системы** (Bare metal recovery).

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. 13.5) 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 выполнять 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 вре-

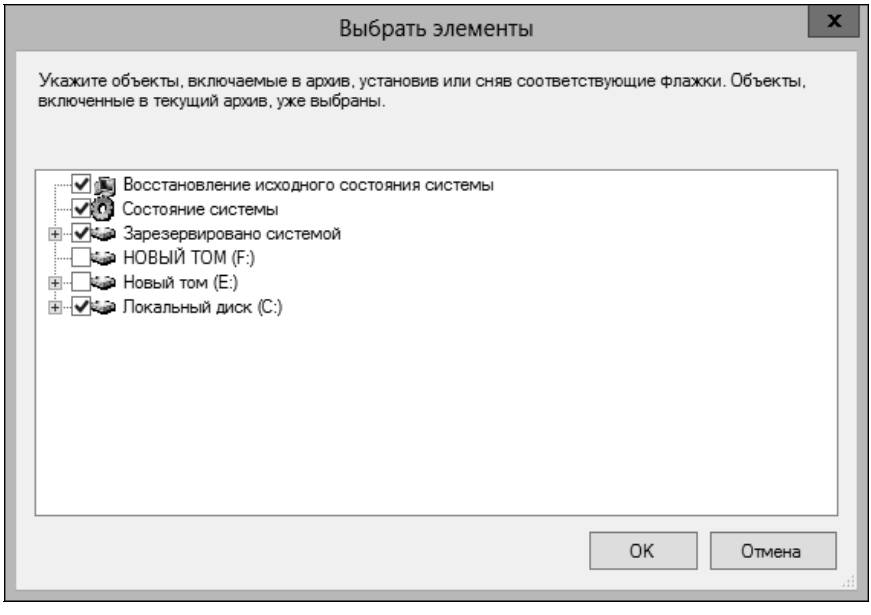


Рис. 13.4. Выберите элементы для включения в резервную копию

Рис. 13.5. Выберите время запуска архивации

мя 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—6 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` — разделенный запятыми список элементов, 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 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 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 может использовать процесс обновления, чтобы отметить файлы для обновления и затем автоматически заменить файлы при следующем запуске приложения. В некоторых случаях Windows Server 2012 может сохранить данные приложения, закрыть приложение, обновить файлы и затем перезапустить приложение. Чтобы улучшить общую производительность системы и скорость отклика, Windows Server 2012 более эффективно использует память, осуществляет упорядоченное выполнение групп потоков и предоставляет несколько механизмов диспетчеризации процессов. Благодаря оптимизации памяти и использованию процесса, в Windows Server 2012 фоновые процессы оказывают меньше влияния на производительность системы.

Операционная система Windows Server 2012 предоставляет дополнительные подробности в сообщениях об ошибке, что в конечном счете упрощает идентификацию и решение проблемы. ОС Windows Server 2012 использует политики восстановления после сбоя служб более эффективно, чем ее предшественники. Восстанавливая отказавшую службу, Windows Server 2012 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 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 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 реше-

ние, 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 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 содержит встроенную диагностику и автоматически обнаруживает поврежденные системы файлов во время запуска и позволяет произвести автоматическое или ручное восстановление. Для решения проблемы запуска Windows Server 2012 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 Монитора производительности (Performance Monitor) и Монитора стабильности работы (Reliability Monitor) *(см. главу 3)*.

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 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 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 примерно 50 000 файлов системного состояния, которые занимают примерно 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 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 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 инсталляционным 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 выберите 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 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. 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 любые 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, начиная с Windows XP SP1 и более поздних версий Windows, используется алгоритм AES (Advanced Encryption Standard) для шифрования файлов в EFS. AES не поддерживается в Windows 2000 или в Windows XP до SP1, а зашифрованные с помощью AES файлы на таких компьютерах считаются поврежденными, хотя на самом деле это не так. 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 использовать 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 управляющий 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, который был назначен пользователю как сертификат 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 которым нужно работать. Нажмите кнопку **OK**, а затем кнопку **Далее**. Нажмите кнопку **Готово** для добавления агента восстановления.

   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.

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.

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**.

часть IV

Администрирование сети в Windows Server 2012

ГЛАВА 14

Управление TCP/IP-сетью

Администратор разрешает компьютерам взаимодействовать по сети, используя базовые сетевые протоколы, встроенные в Windows Server 2012. 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

В Windows Server 2012 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, на которых и основаны эти утилиты:

- **Сетевое обнаружение** (Network Discovery) — компонент Windows Server 2012, управляющий способностью видеть другие компьютеры и устройства;
- **Служба сетевого расположения** (Network Awareness) — компонент Windows Server 2012, 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 компью-

теру подключаться к одному 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 выбора лучшего 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. 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 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. 14.1, 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 не является членом домена, будет отображено соответствующее 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. 14.2, предоставляет информацию о текущем состоянии сети, а также обзор текущей конфигурации сети. Чтобы открыть Центр управления сетями и общим доступом в Панели

