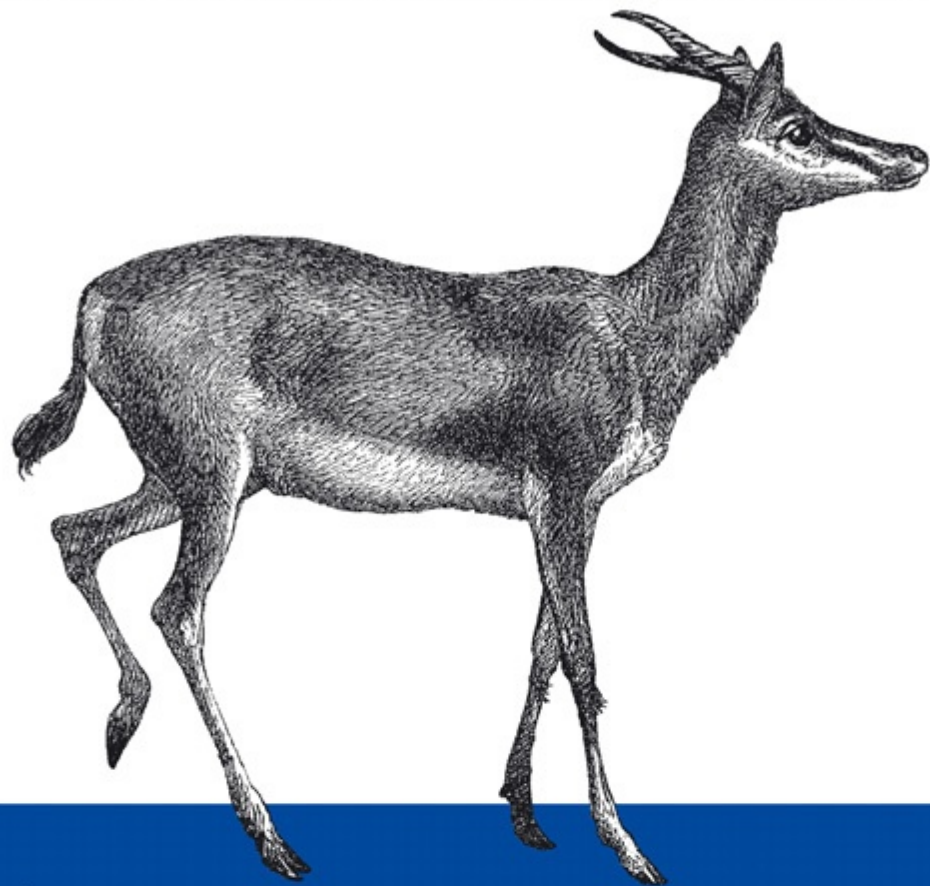


Развертывание, настройка и управление Windows Server 2012



Администрирование
Microsoft
**Windows
Server 2012**

O'REILLY®

Самара Линн



Samara Lynn

Windows Server 2012: Up and Running

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo

Самара Линн

Администрирование

Microsoft

Windows Server 2012



Москва • Санкт-Петербург • Нижний Новгород • Воронеж
Ростов-на-Дону • Екатеринбург • Самара • Новосибирск
Киев • Харьков • Минск

2014

ББК 32.988.02-018.2
УДК 004.451.9
Л59

- Линн С.**
Л59 Администрирование Microsoft Windows Server 2012. — СПб.: Питер, 2014. — 304 с.: ил. — (Серия «Бестселлеры O'Reilly»).

ISBN 978-5-496-00621-7

Эта книга представляет собой руководство по развертыванию, настройке, защите и управлению Windows Server 2012. Здесь рассмотрены такие вопросы, как новый подход к администрированию Windows Server и новые возможности Active Directory, примеры работы с системой Dynamic Access Control, улучшение организации хранилищ данных, кластеризации и Hyper-V, технологии унифицированного удаленного доступа (Unified Remote Access). Также в книге описываются новые способы решения проблем в работе Windows Server 2012 и приводятся дополнительные сведения об этой системе.

12+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.988.02-018.2
УДК 004.451.9

Права на издание получены по соглашению с O'Reilly. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-1449320751 англ.

© Authorized Russian translation of the English edition of titled Windows Server 2012: Up and Running (ISBN 9781449320751) © 2013 Samara Lynn. This translation is published and sold by permission of O'Reilly Media, Inc., which owns or controls all rights to publish and sell the same.

ISBN 978-5-496-00621-7

© Перевод на русский язык ООО Издательство «Питер», 2014

© Издание на русском языке, оформление ООО Издательство «Питер», 2014

Краткое содержание

Предисловие..	14
Глава 1. Обзор Windows Server 2012	18
Глава 2. Аппаратные требования Server 2012 и установка	32
Глава 3. Управление Windows Server 2012	66
Глава 4. Active Directory..	98
Глава 5. Динамический контроль доступа при управлении пользователями и данными	128
Глава 6. Управление хранилищами и кластеризация	154

Глава 7. Hyper-V	175
Глава 8. Сетевые возможности	203
Глава 9. Удаленный доступ	239
Глава 10. Решение проблем, безопасность и мониторинг	279
Об авторе	298

Содержание

Предисловие	14
Об этой книге	14
Читательская аудитория	14
Цели книги	15
Структура книги	15
Правовые вопросы	16
Благодарности	16
 Глава 1. Обзор Windows Server 2012	18
Введение в Windows Server 2012	18
Новые возможности и улучшенные функции	20
Установка и интерфейс	20
Управление	21

Windows Power Shell 3.0	23
Хранилища данных	24
Удаленный доступ	24
Сетевое взаимодействие	25
Hyper-V 3.0	26
IIS 8	29
Безопасность	29
Кластеризация	30
Аппаратные требования	31
Выводы	31

Глава 2. Аппаратные требования Server 2012

и установка	32
Редакции Server 2012	33
Server 2012 Datacenter	33
Server 2012 Standard	34
Server 2012 Essentials	34
Server 2012 Foundation	35
Аппаратные требования Server 2012	35
Аппаратные требования для Hyper-V 3.0	36
Установка Server 2012	36
Конфигурация установки основных компонентов сервера	39
Установка сервера с графическим интерфейсом	50
Переключение между режимами установки	53
Переход от сервера, на котором установлены лишь основные компоненты, к серверу с пользовательским интерфейсом	54
Переход от сервера с пользовательским интерфейсом к серверу, на котором установлены лишь основные компоненты	59
Развертывание минимального интерфейса сервера	60
Настройка интерфейса с помощью компонентов по требованию	63
Выводы	64

Глава 3. Управление Windows Server 2012	66
Интерфейс Server 2012	68
Работа с плиточным интерфейсом	70
Использование средств управления сервером.	73
Поиск средств управления сервером	73
Запуск приложения от имени администратора.	74
Запуск консоли управления Microsoft	74
Настройка интерфейса.	75
Настройка Рабочего стола	75
Настройка начального экрана.. . . .	80
Выход из системы, перезагрузка и отключение питания.	80
Поиск.	81
Диспетчер серверов	82
Запуск диспетчера серверов и работа с ним	83
Добавление серверных ролей и компонентов	83
Управление несколькими серверами и группами серверов	91
Добавление в диспетчер серверов предыдущих версий серверов	91
Удаленное управление Server 2012	93
Установка RSAT	93
Выводы	96
 Глава 4. Active Directory.. . . .	 98
Развертывание доменных служб Active Directory	99
Установка Active Directory	99
Добавление компьютеров к домену Server 2012	106
Подключение к домену Server 2012 компьютера, работающего под управлением Windows 7	107
Добавление компьютеров под управлением Windows 8 к домену Server 2012.. . . .	110
Добавление систем под управлением Server 2012 к домену уровня функциональности Server 2008 R2	112

Управление Active Directory	113
Работа с ADAC	113
Корзина AD	119
Поиск с помощью ADAC	121
Журнал Windows PowerShell	124
Использование PowerShell для развертывания ActiveDirectory . . .	125
Выводы	127

Глава 5. Динамический контроль доступа

при управлении пользователями и данными	128
Составные части DAC	130
Предварительные требования и советы	131
Развертывание DAC	132
Подготовка утверждений	133
Настройка свойства ресурса для файлов	134
Добавление свойства ресурса в глобальный список свойств ресурсов	135
Создание нового централизованного правила доступа	137
Создание централизованной политики доступа	139
Публикация централизованной политики доступа	139
Настройка файлового сервера	141
Применение к папке централизованной политики	141
Проверка конфигурации	142
Помощь при ошибке «Отказано в доступе»	144
Развертывание системы помощи при отказе в доступе	145
Аудит	147
Автоматическая классификация файлов	150
Шифрование классифицированных файлов	152
Выводы	153

Глава 6. Управление хранилищами и кластеризация	154
Сравнение ReFS и NTFS	156
Создание пространства данных	157
Кластеризация	161
Настройка отказоустойчивого кластера	163
Создание кластера	164
Кластерное обновление	170
Выводы	173
 Глава 7. Hyper-V	 175
Системные требования	178
Установка роли Hyper-V.	179
Создание и настройка виртуальных машин.. . . .	182
Настройка виртуальных дисков	182
Создание виртуальных машин	185
Управление виртуальными машинами и виртуальными дисками ..	187
Динамическая миграция виртуальных машин	187
Реплика Hyper-V	191
Клонирование виртуального контроллера домена	194
Объединение мгновенных снимков.. . . .	198
Производительность и управление виртуальной сетью	199
Измерение ресурсов	199
Выводы	202
 Глава 8. Сетевые возможности.	 203
IPAM	205
Установка IPAM.. . . .	207
Настройка IPAM.	208
Использование IPAM.. . . .	213

Объединение сетевых карт	227
Качество обслуживания	231
Групповые политики QoS.	232
Расширяемый управляемый коммутатор Hyper-V	233
Настройка частных виртуальных локальных сетей.. . . .	234
Выводы	237
 Глава 9. Удаленный доступ	 239
Унифицированный удаленный доступ	240
Требования	242
DirectAccess.. . . .	242
Развертывание DirectAccess	243
Настройка DirectAccess	244
BranchCache	252
Требования	253
Развертывание BranchCache	254
Настройка брандмауэра Windows	257
Развертывание роли BranchCache с помощью диспетчера серверов.	258
Развертывание роли BranchCache с помощью PowerShell.	258
Подготовка и тестирование клиентских подключений	260
Инфраструктура виртуальных Рабочих столов	261
Службы удаленных Рабочих столов (RDS)	264
Установка служб удаленного Рабочего стола.	265
Управление службами удаленных Рабочих столов	270
Привязка приложений к коллекции и публикация удаленных приложений.	273
Добавление опубликованных приложений в веб-папку удаленного Рабочего стола	274
Подключение клиентов к удаленным приложениям	276
Установка RemoteFX	276
Выводы	278

Глава 10. Решение проблем, безопасность и мониторинг	279
Диспетчер серверов	280
Добавление сервера	281
Создание групп серверов	282
Значок оповещения	285
Анализатор соответствия рекомендациям	286
Windows PowerShell 3.0	287
Безопасность	292
BitLocker	294
Другие улучшения систем безопасности	296
Выводы	297
Об авторе	298

Предисловие

Об этой книге

Windows Server 2012 — это не только наиболее значительное обновление операционной системы Windows Server, выпущенное за последние годы. Это среда, где все нацелено на организацию облачных вычислений и на основную технологию для построения облачных сервисов — виртуализацию.

В Server 2012 многие функции, знакомые администраторам Server 2008 R2 и других версий Windows Server, были обновлены. Эта книга знакомит читателя с такими функциями и возможностями.

Читая книгу важно помнить о двух важнейших концепциях. Первая — возможности Server 2012 сосредоточены на развертывании, настройке и поддержке облачных платформ — частных, гибридных или общедоступных. Вторая — Server 2012 нацелена также на интеграцию мобильных устройств сотрудников в корпоративные сети.

Читательская аудитория

Вероятно, достаточно сказать, что эта книга подойдет любому, кто хочет узнать о новых возможностях Windows Server 2012. Она предполагает наличие

некоторого опыта в развертывании сетей на основе Windows или управлении ими. В частности, сетей, предусматривающих наличие учетных записей пользователей и наборов разрешений, служб Active Directory, DHCP (Dynamic Host Configuration Protocol — протокол динамического конфигурирования узла), DNS (Domain Name System — службы доменных имен) и других фундаментальных сетевых сервисов и концепций Windows. Любой — от новичка, до опытного системного администратора Windows — извлечет пользу из изучения примеров, приведенных в этой книге. Примеры демонстрируют тестовые инфраструктуры, характерные для малых и средних организаций.

Цели книги

Эта книга посвящена новым функциям и возможностям, благодаря которым Server 2012 можно назвать операционной системой, предназначенной для работы с облачными сервисами. Моя цель заключается в том, чтобы показать системным администраторам новые возможности с помощью примеров развертывания и настройки системы.

Среди тех возможностей, о которых вы узнаете, — новые способы управления виртуальными сетями и хранилищами данных, улучшенная технология унифицированного удаленного доступа (Unified Remote Access), улучшения в области хранения данных, достигнутые благодаря использованию новой файловой системы. Именно они позволяют Server 2012 пребывать на пике технологического прогресса. Пошаговые инструкции, снабженные копиями экранов, проведут вас через развертывание системы и настройку ее возможностей. Все копии экранов и описания основаны на реальных примерах развертывания и настройки системы в тестовой среде и на документации из Microsoft TechNet.

Структура книги

Главы 1 и 2 содержат общий обзор Windows Server 2012. Они посвящены особенностям различных редакций продукта, лицензированию, описанию аппаратных требований и процесса установки.

Последующие главы посвящены отдельным возможностям системы.

В главах 3 и 4 рассмотрены новый подход к управлению Windows Server и новые возможности Active Directory.

Глава 5 посвящена системе Dynamic Access Control (динамический контроль доступа) и содержит примеры ее развертывания.

В главах 6 и 7 подробно рассматриваются улучшения технологий организации хранилищ данных, кластеризации и Hyper-V, а также особенности настройки этих функций.

Глава 8 посвящена новым сетевым возможностям и содержит описание особенностей их развертывания.

Глава 9 посвящена технологии унифицированного удаленного доступа (Unified Remote Access).

В главе 10 исследованы новые способы решения проблем в работе Windows Server 2012, здесь же приводятся дополнительные сведения об управлении системой.

Правовые вопросы

Эта книга призвана помочь вам в работе. В большинстве случаев вы можете использовать программный код, который найдете здесь, в ваших программах и документации. Разрешение на использование кода не нужно, если только вы не собираетесь воспроизводить большие его фрагменты. А если вы продаете или распространяете CD-ROM-диски, содержащие примеры кода из книг издательства O'Reilly, разрешение понадобится. Если вы отвечаете на чьи-либо вопросы с использованием цитат из этой книги или фрагментов кода, разрешение также не нужно. А включение больших объемов кода, приведенного в примерах из книги, в документацию к вашему программному продукту требует получения разрешения.

Хотя мы и не требуем этого в обязательном порядке, мы очень ценим, если при цитировании вы вставите ссылку на первоисточник.

Если вы собираетесь использовать примеры кода в объемах, для которых требуется разрешение, свяжитесь с нами по адресу permissions@oreilly.com.

Благодарности

Большое спасибо Рейчел Роумелиотис (Rachel Roumeliotis) за ее терпение и помощь в написании этой книги. Спасибо редакторам издательства O'Reilly

и Рикку Вановеру (Rick Vanover) за то, что он поделился со мной знаниями. Благодарю за помощь и поддержку моих семью и друзей. Кроме того, хочется поблагодарить Мэри Джо Фоли (Mary Jo Foley) за вдохновение, которое она дала мне и другим людям, пишущим о технологиях, особенно женщинам.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу электронной почты comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства <http://www.piter.com> вы найдете подробную информацию о наших книгах.

1

Обзор Windows Server 2012

Введение в Windows Server 2012

Цель этой книги заключается в том, чтобы познакомить системных администраторов и всех тех, кому предстоит работать с Windows Server 2012, с основными новыми возможностями и улучшениями этой платформы, с тем, как добиться от них максимальной эффективности. Для начала мне хочется предложить небольшой рассказ о том, что лежит в основе эволюции этой новейшей серверной операционной системы от Microsoft.

Microsoft представила Windows Server 2012 через три года после выхода Windows Server 2008 R2. Server 2012 можно считать наиболее значительным обновлением серверной операционной системы от Microsoft с тех пор, когда Windows Server NT 3.51 был обновлен до NT 4.0 и был представлен современный графический интерфейс к Windows Server.

Server 2012 — это столь же значительный шаг вперед, так как, вероятно, это первый выпуск Windows Server, который построен с учетом нужд и ожиданий конечных потребителей, а не только потребностей организаций.

Server 2012 создан в расчете на совместимость с тремя основными тенденциями компьютерного мира и на поддержку этих тенденций. Популяризация каждой из них связана в основном с нуждами конечных пользователей. Это облачные вычисления, виртуализация и тенденция ориентирования информационных технологий (ИТ) на потребителя, или консьюмеризация ИТ, которая характеризуется растущим интересом к использованию сотрудниками компаний персональных вычислительных устройств, в частности мобильных, в обычной рабочей среде.

Microsoft спроектировала Server 2012 для удовлетворения этих трех требований рынка, добавив в эту операционную систему (ОС) некоторые обновления и усовершенствования. Возможности, касающиеся виртуализации и облачных вычислений, поддерживаются благодаря новым технологиям виртуализации, реализованным в Hype-V 3.0. Появились также возможности подключения центров обработки данных к общедоступным облачным сервисам и возможности, которые позволяют системным администраторам создавать гибридные и мультиарендные частные облачные сервисы. Аппаратное обеспечение серверов, хранилищ данных и компьютерных сетей может быть виртуализовано, таким образом, уменьшается стоимость электроэнергии, потребляемой оборудованием, централизуется администрирование, появляется возможность быстрого и эффективного масштабирования при расширении инфраструктуры.

Консьюмеризация ИТ — это тенденция, которая в последние годы привлекает к себе особое внимание. Персональные высокотехнологичные устройства становятся все более сложными и распространенными, люди все чаще хотят использовать эти устройства в офисах. Информационные технологии должны позволить соблюсти тонкий баланс между сохранением контроля над бизнес-сетями, к которым подключаются подобные устройства, и предоставлением пользователям полноценной рабочей среды.

Server 2012 предлагает возможности соблюдения этого баланса благодаря улучшениям службы удаленных рабочих столов (Remote Desktop Services, RDS) и технологии инфраструктуры виртуальных рабочих столов (Virtual Desktop Infrastructure, VDI). Microsoft внесла в VDI улучшения, которые касаются работы с глобальными сетями, так что теперь надежность работы с приложениями с помощью технологии удаленного рабочего стола сопоставима с возможностями, которые ранее были характерны лишь для подключения к приложениям и сетевым ресурсам в локальных сетях. Управление службами удаленных рабочих столов и удаленными клиентами теперь централизовано благодаря обновленному средству управления сервером (Server Manager). В интерфейсе этого средства объединены все основные

инструменты, необходимые системному администратору для управления инфраструктурой Windows.

Улучшения в области безопасности касаются персональных устройств пользователей и ориентированы на предотвращение утечек данных, строгий контроль доступа и соответствие нормативным требованиям, таким как закон Сарбейнза—Оксли (Sarbanes—Oxley, SOX) и закон «О перемещаемости и подотчетности страхования здоровья» (Health Insurance Portability and Accountability, HIPAA). В целом эти улучшения касаются системы динамического контроля доступа (Dynamic Access Control, DAC). Благодаря этой системе осуществляется управление безопасностью данных в организации непрерывно и на определенных интервалах.

Server 2012 не только отвечает потребностям меняющихся технологий, применяемых при организации рабочих мест пользователей, но и предлагает новые возможности и улучшения доступных ранее функций. Существует множество новых функций и улучшений, некоторые из них находятся «под капотом» системы и не бросаются в глаза.

Новые возможности и улучшенные функции

Вот краткий обзор некоторых из этих новых возможностей и улучшений.

Установка и интерфейс

Установка Server 2012 не отличается от Server 2008 R2. Как и ранее, существует два основных варианта установки Server 2012: в виде основных серверных служб (Server Core) и графического пользовательского интерфейса (Server GUI).

Установка основных компонентов сервера, *Server Core*, применяется по умолчанию, благодаря этому уменьшается потребление системных ресурсов, которые необходимы для установки графического пользовательского интерфейса, что оптимизирует производительность сервера. При установке в варианте Server Core уменьшаются объем необходимого дискового пространства, требования к обслуживанию, а также уязвимость сервера к атакам.

Установка сервера с графическим пользовательским интерфейсом, *Server GUI*, — это другое название полной установки (Full Installation) из Server 2008 R2.

При этом варианте установки выполняется загрузка полного интерфейса Server 2012, в том числе интерфейса в стиле Windows 8 Modern UI, а также всех средств для управления сервером, имеющих графический интерфейс.