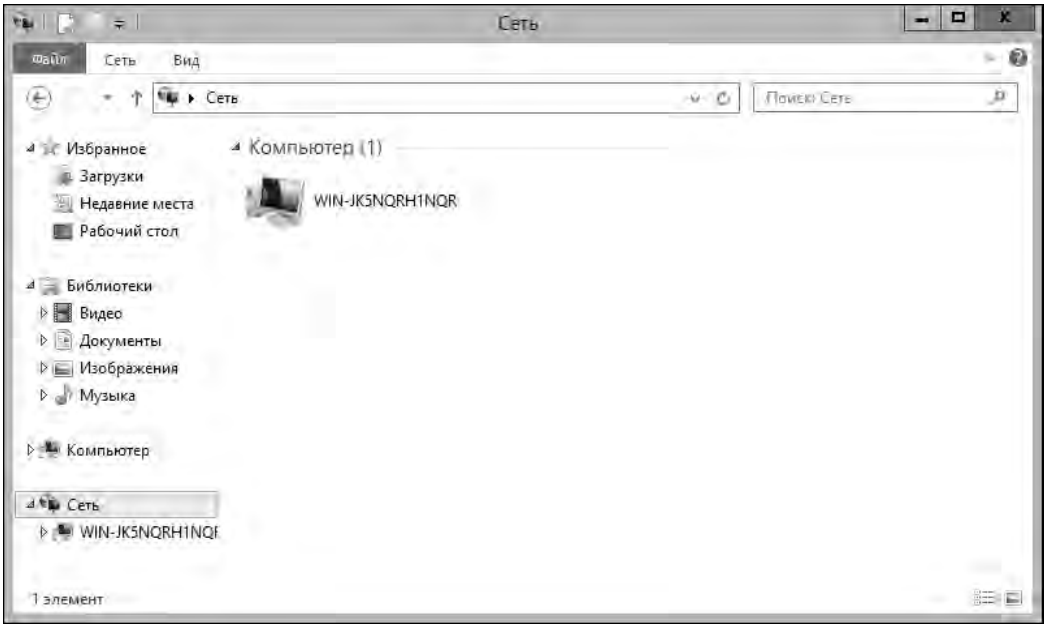


Рис. 14.1. Используйте обозреватель сети для просмотра сетевых ресурсов

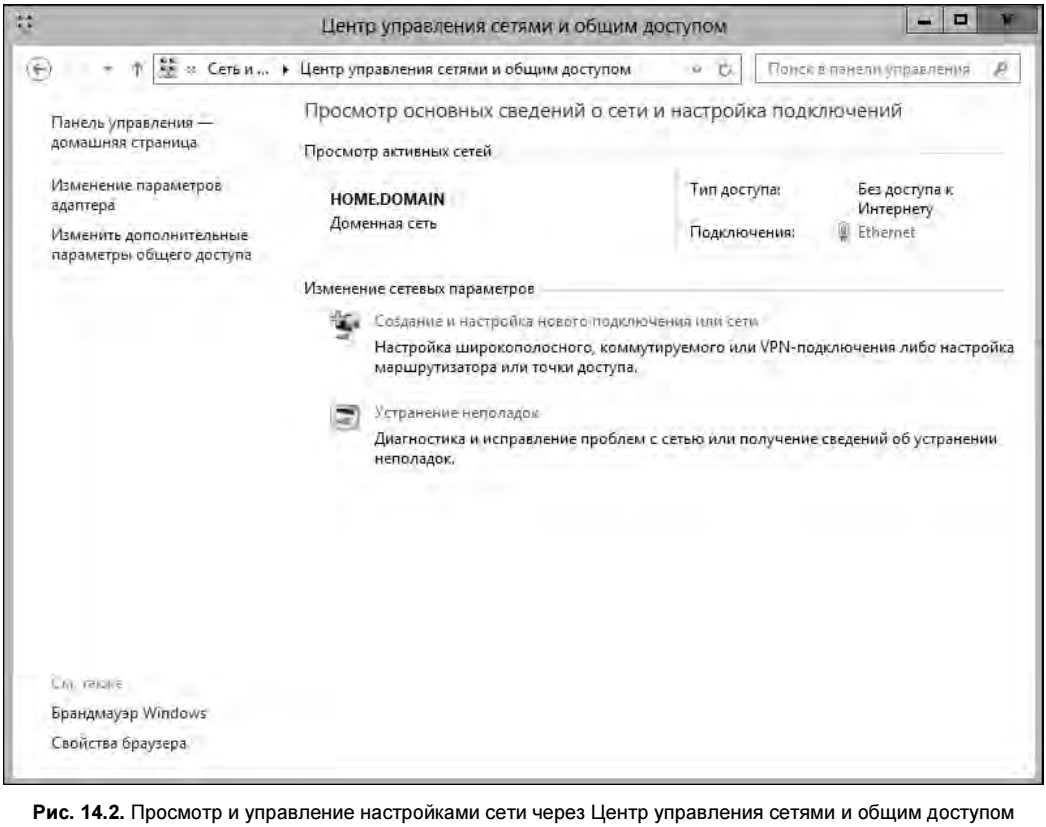


Рис. 14.2. Просмотр и управление настройками сети через Центр управления сетями и общим доступом

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 нажмите 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].

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.

Управление сетью в Windows 8 и Windows Server 2012

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

[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.*

подключения этих клиентов к проводным 802.3 Ethernet-сетям. Для Windows 7 и более поздних версий Windows доступны опции, запрещающие использование общих учетных данных и включающие период блокировки, что запрещает 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. Использование HTTP по SSL 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 CAPI 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 позволяет использовать 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 предоставления 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 установлено это приложение, 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 под-

писывать 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).

Установка сети TCP/IP

Для установки сети на компьютере нужно установить поддержку TCP/IP и сетевой адаптер. В системе Windows Server 2012 протокол TCP/IP используется в качестве стандартного протокола глобальных сетей. Обычно установка сети происходит одновременно с установкой Windows Server 2012. Администратор также может установить протокол TCP/IP в свойствах подключения по локальной сети.

Для установки TCP/IP после установки Windows Server 2012 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).
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. 14.3).

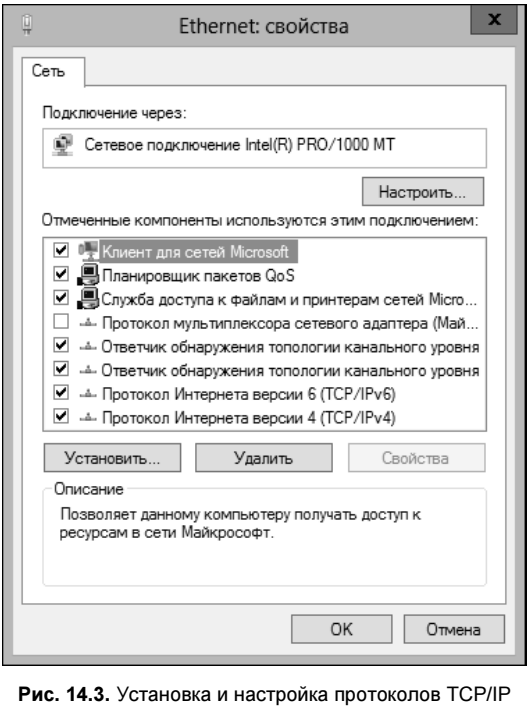


Рис. 14.3. Установка и настройка протоколов TCP/IP

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 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 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 пе-

ременное 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. 14.1.

Таблица 14.1. *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 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 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 или использовать автоматический альтернативный адрес, или 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. 14.1, 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 так, что они будут использовать несколько основных шлюзов. При назначении нескольких шлюзов ОС Windows Server 2012 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 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. 14.4.
4. Панель **Основные шлюзы** (Default gateways) показывает 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 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**.

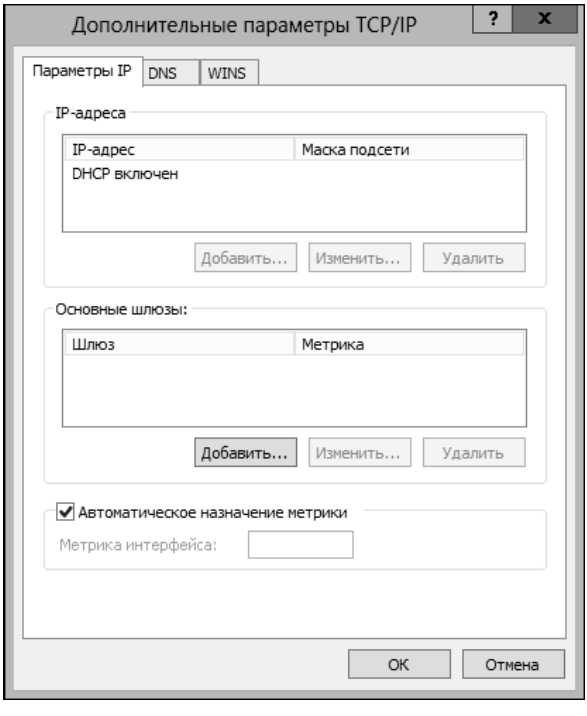


Рис. 14.4. Настройте несколько IP-адресов шлюзов в окне **Дополнительные параметры TCP/IP**

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.

После установки Hyper-V на сервер и включения внешней виртуальной сети будет использоваться переключение виртуальной сети. Как показано на рис. 14.5, 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.

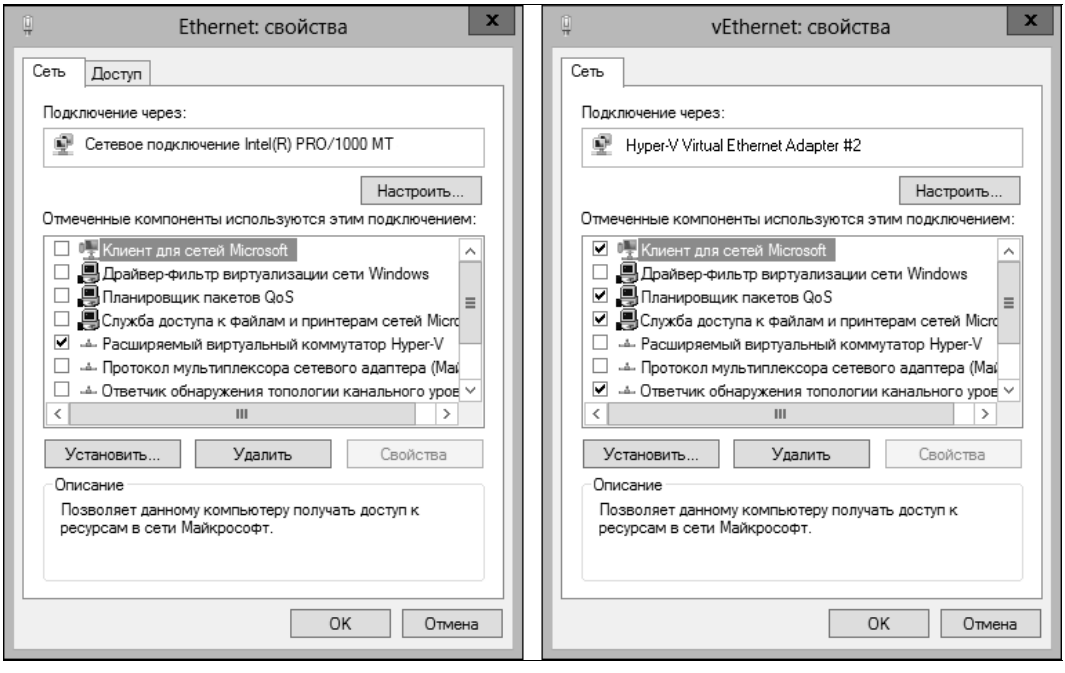


Рис. 14.5. Корректная конфигурация для доступа виртуальных машин к сети

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 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 15