Появился и новый функционал — возможность переключения между вариантами установки. Например, вы можете установить сервер с графическим интерфейсом и использовать соответствующие инструменты для его настройки, а затем переключиться на вариант установки основных компонентов и получить все преимущества повышенного уровня безопасности и экономного потребления ресурсов.

Такая возможность переключения создает дополнительный промежуточный вариант установки, который называется минимальным интерфейсом сервера (*Minimal Server Interface*). Получить данный вариант интерфейса можно установив сервер с графическим интерфейсом, а затем переключившись на вариант установки основных компонентов. При использовании минимального интерфейса сервера доступны консоль управления Microsoft (Microsoft Management Console, MMC), диспетчер серверов (Server Manager) и набор средств из панели управления (Control Panel).

Какой бы вариант установки не был выбран, можно удалить файлы, связанные с возможностями и серверными ролями, которые вам не нужны, благодаря новому функционалу — подключению функций по требованию (*Features on Demand*). Выбор функций для установки позволяет сэкономить дисковое пространство и понизить уязвимость сервера к атакам после установки сервера с графическим интерфейсом.

Новый графический интерфейс, загружаемый после выбора соответствующего варианта установки, основан на плитках, используемых в Windows 8-клиентах. Вы можете использовать этот интерфейс для выполнения обычных административных задач, таких как поиск и запуск инструментов управления сервером, создание ярлыков для часто используемых программ, запуск программ с повышенным уровнем разрешений. Программы наподобие Internet Explorer, оформленные в стиле Windows 8, в работе весьма похожи на мобильные приложения. Вместо того чтобы закрываться после использования, они переходят в фоновый режим, становясь неактивными.

Управление

Диспетчер серверов (Server Manager), который впервые был представлен в Windows Server 2008, позволяет управлять серверами, основываясь на их

ролях, таких как службы каталогов Active Directory (Active Directory Domain Services), служба доменных имен (Domain Name System, DNS) и протокол динамического конфигурирования узлов (Dynamic Host Configuration Protocol, DHCP). В Server 2012 интерфейс диспетчера серверов основан на современном подходе с использованием плиток. В дополнение к управлению локальным сервером диспетчер серверов теперь поддерживает управление множеством серверов.

С помощью обновленного диспетчера серверов можно выполнить большую часть административных задач, в том числе удаленное развертывание функций и ролей на физических и виртуальных серверах.

Диспетчер серверов теперь включает в себя и другие инструменты управления, такие как управление службами RDS, IPAM (IP Address Management, система управления IP-адресами), Нурег-V, файлами и хранилищами данных. Администраторы могут использовать расширенную панель мониторинга диспетчера серверов в качестве центральной точки доступа к большинству инструментов управления сервером.

Active Directory (AD) также играет ключевую роль в управлении Windows-окружением, улучшения были внесены и в службы каталогов Active Directory. Возможность работы с командой `dsprompto`, которая использовалась для добавления контроллеров домена, теперь является частью панели мониторинга диспетчера сервера. Мастером установки Active Directory, построенным на основе PowerShell, предельно просто пользоваться благодаря автоматическим проверкам и встроенным алгоритмам решения проблем, которые могут возникнуть при установке. Все это теперь части процесса установки. Кроме того, установку AD можно запустить удаленно с помощью RSAT (Remote Server Administration Tools, средства удаленного администрирования сервера), установленного на Windows 8-клиенте.

Благодаря технологии динамического контроля доступа (Dynamic Access Control) возросли безопасность системы и возможности управления. Вы можете маркировать файлы и применять политики безопасности, основываясь на классификации файлов. Например, файлы могут иметь метку *Human Resources only* (Только для сотрудников), политики безопасности могут быть установлены на обеспечение доступа только для членов группы Human Resources. Новая возможность поддержки утверждений в списках контроля доступа (например, «пользователь является членом <этой группы> И/ИЛИ <той группы>») дает возможность выборочного управления контролем доступа.

Кроме того, централизованные политики доступа и определения на основе утверждений помогают управлять безопасностью и выполнять аутентификацию пользователей в масштабах организации. Механизм помощи при ошибке «Отказано в доступе» позволяет администраторам оперативно принимать меры, когда с такой ошибкой сталкиваются пользователи при попытках обращения к файлам или папкам. Он позволяет, если нужно, мгновенно предоставлять им доступ к нужным материалам. Классификация файлов и папок «Только для внутреннего использования», или «Конфиденциально», выполняется с помощью диспетчера ресурсов файловой системы (File System Resource Manager).

Знакомый всем инструмент CHKDSK, который используется для проверки жестких дисков, расширен. Microsoft заявляет, что CHKDSK может проверить 300 млн файлов за 8 секунд, в то время как диск продолжает работать и остается доступным для других приложений.

Windows Power Shell 3.0

Microsoft рекомендует системным администраторам выполнять множество задач по управлению сервером с использованием расширенных PowerShell-сценариев Server 2012. В прошлом использование PowerShell требовало изучения командлетов (cmdlets) и синтаксиса, необходимого для управления окружением Windows. В итоге многие системные администраторы просто пользуются инструментами управления с графическим интерфейсом.

PowerShell 3.0 облегчает освоение возможностей управления системой несколькими способами. Во-первых, PowerShell использует упрощенный синтаксис языка, близкий к естественному. Кроме того, улучшенная работа с командлетами и автоматическая загрузка модулей делают поиск и запуск командлетов простыми, как никогда ранее. Интегрированная среда сценариев Windows PowerShell (Windows PowerShell Integrated Scripting Environment, ISE) 3.0 помогает начинающим пользователям PowerShell осваивать сценарии и предоставляет дополнительную поддержку.



Поставка Server 2012 включает в себя более 140 новых командлетов PowerShell, предназначенных для управления сетевыми возможностями и Hyper-V.

Хранилища данных

ReFS (Resilient File System, отказоустойчивая файловая система) — это новая локальная файловая система, впервые представленная в Server 2012. ReFS спроектирована для работы с хранилищами данных большой емкости — вплоть до петабайтов. ReFS предназначена для использования вместе с технологией пространств данных (Storage Spaces), о которой читайте в дальнейшем. С помощью ReFS зеркалированное пространство данных может обнаруживать повреждения данных и автоматически восстанавливать их.

Пространства данных (Storage Spaces) — это возможность, которая позволяет виртуализировать хранилища данных в Server 2012. При использовании данной технологии создаются пулы хранилищ данных и пространство для хранения файлов выделяется из пула хранилища. Для Windows это пространство выглядит как виртуальный диск. Поскольку данное хранилище виртуализовано, организациям не нужно использовать дополнительное аппаратное обеспечение для организации хранилища, в итоге использование данной возможности означает экономию и гибкость при возникновении необходимости расширения хранилищ.

Дедупликация данных (data deduplication) — это автоматический поиск и удаление дублирующейся информации, в частности, при создании резервных копий данных. Это неотъемлемое свойство Server 2012. Данная технология позволяет использовать меньшее количество дискового пространства для хранения большего количества данных. Управлять файлами и хранилищами данных можно с помощью средства диспетчера серверов, называемого файловыми службами и службами хранилища (File and Storage Services), и с помощью службы хранилищ (Storage Service). И то и другое доступно в диспетчере серверов, но данные средства можно запустить и настроить также с помощью PowerShell.

Удаленный доступ

В Server 2012 расширены возможности удаленного доступа, они спроектированы для обеспечения *унифицированного удаленного доступа (Unified Remote Access)*. Эта концепция реализует управление удаленным доступом к рабочим местам всей организации с единственной консоли диспетчера серверов.

Механизм унифицированного удаленного доступа предусматривает две улучшенные возможности: DirectAccess и BranchCache. DirectAccess позволяет пользователям прозрачно подключаться к корпоративным ресурсам. В Server 2012 по сравнению с Server 2008 R2 развертывание этой возможности

улучшено. BranchCache позволяет хранить данные в удаленных офисах (филиалах (branch) основной организации), в Server 2012 удаленный доступ к таким данным выполняется более эффективно.

В дополнение к управлению удаленным доступом с помощью графического интерфейса диспетчера серверов Server 2012 позволяет пользователю настраивать удаленный доступ с помощью команд PowerShell.

Со стороны клиента удаленный рабочий стол теперь оснащен интерфейсом в стиле Windows 8 — с плитками и возможностями операционной системы, сближающими ее с мобильными ОС. Кроме того, удаленные клиенты могут работать с мультимедийными данными с помощью расширенной технологии RemoteFX, которая позволяет им использовать 3D-графику и систему VoIP (Voice over IP, система телефонии, использующей сети передачи данных).

Сетевое взаимодействие

Новое и весьма значительное улучшение сетевых функций Server 2012 заключается в поддержке объединения сетевых карт (NIC, network interface card). Это позволяет объединить несколько сетевых карт в одно логическое устройство. Объединение сетевых карт обеспечивает отказоустойчивость сетевых соединений, или агрегирование пропускной способности, увеличение скорости передачи данных по сети. До Server 2012 объединение сетевых карт было доступно в серверных ОС семейства Windows только благодаря продуктам сторонних разработчиков и только при наличии подходящего аппаратного обеспечения. Теперь же объединение сетевых карт является собственной возможностью Server 2012 и Hyper-V 3.0.

Система управления IP-адресами (IPAM) — это еще одна новая сетевая возможность. С помощью IPAM сетевые администраторы могут обнаруживать IP-адреса, импортировать информацию об IP-адресах в электронные таблицы с целью управления активами, контролировать DHCP и DNS, отслеживать изменения IP-адресов (а также контролировать наличие подозрительных адресов) и т. д.

Расширения безопасности системы доменных имен (Domain Name System Security Extensions, DNSSEC) помогают обезопасить DNS-трафик. В Server 2012 упрощены установка DNSSEC и ее интеграция с Active Directory.

Некоторые сетевые функции были улучшены и в Hyper-V — технологии виртуализации Server 2012. В частности, улучшены системы QoS (Quality of Service, качество обслуживания) и мониторинга сети.

Hyper-V 3.0

В платформе виртуализации Server 2012, Hyper-V, можно найти множество новых возможностей и улучшений. Платформа Hyper-V улучшена настолько значительно, что эксперты по технологиям говорят о том, что возможности виртуализации платформы от Microsoft теперь на таком уровне, который позволяет им конкурировать с такими средами виртуализации, как Citrix и VMware.

Поскольку Hyper-V включает в себя множество новых возможностей и улучшений, легче всего рассказать о них, разбив их на категории.

Улучшения, касающиеся мультиарендности и технологии изоляции

- Частные виртуальные локальные сети (Private virtual local area networks, PVLANs), которые позволяют добиться изоляции между двумя виртуальными машинами, работающими в одной и той же локальной сети.
- Списки контроля доступа для виртуальных портов (Virtual port access control lists, port ACLs) предоставляют средство для управления сетевым трафиком, поступающим в виртуальные машины, на основе IP- и MAC-адресов.
- Расширяемый виртуальный коммутатор Hyper-V позволяет сторонним разработчикам создавать программное обеспечение, которое расширяет возможности управления Hyper-V. В частности, среди подобных приложений могут быть средства для мониторинга сетевого трафика, фильтры брандмауэров и приложения для обнаружения сетевых вторжений.



Мультиарендность (multitenancy) — это ситуация, при которой организация поддерживает несколько различных виртуальных инфраструктур в одном физическом окружении. У компаний, которые поддерживают службы для множества клиентов на одной и той же платформе, имеются мультиарендные среды. Данные одних клиентов отделены от данных других клиентов даже в том случае, если они хранятся на одном и том же физическом носителе. Изоляция данных подразумевает, что управлять ими может тот, у кого имеется доступ к конкретным виртуализированным ресурсам.

Гибкость и масштабируемость

- Расширенная динамическая миграция подразумевает возможность переноса работающей виртуальной машины между двумя узлами без простоя машины.
- С помощью нового мастера импорта администратор может импортировать виртуальные машины с одного узла на другой. Вдобавок мастер импорта позволяет обнаруживать и исправлять ошибки.
- Динамическое объединение позволяет выполнять слияние моментальных снимков машины с работающей виртуальной машиной.

Производительность

- Измерение ресурсов позволяет отслеживать уровень использования виртуальной машиной ресурсов центрального процессора, оперативной памяти, хранилища данных и сети.
- Использование формата виртуальных жестких дисков (Virtual Hard Disk Format, VHDX) позволяет увеличить производительность дисков с большими размерами секторов. VHDX поддерживает хранилища данных объемом до 16 Тбайт, имеет механизмы для защиты данных от повреждения и обеспечения высокого уровня производительности.
- Поддержка секторов виртуальных жестких дисков размером 4 Кбайт — это новая возможность, касающаяся поддержки больших дисковых секторов, идущая в ногу с инновациями в области систем хранения данных. Индустрия хранения данных переводит физический формат жестких дисков с 512-байтных секторов на 4096-байтные (также известные как 4К или 4KB-сектора). Этот переход обусловлен несколькими причинами, в том числе увеличением плотности и надежности хранения данных.

Однако основная масса программного обеспечения создана в расчете на 512-байтные сектора жестких дисков. Изменение размера сектора приводит к проблемам совместимости с многими приложениями. Производители систем хранения данных представили жесткие диски с секторами по 4 Кбайт для поддержки увеличивающейся емкости накопителей.

- Технология QoS (Quality of Service, качество обслуживания) для обеспечения минимальной заданной полосы пропускания — это новая функция, которая позволяет назначать виртуальным машинам и сервисам некий гарантированно доступный уровень полосы пропускания

и приоритет. Технология QoS важна, так как она дает администраторам возможность задавать, какой именно виртуальной машине нужно предоставить приоритетный доступ к полосе пропускания, и предоставляет средства, которые позволяют прогнозировать уровень пропускной способности сети. Для организаций, которые поддерживают службы клиентов, QoS позволяет придерживаться заключенных с клиентами соглашений об уровне обслуживания (SLA, service-level agreement), которые гарантируют клиентам некую минимально доступную полосу пропускания для доступа к службам.

Высокая доступность

- Теперь Hyper-V поддерживает инкрементное резервное копирование виртуальных жестких дисков, которое не прерывает функционирования виртуальной машины.
- Улучшенная кластеризация Hyper-V предоставляет защиту от сбоев приложений и служб, а также от системных сбоев и неполадок с аппаратным обеспечением.

Хранилище данных

- Неограниченная динамическая миграция хранилищ дает пользователям возможность выполнять множественные одновременные динамические миграции. Кластеризованное окружение может использовать высокие уровни пропускной способности сети (до 10 Гбайт).
- Поддержку общих томов кластера (Cluster Shared Volumes, CSV) можно интегрировать с дисковым массивом для целей репликации и создания мгновенных аппаратных снимков.
- Виртуальный адаптер Fibre Channel (Virtual Fibre Channel) позволяет подключать виртуальные операционные системы к дисковым массивам, интегрируя виртуальные машины с сетями хранения данных (SAN, Storage Array Networks).

Посредством PowerShell вы можете выполнять множество задач по администрированию и управлению Hyper-V. Существуют и команды PowerShell, предназначенные для настройки хранилищ данных и сетей и управления ими, как для виртуальных машин, так и для узлов внутри Hyper-V.

В дополнение к этим новым возможностям и улучшениям узлы Hyper-V теперь поддерживают до 320 логических процессов и до 4 Тбайт оперативной памяти. Виртуальные машины поддерживают до 64 виртуальных процессоров и до 1 Тбайт оперативной памяти.

IIS 8

Server 2012 представляет новую службу Internet Information Service 8 (IIS, набор служб для организации веб-серверов) и ASP.NET 4.5. Новые функции в IIS включают более совершенную систему безопасности: IIS защищает веб-сайты от внешних угроз, таких как веб- и FTP-атаки методом грубой силы, и предлагает защиту от DoS-атак (denial of service, отказ в обслуживании).

Теперь IIS может более эффективно использовать большее число процессорных ядер, не отставая от улучшений в серверном аппаратном обеспечении. Поддержка централизованных SSL-сертификатов (Secure Socket Layer, уровень защищенных соединений) позволяет хранить SSL-сертификаты в едином хранилище и автоматически связывать их с веб-приложениями. Регулирование нагрузки IIS на процессор (IIS CPU Throttling) — это новая функция, которую администраторы могут использовать для увеличения процессорного времени, выделенного веб-приложению для наращивания производительности, если в этом есть необходимость. Эту технологию можно использовать и для уменьшения доступного процессорного времени, когда использование приложения возвращается к нормальному уровню.

Безопасность

Безопасность системы обеспечивается кроме прочего теми новыми возможностями, которые мы уже рассмотрели. Среди них технология Dynamic Access Control (динамический контроль доступа), которая позволяет управлять данными, аутентификацией, верификацией и проверкой подлинности пользователей в организации. Внутренние системы безопасности Hyper-V позволяют изолировать виртуализированные сети в мультиарендных окружениях.

IIS 8 имеет также встроенные механизмы безопасности, такие как ограничения на FTP-подключения, которые позволяют предотвращать атаки методом грубой силы, направленные на FTP-серверы.

В дополнение к механизмам безопасности, уже доступным в составе описанных ранее возможностей, существует и технология *BitLocker* (шифрование дисков), представленная еще в Windows Vista и обновленная в Server 2012. Механизм шифрования BitLocker можно включить и на сервере, и на Windows 8-клиенте. Для обеспечения дополнительного уровня безопасности служба BitLocker может быть развернута на компьютерах, которые поддерживают работу с доверенным платформенным модулем (Trusted Platform

Module, TPM) — доступным на новых компьютерах аппаратным устройством, которое помогает защитить данные пользователей и предотвратить фальсифицированные подключения от имени пользователя, когда его компьютер отключен от сети.

В Server 2012 (и в клиентской системе Windows 8) в технологию BitLocker внесены некоторые улучшения. И сервер, и клиент теперь поддерживают установку в зашифрованном виде.

Теперь BitLocker предоставляет два варианта шифрования: Full Volume Encryption (полное шифрование тома) и Used Disk Space Only (шифрование только занятого пространства диска). Во втором случае на целевом томе шифруются только занятые блоки, что ускоряет процесс.

Пароли BitLocker к зашифрованным томам дисков, хранящих данные, можно менять так же, как и PIN-коды и пароли на клиентских системах.

В доверенной проводной сети систему BitLocker можно настроить на автоматическую разблокировку тома операционной системы при загрузке.

И наконец, Server 2012 включает в себя поддержку BitLocker для Windows Failover Cluster Shared Volumes (общих томов отказоустойчивых кластеров Windows) на Windows Server с включенной функцией отказоустойчивого кластера Windows (Windows Failover Cluster).

Кластеризация

Кластеризация (clustering) — это объединение отдельных серверов таким образом, что они могут действовать как единая система. Этот подход позволяет добиться высокой доступности услуг в том случае, если один из серверов окажется неработоспособным. В Server 2012 были внесены улучшения, которые касаются кластеризации физических и виртуальных серверов.

Отказоустойчивый кластер теперь поддерживает до 64 узлов. Улучшения, коснувшиеся мастера проверки конфигурации кластера (Validation Wizard) и мастера миграции в отказоустойчивом кластере, упрощают настройку кластеризованных файловых серверов и миграцию существующих серверов в новые кластеры.

В Hyper-V 3.0 отказоустойчивая кластеризация поддерживает до 4000 виртуальных машин. Улучшенная возможность работы с общими томами кластеров (Cluster Shared Volumes) упрощает конфигурирование кластеризованных виртуальных машин и работу с ними.

Обновление отказоустойчивых кластеров с поддержкой доступности (Cluster-Aware Updating, CAU) — это серверная роль, позволяющая администраторам планировать автоматические обновления кластеризованных серверов, которые при выполнении обновления остаются доступными.

Аппаратные требования

Аппаратные требования для установки Server 2012 включают в себя 64-битный процессор с частотой минимум 1,4 ГГц, 512 Мбайт оперативной памяти и 32 Гбайт свободного дискового пространства.

Поддерживается обновление с Server 2008 R2.

Выводы

Практически каждый компонент или функция, присутствовавшие в Server 2008 R2, обновлены или расширены в Server 2012. Эти расширения вместе с новыми компонентами позволяют говорить о богатом наборе возможностей Server 2012. Основное количество этих новых и улучшенных возможностей работают на уровне операционной системы и не предусматривают взаимодействия с конечными пользователями. Они обычно разворачиваются в самых разных организациях, от малых до самых крупных.

В следующих главах вы найдете пошаговые руководства по развертыванию и конфигурированию новых и улучшенных компонентов Server 2012.

2 **Аппаратные требования Server 2012 и установка**

В этой главе вы узнаете о существующих редакциях Server 2012 и о том, какая из них подойдет вашей организации. В дополнение к этому вы ознакомитесь с аппаратными требованиями, предъявляемыми к оборудованию, на котором планируется устанавливать Server 2012, и с тем, что нужно для успешного развертывания Hyper-V.