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 информа-

цию 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 нужно установить в сети. Обычно нужно как минимум два DHCP-сервера в физическом сегменте сети. Операционная система Windows Server 2012 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 *главах 1* и *14*, 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 получений 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. У клиентов IPv6 под управлением Windows XP или Windows Server 2003 нет DHCPv6-клиента, поэтому они игнорируют флаги M и O в объявлениях маршрутизаторов.

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 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 жесткий 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 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 **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 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 использованием 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. 15.1. Главное окно 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.

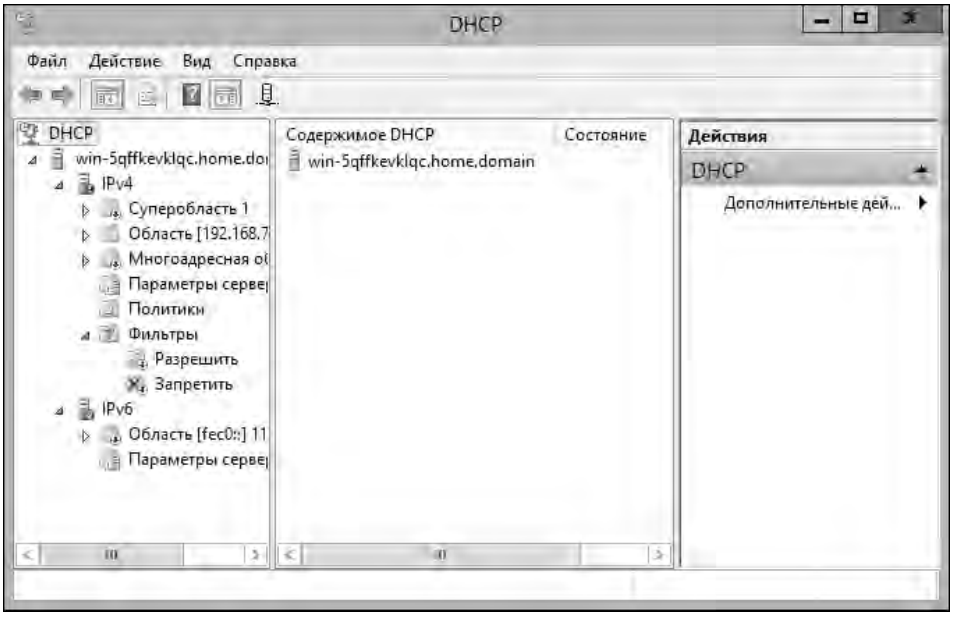


Рис. 15.1. Используйте консоль DHCP
для создания и управления конфигурациями DHCP-сервера

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. 15.2.
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.

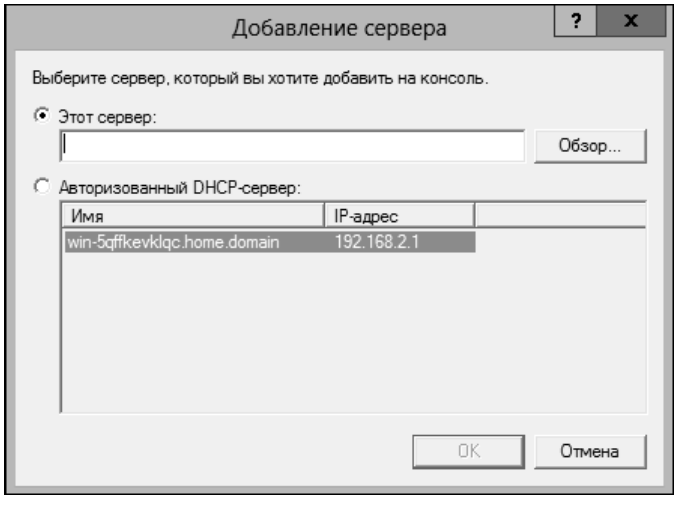


Рис. 15.2. Если нужного DHCP-сервера нет в списке, добавьте его с помощью команды **Добавить сервер**

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 авторизация требуется для предотвращения обслуживания клиентов неавторизованными DHCP-серверами.

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).

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.
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 и 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 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 одни и те же журналы, но можно настроить и раздельный аудит. Стандартное расположение журналов DHCP — *%SystemRoot%*\System32\DHCP. В этой папке находятся журналы для каждого дня недели. Файл журнала понедельника называется DhcpSrvLog-Mon.log, файл журнала вторника — Dhcp-SrvLog-Tue.log, 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 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 Windows Server 2012 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. 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. 15.3 показаны значения DNS-интеграции по умолчанию для IPv4 и IPv6. Поскольку параметры настроены по умолчанию, обычно их не нужно модифицировать.

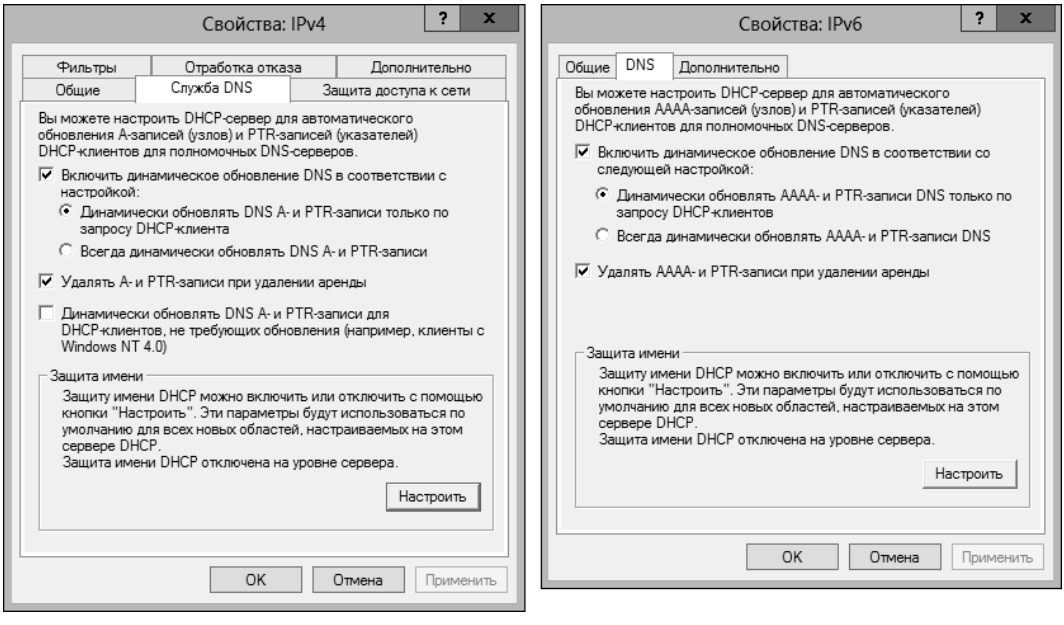


Рис. 15.3. Параметры DNS-интеграции для IPv4 и IPv6

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**.

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. Из меню **Средства** диспетчера серверов выберите команду **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. 15.4, имя политики по умолчанию будет **NAP DHCP**. Нажмите кнопку **Далее**.