Кроме того, эта глава раскрывает возможности обновления предыдущих серверных продуктов от Microsoft и содержит пошаговую демонстрацию различных вариантов установки: основных компонентов сервера (Server Core) и сервера с графическим интерфейсом (Server GUI). Вы найдете здесь и инструкции по переходу между различными вариантами установки Server 2012, а также пояснения, касающиеся того, зачем администраторам это нужно. Кроме того, здесь вы узнаете, как установить и сконфигурировать минимальный интерфейс сервера (Minimal Server Interface), ознакомитесь с настройкой возможностей сервера с использованием технологии подключения компонентов по требованию (Features on Demand).

Редакции Server 2012

Windows Server 2012 доступен в четырех редакциях, известных также как идентификаторы товарных позиций (SKU, stock keeping units). Как и в предыдущем выпуске, Server 2008 R2, все товарные позиции доступны лишь в 64-битном виде. Серверные ОС не предлагаются в 32-битных вариантах. Microsoft отошла от варианта Server 2008 R2 Enterprise в стремлении рационализировать управление версиями и лицензирование. Сегодня доступны следующие редакции продукта: Windows Server 2012 Datacenter, Windows Server 2012 Standard, Windows Server 2012 Essentials и Windows Server 2012 Foundation.

Естественно, стоимость каждой из редакций варьируется в зависимости от количества серверов, пользователей или устройств, прямо или косвенно взаимодействующих с сервером. Для каждого пользователя или устройства нужна отдельная клиентская лицензия (CAL, client access license).

Для того чтобы сориентировать вас в ценах, приведем приблизительную розничную стоимость каждой редакции и модель лицензирования:

- *Datacenter*. Процессор и CAL — \$4,809.
- *Standard*. Процессор и CAL — \$882.
- *Essentials*. Сервер и до 25 пользователей — \$425.
- *Foundation*. Сервер и до 15 пользователей — предлагается лишь для OEM-партнеров (производителей оборудования, original equipment manufacturer), то есть предустанавливается на серверы.

Server 2012 Datacenter

Редакция Datacenter обладает максимальным набором возможностей и предназначена для крупных организаций. Если работа в вашей организации серьезно зависит от виртуализации и облачных сервисов, редакция Datacenter — это наилучший выбор.

Обеспечение высокой доступности служб — ключевое преимущество данной редакции, так как вы можете выполнять *горячее добавление (hot-add)* и *горячую замену (hot-replace)* процессоров и памяти. В данном случае это означает возможность заменять и добавлять данные компоненты без необходимости выключения сервера.

Редакция Datacenter поддерживает неограниченное количество виртуальных машин (VM, virtual machines), выполняемых на одном-двух процессорах. Кроме того, данная редакция поддерживает неограниченные возможности обеспечения сетевых подключений и удаленного доступа. Количество соединений ограничено лишь доступной пропускной способностью сети и аппаратными особенностями устройств. На эту редакцию следует обратить внимание в том случае, если в вашей сети нужна виртуализация на уровне организации и вы нуждаетесь в высокой масштабируемости. Сервер, работающий под управлением данной редакции ОС, можно оперативно расширять для того, чтобы его возможности соответствовали нуждам организации при добавлении большого количества пользователей и ресурсов, таких как данные или устройства.

Пользователи редакции Datacenter обычно приобретают корпоративные лицензии (volume licenses). Кроме того, корпоративные лицензии можно приобрести, воспользовавшись программой поддержки корпоративных пользователей Microsoft Software Assurance. Стоимость лицензирования основывается на размерах организации и количестве персональных компьютеров и устройств, которые нужно подключить к серверу. Если в вашей организации планируется использовать много виртуальных машин, если ей нужна платформа, подходящая для развертывания облачных сервисов, и имеются сотни клиентских компьютеров, редакция Datacenter — это наилучший выбор.

Server 2012 Standard

Редакция Windows Server 2012 Standard предназначена для организаций среднего размера, не имеющих серьезных потребностей в виртуализации, в которых основная часть бизнес-приложений и систем запускается в местах их использования. Используя данную редакцию, организация получает аналогичные возможности с учетом ограничения на запуск максимум двух виртуальных машин на двух процессорах.

Server 2012 Essentials

Server 2012 Essentials — это редакция, которая подходит для небольших организаций (менее чем 25 ПК, устройств и/или пользователей). Эта редакция не предлагает возможностей Hyper-V, предоставляет ограниченную роль

сервера приложений и не поддерживает сервер службы обновления Windows (Windows Server Update Services, WSUS). Эту редакцию можно запускать на серверах, содержащих до двух процессоров.

Server 2012 Foundation

Данная редакция поставляется предустановленной на серверы, предназначенные для малого и среднего бизнеса (Small to midsize business, SMB). Она идеальна для небольших организаций, в которых не более 15 пользователей. Данная редакция не поддерживает такие технологии, как Hyper-V или WSUS. Она включает в себя файловые службы с ограниченными возможностями, сетевые политики, службы доступа и службы удаленных рабочих столов с ограничениями.

Если в вашей организации имеются серверные и клиентские лицензии для предыдущих версий Windows Server, некоторые из них можно применить при обновлении до Windows Server 2012. Обратитесь к списку вопросов и ответов Microsoft по лицензированию Windows Server 2012 (<http://www.microsoft.com/ru-ru/server-cloud/buy.aspx>), для того чтобы определить, какая именно модель лицензирования необходима вашей организации.

Аппаратные требования Server 2012

Server 2012 предъявляет специфические требования к аппаратному обеспечению независимо от редакции, которую вы собираетесь использовать. Минимальные системные требования выглядят следующим образом:

- 1,4 ГГц x64 процессор (поддерживается только 64-битная серверная архитектура);
- 512 Мбайт оперативной памяти;
- 32 Гбайт свободного дискового пространства;
- DVD-ROM-дисковод;
- монитор с разрешением Super VGA (800 600) или более высоким;
- клавиатура;
- мышь или совместимое устройство позиционирования.

Помните о том, что если вы устанавливаете Server 2012 на компьютер, имеющий более 12 Гбайт оперативной памяти, вам понадобится более 32 Гбайт свободного дискового пространства для организации работы файла подкачки, механизма гибернации и хранения дампов-файлов. Кроме того, понадобится больше памяти, если вы выполняете установку через сеть.

Также учтите, что эти минимальные требования приведены для системы без ролей, добавленных при установке. Для того чтобы достичь оптимальной производительности системы после установки, используйте самое лучшее из доступного вам аппаратного обеспечения. Если вы хотите улучшить какую-либо характеристику системы, работая в рамках ограниченного бюджета на аппаратное обеспечение, отдайте предпочтение наибольшему из возможных объему памяти. В настоящее время основное количество серверов, в особенности те, которые рассчитаны на малый или средний бизнес, поставляются с как минимум 2 Гбайт оперативной памяти.

Аппаратные требования для Hyper-V 3.0

Для того чтобы добавить в Server 2012 роль Hyper-V, система должна соответствовать некоторым дополнительным требованиям. Если вы планируете использовать Hyper-V, понадобится увеличить минимальные аппаратные требования.

В частности, для развертывания Hyper-V на Server 2012 нужно следующее:

- 64-битный процессор, поддерживающий технологии виртуализации AMD-V или Intel-VT;
- минимум 4 Гбайт оперативной памяти для запуска до четырех виртуальных машин. Обратите внимание на то, что эти требования к оперативной памяти отличаются от минимальных, необходимых для установки лишь Server 2012. Если вы планируете использовать пять или больше виртуальных машин, планируйте оснастить свой сервер большим количеством памяти.

Установка Server 2012

В этом разделе я приведу подробные инструкции по установке Server 2012 в двух предлагаемых конфигурациях: только основных серверных компонентов (Server Core) и конфигурации с графическим пользовательским

интерфейсом сервера (Server with a GUI). Microsoft рекомендует: прежде чем приступать к установке сервера в той или иной конфигурации, ознакомьтесь с некоторыми практическими указаниями. Им желательно следовать, хотя мой опыт подсказывает, что одна из обязательных задач, предшествующих установке сервера, заключается в выяснении любых возможных проблем с совместимостью драйверов и приложений, которые должны исполняться на сервере. Если у вас есть некие бизнес-приложения, жизненно важные для вашей организации, вам вряд ли захочется выполнять обновление до Server 2012 только для того, чтобы нарушить работу этих приложений. Такая установка совершенно бесполезна. Если на вашем сервере имеются драйверы и приложения, которые не совместимы с Server 2012, вы также можете столкнуться с проблемами после установки или обновления, даже если тщательно исполняете практические указания Microsoft.



Опытные системные администраторы выполняют обновление до новой версии серверного ПО или установку новой версии на тестовом сервере, не подключенном к рабочей среде. Поскольку бюджетные ограничения не всегда позволяют ИТ-подразделению приобретать резервные серверы, конфигурации которых идентичны рабочим, неплохо будет иметь более старый сервер, на котором можно развернуть Нурег-V для создания виртуальных машин. Таким образом вы можете протестировать установку Server 2012 или обновление до данной версии сервера, а затем установить любые приложения, важные для вашей организации, для того чтобы убедиться в том, что программное обеспечение нормально функционирует в новой среде.

Не только своевременно решить возможные проблемы с совместимостью, но и выполнить установку максимально быстро и эффективно вы сможете, если будете следовать приведенным далее практическим рекомендациям:

1. **Отключите источники бесперебойного питания** (uninterruptible power source, UPS, ИБП). Различные ИБП обычно подключают к компьютерам с помощью последовательного порта. Такое подключение может привести к проблемам с обнаружением оборудования при установке, поэтому перед установкой интерфейса передачи данных ИБП лучше отсоединить от компьютера.
2. **Сделайте резервную копию серверов.** Крайне важно перед установкой Server 2012 сделать резервную копию. В нее должны входить не только

данные, но и конфигурация сервера, и ключевые компоненты инфраструктуры, такие как DHCP. В дополнение вам может понадобиться создать резервную копию загрузочных и системных разделов и текущих данных состояния системы. Один из способов создания резервной копии конфигурационной информации заключается в создании резервного набора данных для системы ASR (Automated System Recovery, автоматическое восстановление системы).