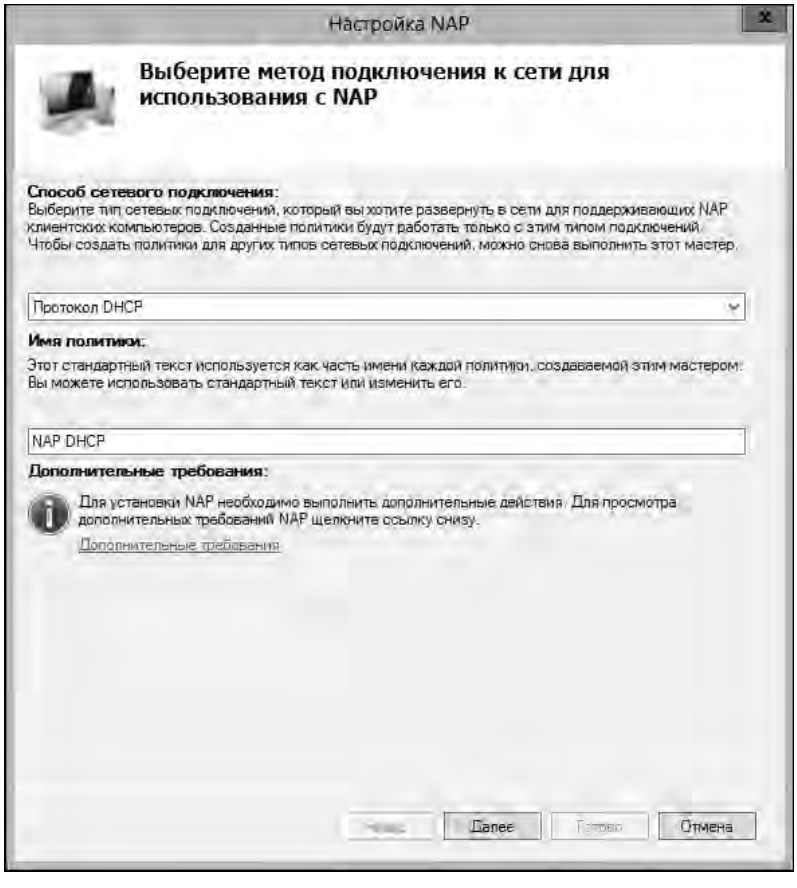


Рис. 15.4. Настройка политики NAP для локального DHCP-сервера

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**.
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. 15.5) 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.

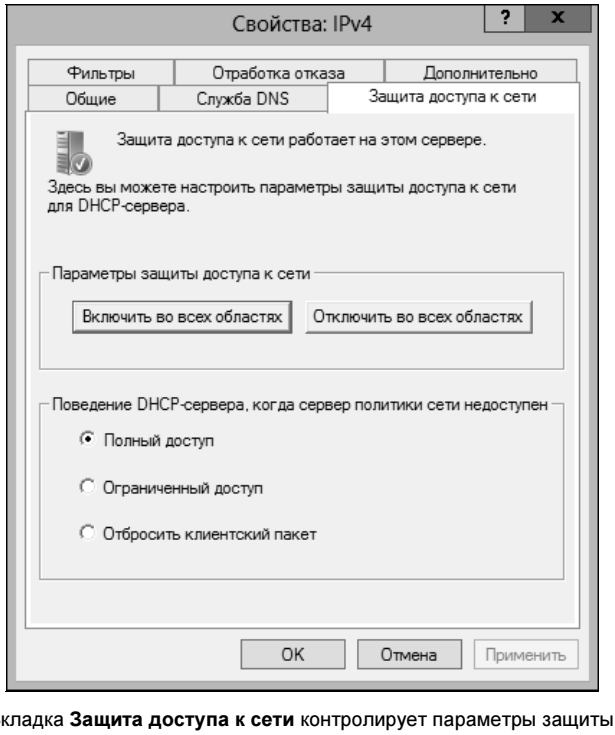


Рис. 15.5. Вкладка **Защита доступа к сети** контролирует параметры защиты для DHCP

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 использовать, а любой другой компьютер, который пытается использовать этот же адрес, будет блокирован от его использования.

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 определяет 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.

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 ранее в *разд. "Области адресов"*, 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 нужно 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. 15.6). Если подсети не используются, оставьте стандартные значения.
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.

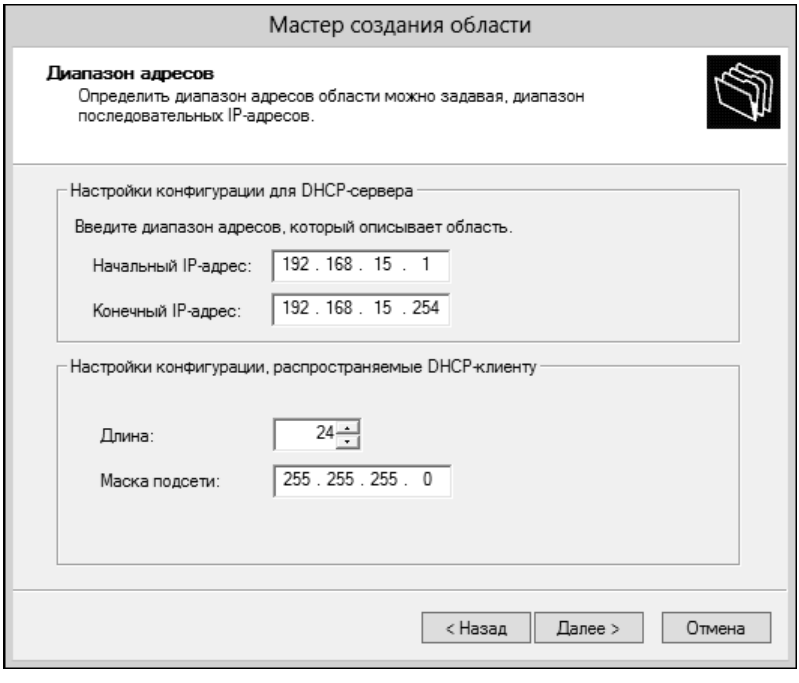


Рис. 15.6. В мастере создания области введите диапазон IP-адресов для области

- 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 3 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. 15.7. Введите имя родительского домена, который следует использовать для разрешения не полностью определенных имен компьютеров.

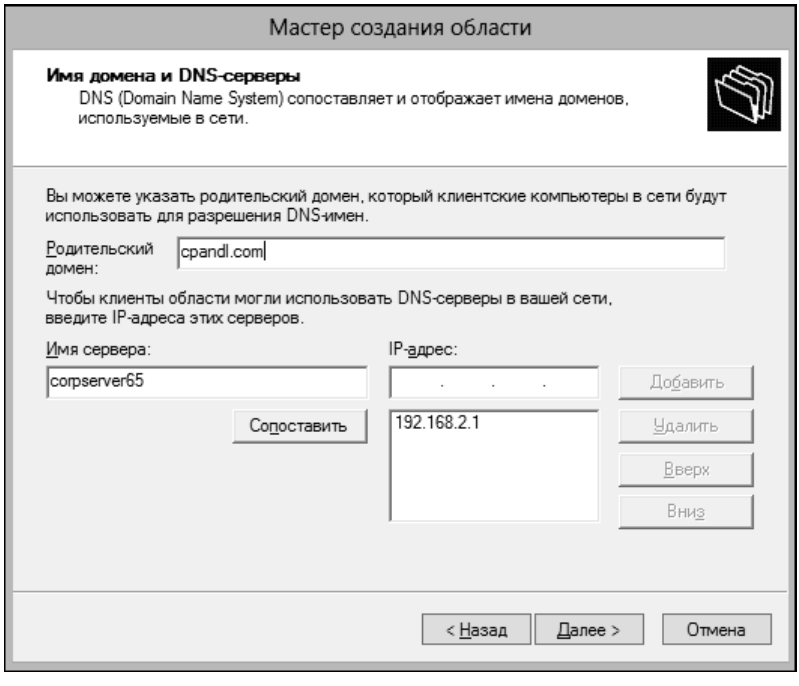


Рис. 15.7. Используйте страницу **Имя домена и DNS-серверы** для настройки параметров DNS по умолчанию для DNS-клиентов

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**.