3. **Отключите антивирусы и другое программное обеспечение для защиты от вредоносного ПО.** Такое программное обеспечение, работающее во время установки или обновления, может помешать и тому и другому.
4. **Если вы выполняете обновление с Windows Server 2008 R2, запустите диагностику памяти Windows (Windows Memory Diagnostics, WMD).** При обновлении протестируйте память на потенциальные проблемы с помощью средства WMD из состава средств администрирования Server 2008 R2.
5. **Заранее подготовьте драйверы для накопителей информации.** Иногда в ходе установки неожиданно обнаруживаются проблемы с распознаванием устройств, с которых вы пытаетесь выполнить установку, таких как DVD-дисководы или USB-диски. Для того чтобы предотвратить появление подобных проблем, если производитель устройства предоставляет драйверы, сохраните их либо в корневой директории носителя, либо (для систем, основанных на процессорах от AMD) в папке amd6. Чтобы в процессе установки предоставить системе эти драйверы, на странице выбора диска щелкните **Загрузить драйвер (Load Driver)** или нажмите **F6**. Вы можете самостоятельно указать системе нужный драйвер или позволить программе установки выполнить поиск на носителе.
6. **Настройте брандмауэр Windows.** После обновления или установки серверные приложения, которые должны принимать входящие соединения, могут не работать до тех пор, пока вы не создадите для них правила, разрешающие такие соединения. Узнайте, указал ли производитель программного обеспечения необходимые для его нормальной работы порты и протоколы.

Далее я приведу пошаговые процедуры выполнения установки Windows Server 2012 в конфигурациях установки основных компонентов и пользовательского интерфейса.



Существует лишь один способ обновления до Server 2012 с сохранением существующих данных и работоспособности установленного ПО. Он заключается в обновлении с Server 2008 R2. Вам как системному администратору следует убедиться в том, что программы, ранее установленные в системе с Server 2008 R2, работоспособны после обновления до Server 2012, то есть доступны и могут запускаться. Вы можете узнать, какое программное обеспечение сертифицировано или будет сертифицировано на совместимость с Windows Server 2012, обратившись к каталогу Microsoft (<http://www.windowsservercatalog.com/>). Обновление сервера, который работает под управлением других версий операционных систем от Microsoft, включая Server 2003 и Server 2008 (не R2), требует создания резервной копии всех данных, хранящихся на сервере, выполнения чистой установки Server 2012 и переустановки приложений.

Конфигурация установки основных компонентов сервера

Начинать работу с Server 2012 Microsoft рекомендует с варианта установки основных компонентов сервера — Server Core. Это так, потому что использование интерфейса Server Core уменьшает объем дискового пространства, необходимый для установки, и снижает риск потенциальных атак на сервер. Отсутствие графической оболочки означает меньшее число точек входа для различных угроз и вредоносного ПО. Если вы не нуждаетесь в дополнительных графических средствах управления и интерфейсе, которые соответствуют полному варианту установки, остановитесь на варианте Server Core, если вы полагаете, что готовы к работе с ним. Конечно, при установке сервера в данной конфигурации управление им реализуется посредством PowerShell. В Server 2012 с PowerShell легче работать, чем с аналогичным средством в предыдущих версиях системы. Это достигается благодаря более чем 2300 командам и расширенному интегрированному системному окружению (Integrated System Environment), которое позволяет легко находить команды, необходимые для тех или иных административных задач. Однако многим администраторам все еще требуется некоторое время на освоение PowerShell.

PowerShell в Server 2012 остается контекстно-зависимой. Если вы введете команду с ошибкой, даже если это будет лишний пробел, команда выполняться не будет. В итоге вам для того, чтобы все работало как нужно, нередко придется разбираться с сообщениями об ошибках.



То, что вы не слишком уверенно чувствуете себя в PowerShell при отсутствии графических средств управления сервером, — одна из причин выбора варианта установки системы с графическим интерфейсом.

Если вы не слишком хорошо умеете пользоваться PowerShell, некоторые серверные задачи гораздо легче выполнять с помощью графического интерфейса. Администрирование сервера обычно подразумевает своевременное выполнение ряда задач. И выполнение задач, которое подразумевает поиск и правильный ввод соответствующих команд PowerShell, отличается от подхода, при котором достаточно пары щелчков мышью в графическом интерфейсе сервера. В итоге многие администраторы выбирают последнее.

Однако не стоит пренебрегать изучением PowerShell для выполнения некоторых задач по администрированию сервера. У PowerShell есть преимущества по сравнению с графическим интерфейсом, когда дело касается автоматизации рутинных операций. Новая возможность PowerShell — сниплеты. Их синтаксис напоминает синтаксис обычных PowerShell-команд, и они позволяют серьезно экономить время на выполнении повседневных задач. Во многих компаниях требуются регулярные отчеты по безопасности, например о том, кто и с какими данными работал по сети. Для построения таких отчетов можно использовать PowerShell. С его помощью можно создать автоматически запускаемый сценарий, который регулярно будет получать списки контроля доступа (access control list, ACL) для файлов и папок, доступных в сети.

Хотя вы можете установить Server 2012 в двух вариантах, большой плюс этой ОС заключается в том, что сейчас как никогда легко использовать оба варианта установки для целей администрирования сервера. Одно из значительных преимуществ Server 2012 перед Server 2008 R2 заключается в возможности переключаться между вариантами установки. Для установки некоторых приложений требуется наличие графического интерфейса, поэтому такая гибкость удобна в тех случаях, когда без полного графического интерфейса сервера не обойтись. Далее в этой главе мы поговорим о преобразовании варианта установки сервера с основными компонентами в вариант с графическим интерфейсом.

В режиме с установкой основных компонентов задачи по управлению сервером выполняются либо с использованием командной строки Windows PowerShell, либо удаленно. Эти задачи включают в себя добавление, настройку и деинсталляцию серверных ролей, таких как DHCP.

По умолчанию в режиме с установкой основных компонентов сервера доступны следующие 13 серверных ролей.

- Active Directory Certificate Services (службы сертификатов Active Directory, AD CS). Выдают цифровые сертификаты с открытым ключом и позволяют управлять ими. Сертификаты обеспечивают повышенный уровень безопасности в сети, обеспечивая проверку подлинности пользователей, устройств или служб, привязанных к соответствующему закрытому ключу.
- Active Directory Domain Services (доменные службы Active Directory, AD DS). Это каталог, который предназначен для хранения данных, используемых при взаимодействии между пользователями и доменами, и управления этими данными. AD DS позволяет управлять учетными записями пользователей, аутентификацией и службами каталогов. AD DS — это одна из центральных служб Windows-сетей.
- Служба Dynamic Host Configuration Protocol (DHCP, служба протокола динамического конфигурирования узла). Динамически назначает IP-адреса устройствам, подключенным к сети.
- Служба Domain Name System (DNS, система доменных имен). Используется для установления соответствия между сетевыми адресами узлов и служб и IP-адресами и/или для разрешения имен интернет-узлов по IP-адресам.
- File Services (файловые службы). Позволяют централизованно управлять имеющимися в сети файлами и папками и доступом к ним. File Server Resource Manager (FSRM, диспетчер ресурсов файлового сервера) — это набор инструментов, устанавливаемый вместе с файловыми службами, который можно использовать для управления серверными ресурсами на локальных и удаленных серверах.
- Active Directory Lightweight Directory Services (AD LDS, службы Active Directory облегченного доступа к каталогам). AD LDS предоставляет службы каталогов практически так же, как и AD DS, но без необходимости развертывания доменов и контроллеров доменов.
- Hyper-V. Hyper-V 3.0 — это технология виртуализации, применяемая в Windows Server 2012.
- Print and Document Services (службы печати и документов). Позволяют организовывать совместное использование в сети принтеров и сканеров, предоставляют возможность централизованного управления

серверами печати и сетевыми принтерами. Кроме того, они позволяют организовывать перенос серверов печати и развертывать подключения с использованием групповой политики (Group Policy).

- Streaming Media Services (службы потокового мультимедиа). С помощью служб потокового мультимедиа сетевые клиенты могут принимать потоковое мультимедийное содержимое.
- Web Server (веб-сервер). Роль веб-сервера предусматривает установку IIS (Internet Information Services, набор служб для организации веб-серверов) 8.0. Веб-сервер предназначен для создания и размещения веб-сайтов и развертывания веб-приложений в организации.
- Windows Server Update Services (WSUS, сервер службы обновления Windows). Предоставляет централизованные инструменты для развертывания обновлений Windows на клиентских системах по сети.
- Active Directory Rights Management Server (AD RMS, сервер управления правами Active Directory). Это технология защиты данных, которая работает с поддерживаемыми ее приложениями, помогая защитить цифровые данные от несанкционированного использования. С помощью данной службы вы можете указать, кому разрешено открывать, изменять, распечатывать, пересылать информацию или выполнять другие действия с ней.
- Routing and Remote Access Server (RRAS, сервер маршрутизации и удаленного доступа). Обеспечивает удаленным пользователям доступ к сетевым ресурсам.

Установка в конфигурации Server Core не предусматривает наличия графической оболочки для Windows Server или Рабочего стола. Кроме того, данный вариант установки не содержит консоли управления Microsoft (MMC, Microsoft Management Console). Задачи управления сервером, которые выполняются с помощью MMC, можно реализовать посредством командной строки или PowerShell.

Конечно, то, что вы устанавливаете систему, содержащую лишь основные серверные компоненты, не означает, что в нее нельзя добавлять инструменты и средства управления. Благодаря новой возможности подключения компонентов по требованию (Features on Demand) вы можете добавлять и удалять компоненты и инструменты управления. Добавление и удаление функций будет рассмотрено далее в этой главе. Сейчас рассмотрим пошаговый пример установки Server 2012 в конфигурации Server Core.

Процедура установки сервера в конфигурации установки основных компонентов

После того как вы начнете установку с диска CD-ROM, DVD, USB-диска или запустите процедуру установки через сеть, начнет работать мастер установки. На первом экране вам предлагается выбрать параметры установки, такие как язык, формат отображения времени, раскладку клавиатуры или другие параметры устройств ввода (рис. 2.1).



Рис. 2.1. Параметры установки

После нажатия кнопки **Далее** (Next) будет показано окно, содержащее кнопку **Установить** (Install now), нажатие которой продолжит процесс установки (рис. 2.2).

Следующим шагом является выбор режима установки. Для варианта Server Core можно выбрать пункт **Ознакомительная версия Windows Server 2012 Data-center** (установка основных серверных компонентов) (Server Core Installation) или аналогичный пункт для редакции Standard (рис. 2.3) и нажать **Далее** (Next).