> ***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).

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. 15.8) введите 64-битный префикс сети и затем установите предпочтение. Нажмите кнопку **Далее**.

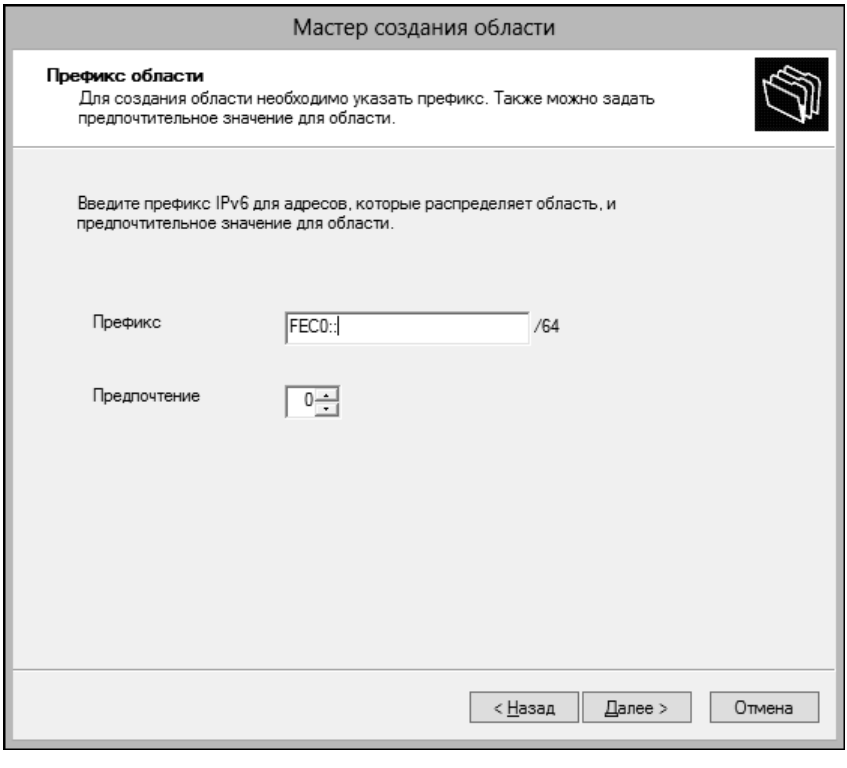


Рис. 15.8. В окне мастера создания области введите префикс сети и предпочтение

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. 15.9) 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**.

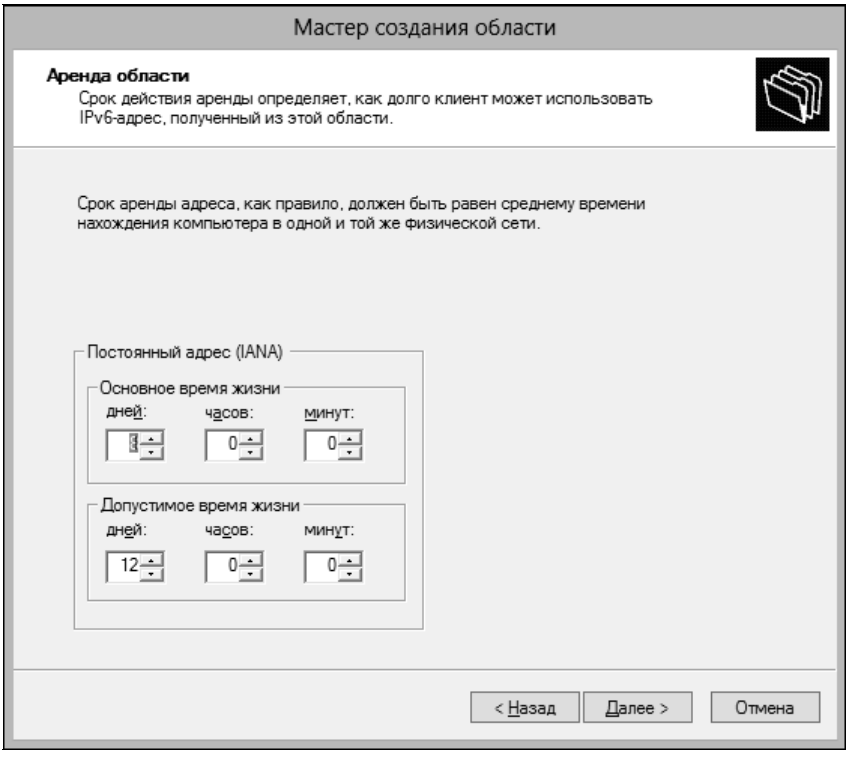


Рис. 15.9. Укажите продолжительность постоянной аренды

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 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 новую 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 определенное 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. 15.10). Повторите этот процесс для настройки всех остальных параметров.
4. Нажмите кнопку **OK**.

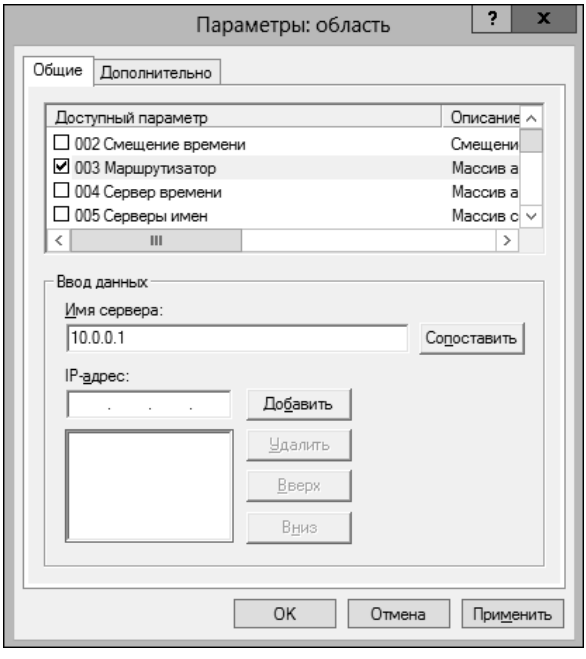


Рис. 15.10. Выберите параметр, который нужно настроить в окне **Параметры: область**, и введите требуемую информацию в область **Ввод данных**

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 **Параметры: 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 по ней правой кнопкой мыши в консоли DHCP и выберите команду **Активировать**. Чтобы деактивировать активную область, щелкните ее правой кнопкой мыши в консоли DHCP и выберите команду **Деактивировать**.

> ***Совет***
>
> 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**.

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 балансировку 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**.
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. 15.11) 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;
   - 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.