Рис. 2.2. Начало установки Server 2012

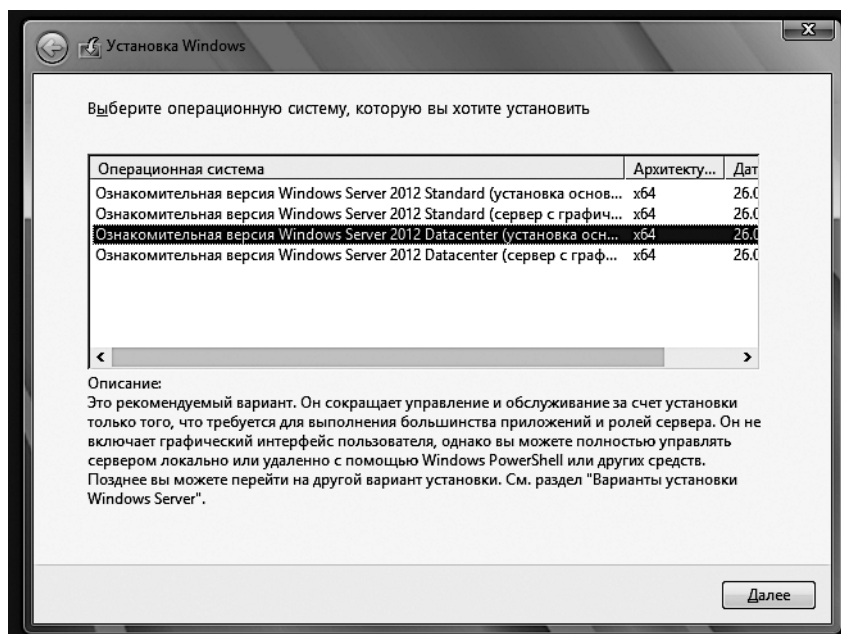


Рис. 2.3. Выбор режима установки сервера

Затем вам предложат принять условия лицензии. Установку нельзя продолжить до тех пор, пока вы не установите соответствующий флажок (рис. 2.4). Как только сделаете это, щелкните **Далее (Next)**.

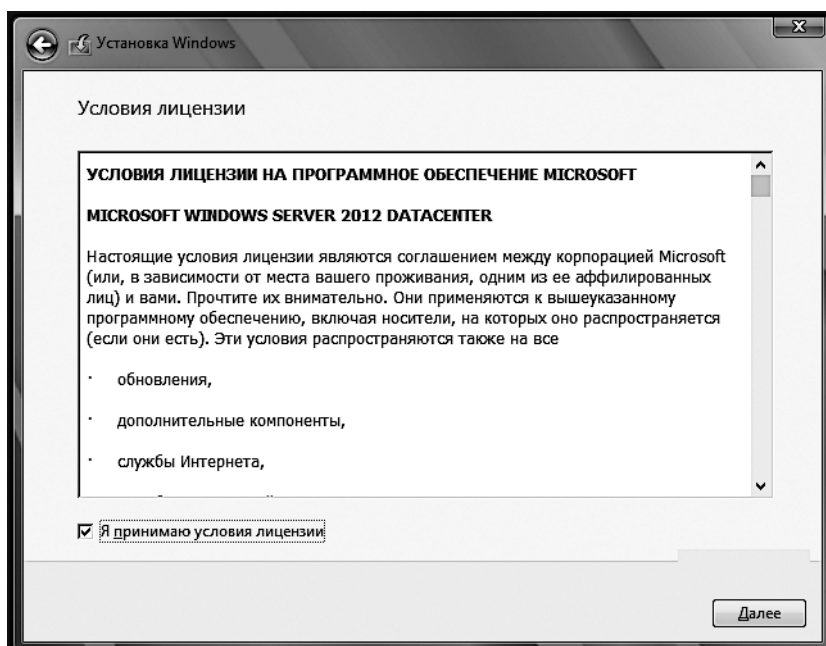


Рис. 2.4. Лицензионное соглашение

Затем у вас будет возможность либо начать чистую установку системы, либо выполнить обновление с Server 2008 R2 (рис. 2.5). Выберите вариант **Выборочная: только установка Windows (для опытных пользователей)** (Custom: Install Windows only (advanced)) для установки с нуля или **Обновление: установка Windows с сохранением файлов, параметров и приложений** (Upgrade: Install Windows and keep files, settings, and apps) для обновления.

Теперь вам нужно указать диск для установки системы и настроить его разбиение на разделы (рис. 2.6). Большинство администраторов создают системный раздел для установки серверной ОС. Вы, учитывая наличие свободного места, можете создать и другие разделы для того, чтобы затем использовать их в виде логических жестких дисков в зависимости от ваших потребностей в хранении данных.

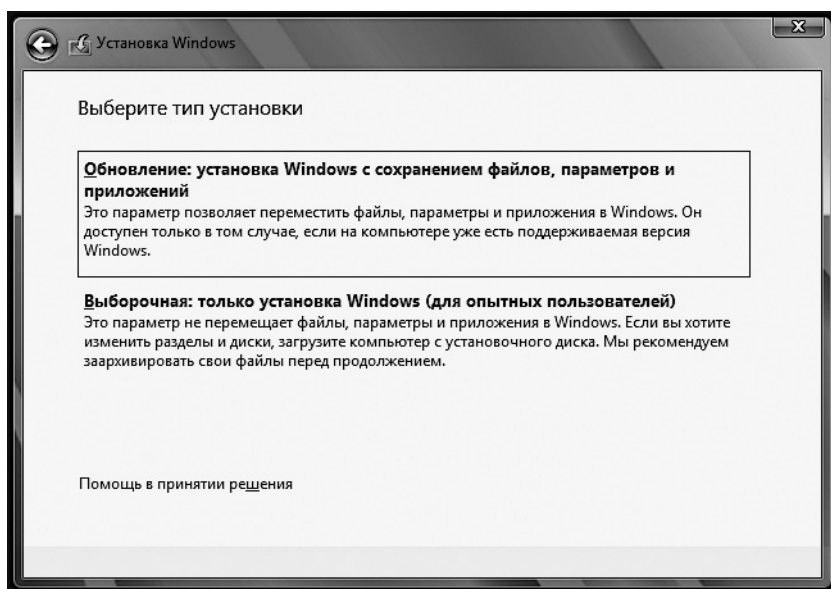


Рис. 2.5. Выбор типа установки

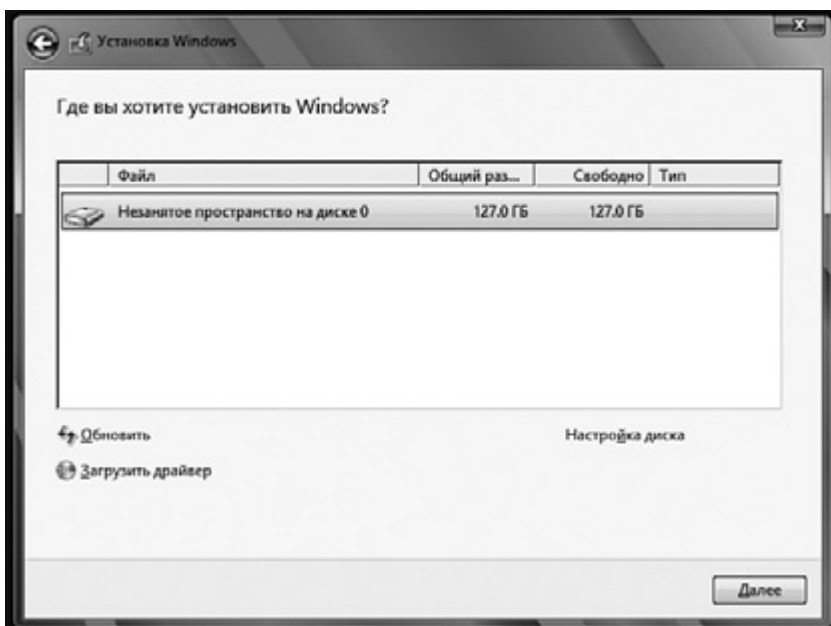


Рис. 2.6. Выбор раздела диска для установки системы

Я рекомендую устанавливать операционную систему, в данном случае Server 2012, в отдельный системный раздел и затем создавать разделы для хранения данных. Эти разделы и тома, содержащие серверные данные, обычно включают в регулярно выполняемые задачи резервного копирования. Таким образом, если сервер окажется поврежденным или его работоспособность будет нарушена, вы можете при необходимости переустановить операционную систему, а затем восстановить данные из резервной копии. Данная методика хорошо подходит как для небольших настольных серверов с одним-двумя жесткими дисками, так и для более крупных, монтируемых в стойку и содержащих до восьми жестких дисков. Настройки могут различаться в зависимости от наличия RAID-конфигураций (Redundant Array of Inexpensive Disks, избыточного массива недорогих дисков), но в любом случае лучше всего устанавливать операционную систему не в тот же раздел, где планируется хранить данные.

На данном этапе вы можете также загрузить драйверы сторонних производителей, которые могут понадобиться Windows 2012 для работы с подключенными к серверу устройствами.

Далее Windows копирует файлы сервера на жесткий диск, и на этом установка сервера в конфигурации установки основных серверных компонентов завершается. Следующий экран, который потребует вашего внимания, — это окно ввода пароля администратора (рис. 2.7). Здесь будет предложено ввести пароль для локальной учетной записи администратора.

Если раньше вы работали с Windows Server, то заметите, что интерфейс экрана входа в систему в Windows Server 2012 изменен. Одна из новых особенностей интерфейса заключается в наличии значка в виде глаза в поле ввода пароля (рис. 2.8). Если после ввода пароля щелкнуть на этом значке и удерживать кнопку мыши, в поле вместо звездочек будут показаны введенные символы.

После того как вы войдете в Server 2012, установленный в конфигурации Server Core, вы увидите окно командной строки сервера и больше ничего — ни значков на Рабочем столе, ни кнопки Пуск, ни Проводника Windows (рис. 2.9). Все задачи управления сервером нужно выполнять только с помощью командной строки.

Интерфейсные функции при установке основных компонентов сервера не отличаются разнообразием, однако здесь вы можете выполнить практически любую административную задачу из командной строки. Например, установить PowerShell, выполнив команду **sconfig** в командной строке (рис. 2.10). Из командной строки вы можете выполнять и другие административные задачи. Например, такие, как присоединение сервера к домену или рабочей группе, переименование сервера или конфигурирование сетевых параметров и др.