[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.*

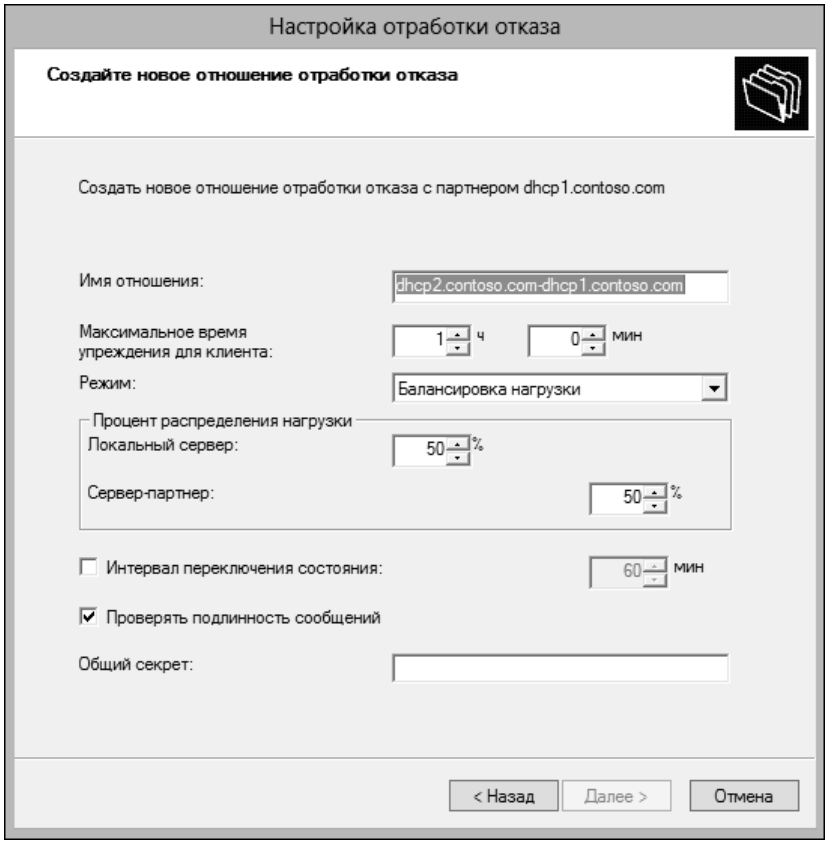


Рис. 15.11. Укажите процент разбивки

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

область 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:

1. 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.
2. 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.
3. 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**.

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.

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 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 фалы, 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;
- J500000A.log, J500000B.log, J500000C.log, J500000D.log, J500000E.log, J500000F.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.
5. Чтобы вернуть активные аренды для каждой области, нужно согласовать области сервера, как будет показано в следующем разделе.
6. 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 16

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. 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. Эти 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 называются *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

Как было упомянуто в *главе 6*, 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.

При установке 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.

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 14*, 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 FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2 и FEC0:0:0:FFFF::3. Чтобы добавить IPv6-адреса DNS-серверов используйте окно свойств протокола TCP/IPv6 или следующую команду:

```
netsh interface IPV6 ADD DNS
```

Серверы DNS, работающие под управлением Windows Server 2008 R2 или более поздних выпусков, в равной мере поддерживают протоколы IPv4 и IPv6. В консоли **Диспетчер DNS** (DNS Manager) адреса хостов отображаются как IPv4- или IPv6-адреса, соответственно. 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 15*. 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 Windows Server 2012 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**. В окне **Сетевые подключения** щелкните правой кнопкой мыши по нужному подключению и выберите команду **Свойства**.
2. Дважды щелкните по протоколу, который хотите настроить — **TCP/IPv6** или **TCP/IPv4**.
3. 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.
4. 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 роди-

тельском 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 выполняется. 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 задастся 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 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 хранится 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 база 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 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 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 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\WinServer2-12\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. 16.1) выберите команду **DNS** из меню **Средства** в диспетчере серверов.

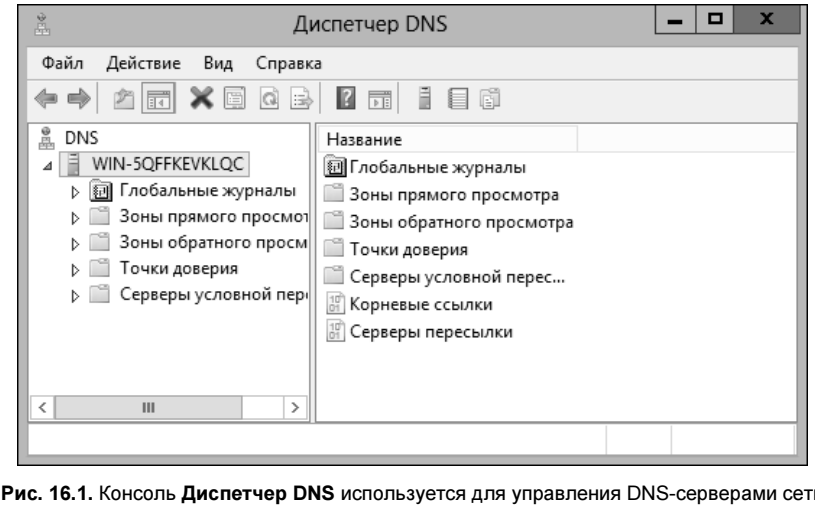


Рис. 16.1. Консоль **Диспетчер DNS** используется для управления DNS-серверами сети

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**;
    - 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. 16.2).

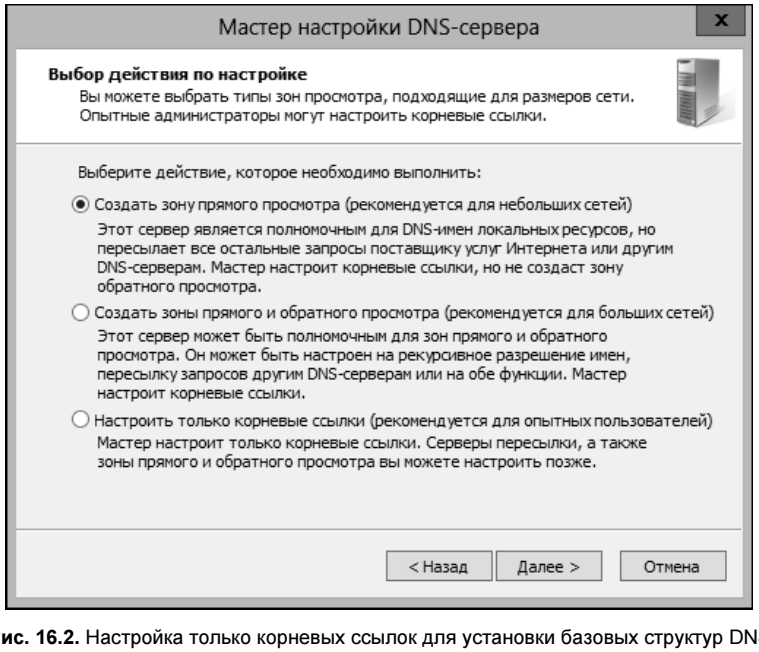


Рис. 16.2. Настройка только корневых ссылок для установки базовых структур DNS

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. 16.3). 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**.

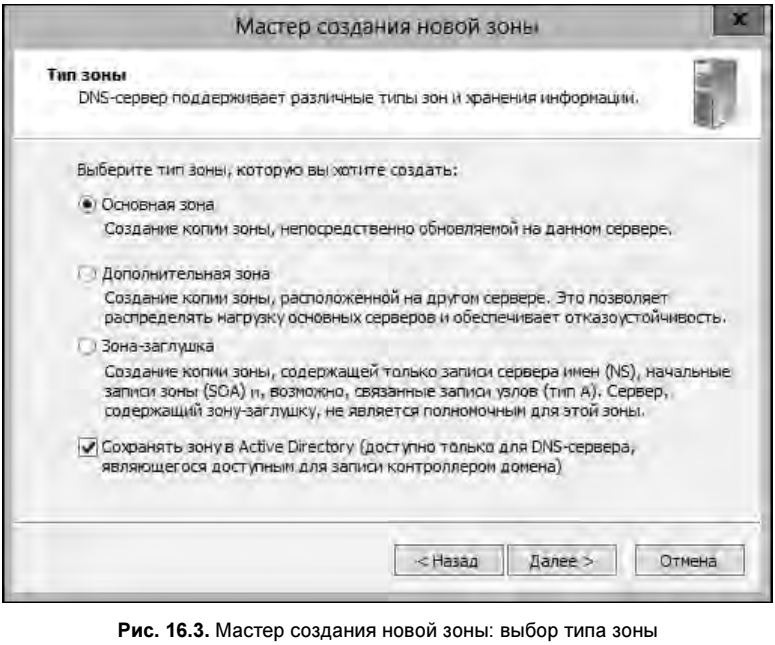


Рис. 16.3. Мастер создания новой зоны: выбор типа зоны

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.
   - **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 зона 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 повто-

рить 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.
>
> Приватные 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 приватной 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 14*.

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.

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 выбери-

те 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**.
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 `dnscmd` *`ServerName`* `/enableglobalnamessupport 1`, где *`ServerName`* — имя DNS-сервера, содержащего зону GlobalNames. Чтобы указать локальный компьютер, введите точку (.) вместо имени компьютера, например, `dnscmd . /enableglobalnamessupport 1`.
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. 16.4, 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.

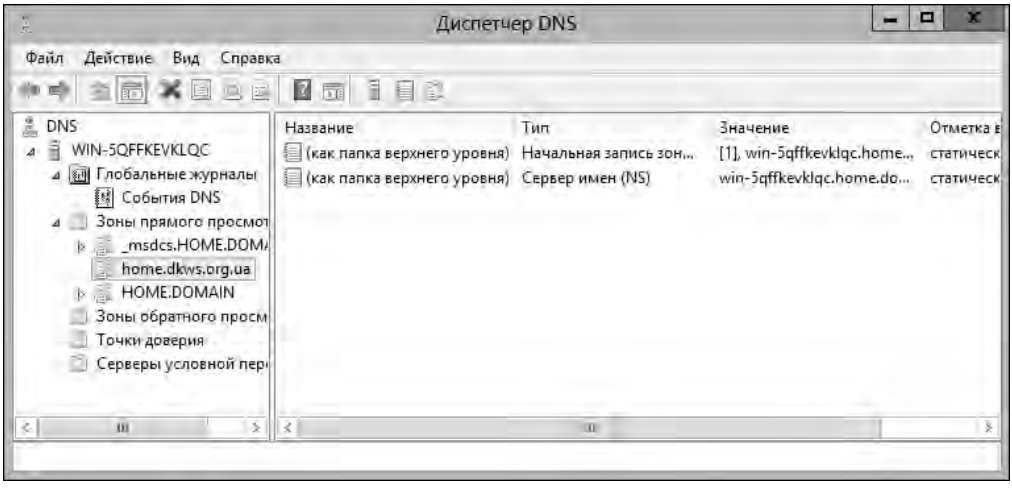


Рис. 16.4. Управляйте локальным и удаленными DNS-серверами с помощью консоли **Диспетчер DNS**

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 попытается подключиться к серверу. Если получится, сервер будет добавлен в консоль.

> ***Примечание***
>
> Если сервер отключен от сети или недоступен по другой причине, 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 удаляет 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 сервер 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 определяется 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 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 обновленными стандартами DNSSEC (стандарты NSEC3 и RSA/SHA-2). Ранее записи подписывались с помощью стандартов NSEC3 и RSA/SHA-2.

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 системой, 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. Закрытый 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 DNS** 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. 16.5). Введенное имя будет отражено в поле **Полное доменное имя (FQDN)** (Fully qualified domain name (FQDN)).

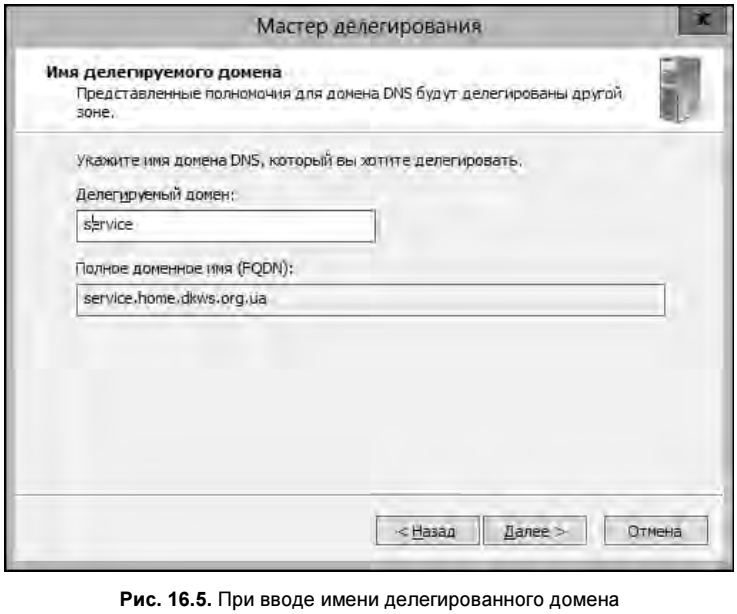


Рис. 16.5. При вводе имени делегированного домена

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.

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. 16.6.

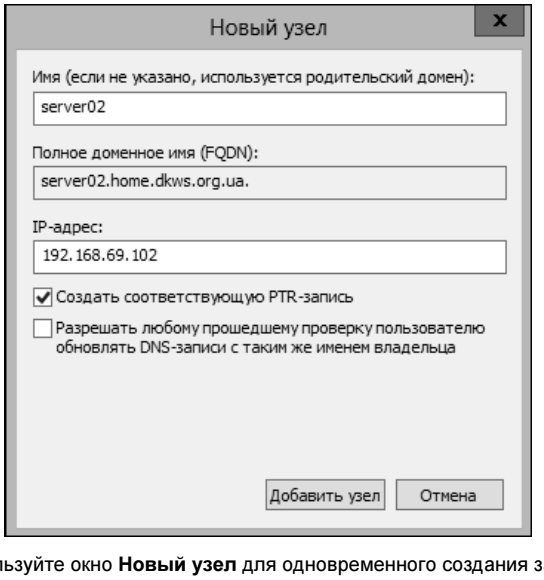


Рис. 16.6. Используйте окно **Новый узел** для одновременного создания записей A и PTR

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. 16.7).
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.

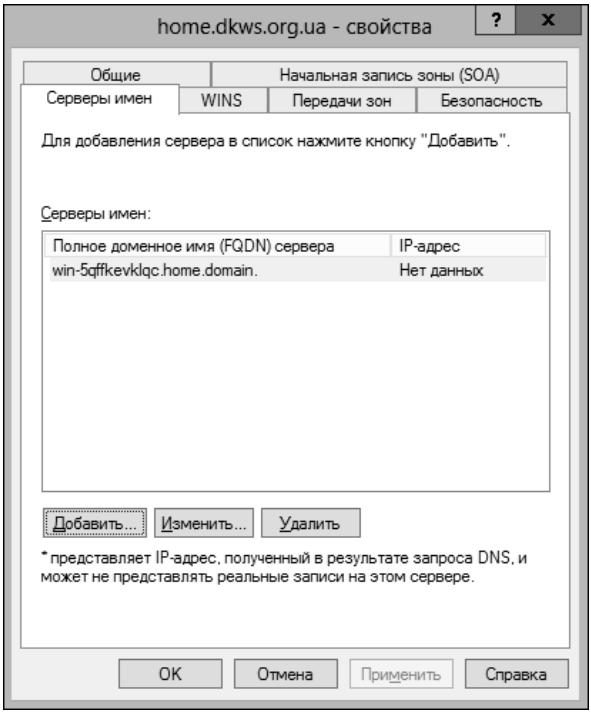


Рис. 16.7. Настройте серверы имен для домена

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. 16.8.

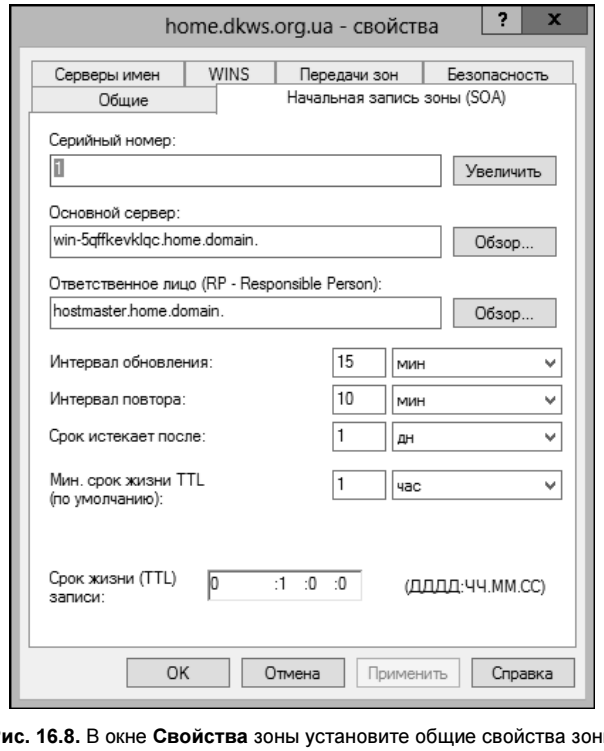


Рис. 16.8. В окне **Свойства** зоны установите общие свойства зоны

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 жизни 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 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. 16.9).

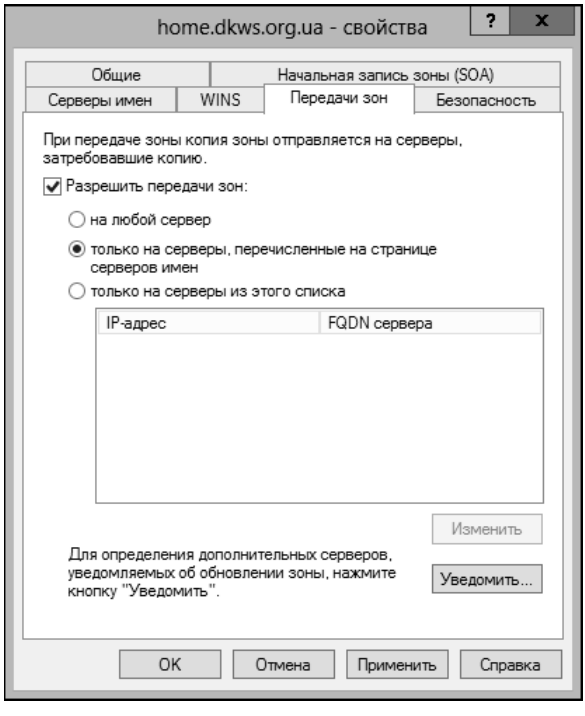


Рис. 16.9. Настройка передачи зон

3. Чтобы ограничить переносы серверами имен, перечисленными на вкладке **Серверы имен** (Name Servers), установите флажок **Разрешить передачи зон** (Allow zone transfers) и установите 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. 16.10.

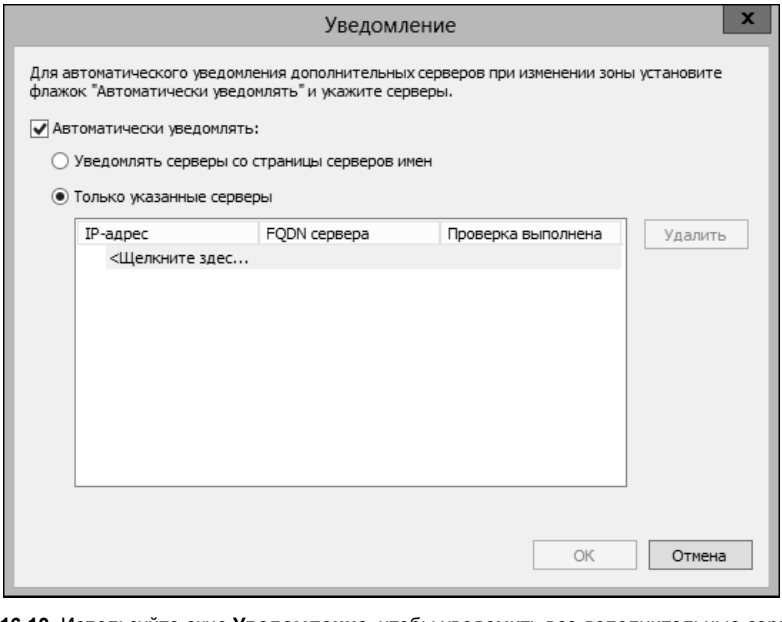


Рис. 16.10. Используйте окно **Уведомление**, чтобы уведомить все дополнительные серверы, указанные либо на вкладке **Серверы имен**, или в списке этого окна

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 15*.

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 серве-

ра 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 об-**

разом (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 (для совместимости с ОС Windows 2000)** (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

Как правило, 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. 16.11), установите флажок **Записывать пакеты в журнал для отладки** (Log packets for debugging), а затем отметьте флажки событий, временное наблюдение за которыми необходимо вести.

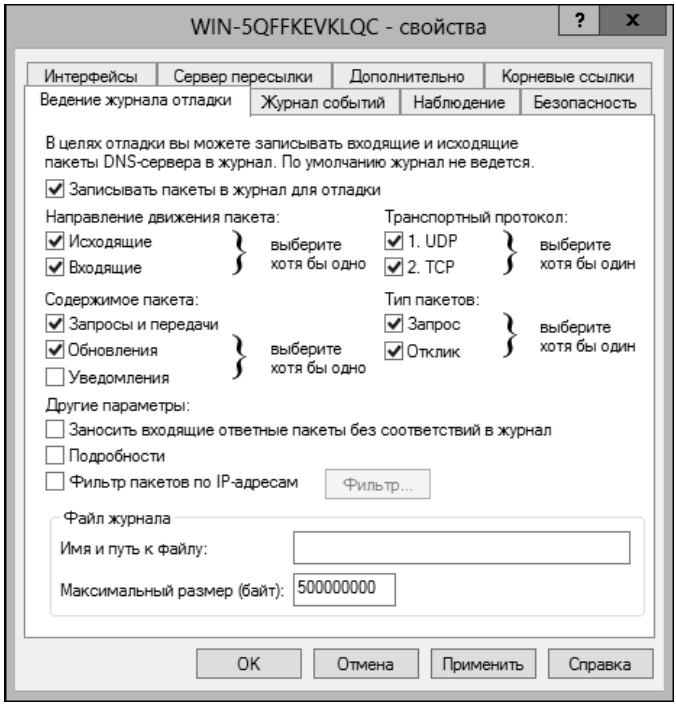


Рис. 16.11. Используйте вкладку **Ведение журнала отладки** для выбора отслеживаемых событий

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).

Мониторинг DNS-сервера

В ОС Windows Server 2012 есть встроенная возможность 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. 16.12). 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.

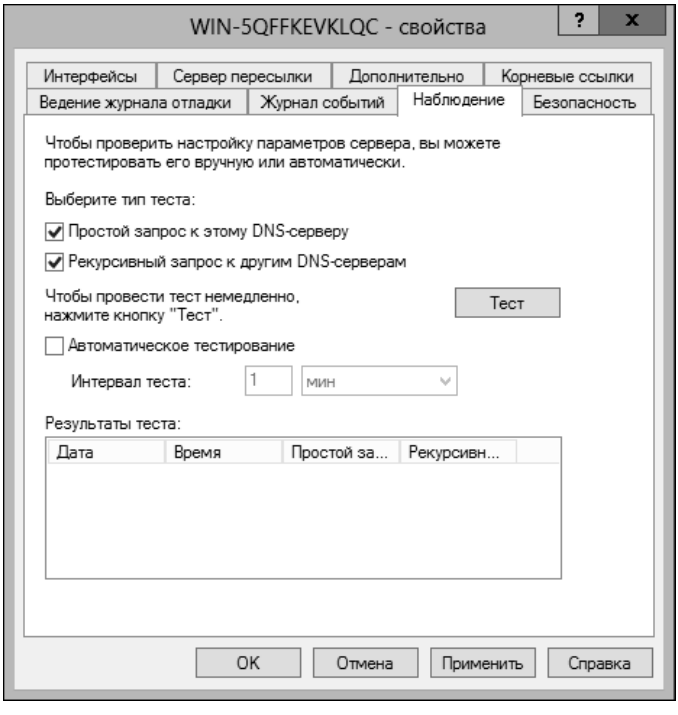


Рис. 16.12. Можно произвести ручное наблюдение или настроить сервер для автоматического мониторинга

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**.

Практический совет

Если 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 длинный временной интервал, например два или три часа.

Предметный указатель

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

Д

Ж

З

И

К

Л

М

О

П

P

C

T

У