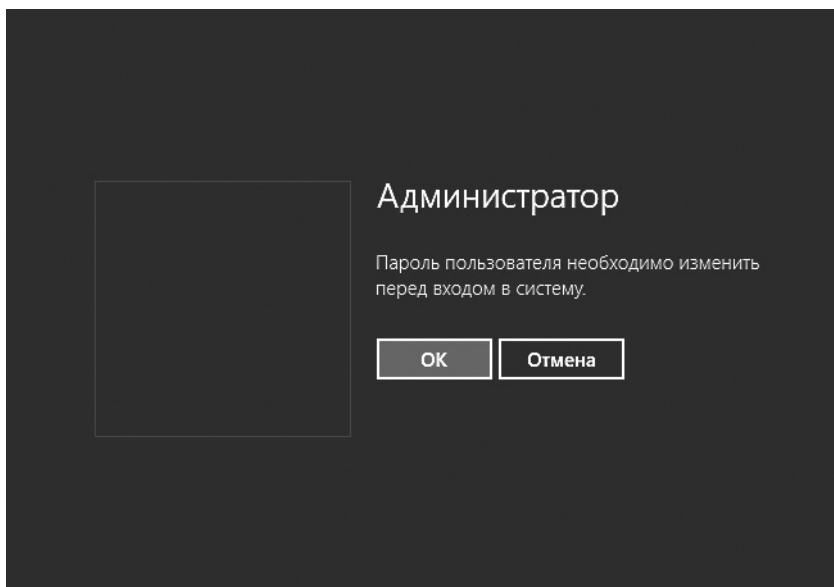


Рис. 2.7. Первый вход с локальной учетной записью администратора

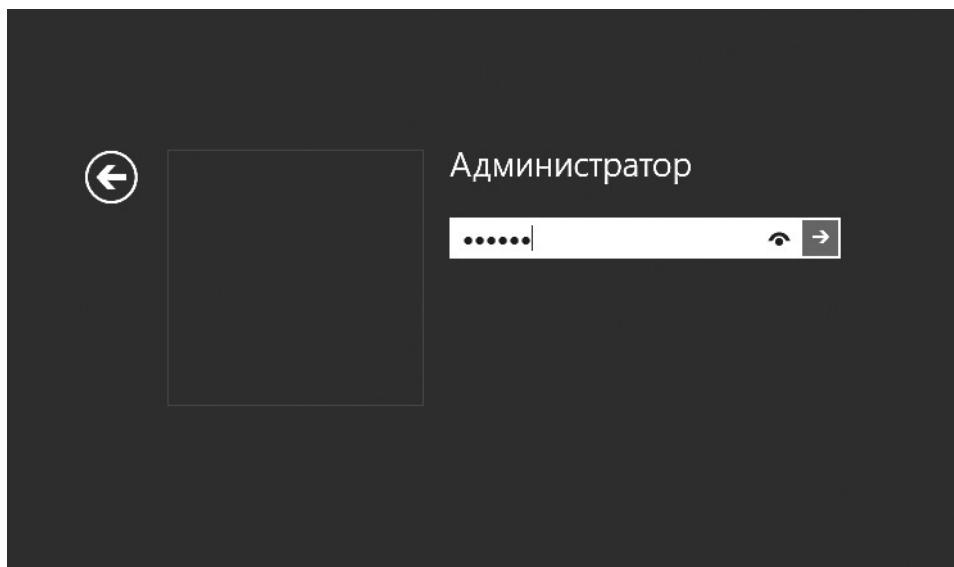
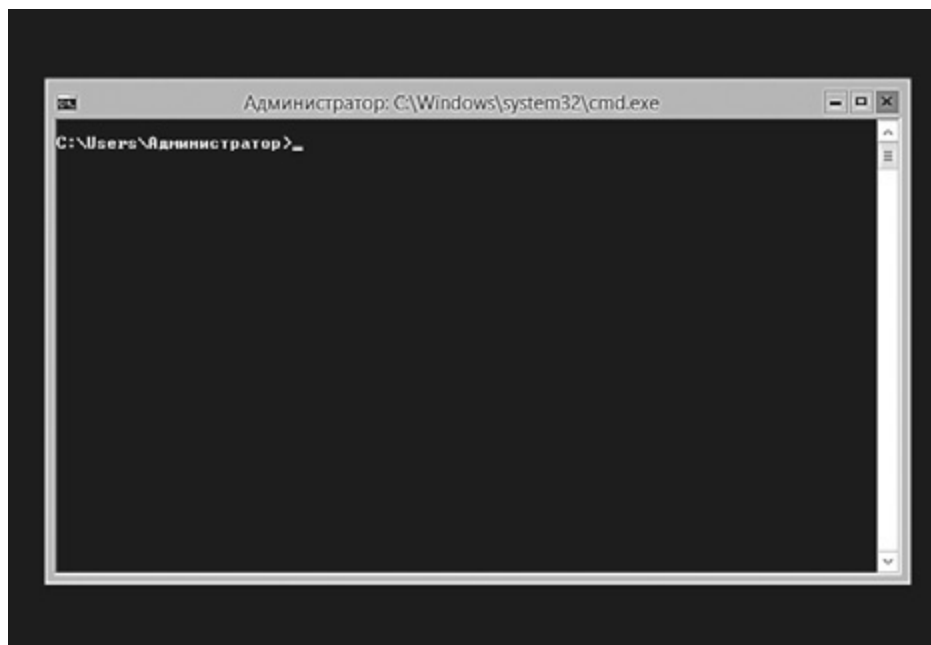
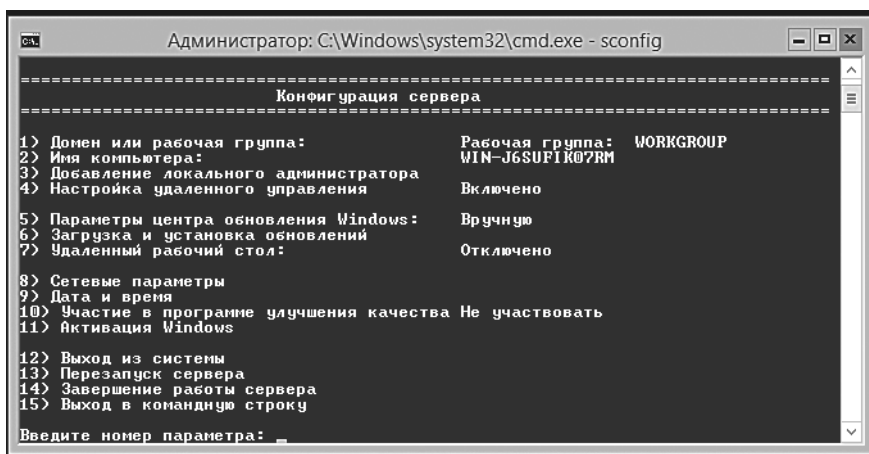


Рис. 2.8. Значок глаза позволяет отобразить вместо звездочек текст

**Рис. 2.9.** Интерфейс Server Core**Рис. 2.10.** Запуск утилиты Sconfig из командной строки

Установка сервера с графическим интерфейсом

Вариант установки сервера с графическим интерфейсом в Server 2012 аналогичен варианту Full Installation (Полная установка) в Server 2008 R2. При выборе данного варианта выполняется полная установка стандартного пользовательского интерфейса Windows Server и всех средств управления сервером.

В Server 2012 используется интерфейс, аналогичный интерфейсу Windows 8-клиентов. Однако по умолчанию поддержка приложений для Windows 8 отключена. Для того чтобы включить поддержку таких приложений, вам нужно установить компонент **Возможности рабочего стола (Desktop Experience)**. Данный компонент можно установить либо с помощью диспетчера серверов (Server Manager), либо с помощью PowerShell. Речь об этом пойдет в главе 3.

Сервер с графическим интерфейсом требует примерно на 4 Гбайт больше дискового пространства, чем сервер в варианте установки основных серверных компонентов. Как и в случае с установкой основных компонентов сервера, при установке сервера с графическим интерфейсом вы не привязаны к этому интерфейсу. Далее мы рассмотрим возможности преобразования вариантов установки.

Многим администраторам серверов удобнее управлять сервером с помощью полного графического интерфейса. Однако, как уже было сказано, преимущество использования PowerShell заключается в автоматизации рутинных административных задач. Если ваша сеть сравнительно невелика (менее 250 пользователей и устройств) и у вас нет значительного опыта работы с PowerShell, вы можете начать работу с Windows Server 2012, используя графический интерфейс. А позже при необходимости сможете изучить PowerShell и приступить к использованию этого инструмента.

Начальные шаги установки сервера с графическим интерфейсом пользователя похожи на процедуру установки сервера, содержащего лишь основные компоненты.

Процедура установки сервера с графическим интерфейсом

По всей вероятности, сервер с графическим пользовательским интерфейсом выбирают большинство администраторов, особенно тогда, когда устанавливают Server 2012 или обновляют до него систему в первый раз.

Microsoft приводит достойные внимания причины, чтобы рекомендовать установку конфигурации, содержащей лишь основные компоненты, вместо сервера с пользовательским интерфейсом. Среди них безопасность, экономия системных ресурсов и даже автоматизация некоторых задач. Однако я предпочитаю работать с полным графическим интерфейсом. В таком режиме всегда можно запустить PowerShell. Я предпочитаю, чтобы у меня были все доступные средства управления сервером. Если вы — виртуоз PowerShell, который может писать сценарии даже во сне, вы, как уже было сказано, получите очевидные преимущества от варианта с установкой основных серверных компонентов. Но если вы не искушены в PowerShell, полный пользовательский интерфейс — это то, что вам нужно, по меньшей мере на начальном этапе знакомства с Server 2012.

Первые шаги по установке сервера в данной конфигурации совпадают с теми, которые мы уже рассматривали: вставить носитель с установочными файлами в дисковод сервера, позволить загрузиться мастеру установки, где можно выбрать параметры установки, и запустить процесс. Разница заключается лишь в том, что вместо варианта установки основных серверных компонентов (Server Core Installation) нужно выбрать вариант установки сервера с графическим интерфейсом пользователя (Server with a GUI).

Как и в случае с установкой основных серверных компонентов, вам нужно будет принять условия лицензии, настроить разделы и параметры диска и следовать указаниям мастера установки.

После того как установка сервера с пользовательским интерфейсом будет завершена, вы увидите страницу с предложением нажать **Ctrl+Alt+Del**. В результате нажатия этого сочетания клавиш будет открыт экран входа в систему (рис. 2.11). И хотя похожий экран появляется и при установке сервера, включающего лишь основные компоненты, в данном случае его можно назвать первым вестником интерфейса в стиле Modern-UI Windows 8.

Нажмите **Ctrl+Alt+Del** для того, чтобы открыть экран входа в систему (рис. 2.12).

После входа в систему будут загружены службы Windows (Windows Services), заданы персональные настройки, и вы увидите Рабочий стол Server 2012. Кроме того, по умолчанию открывается панель мониторинга диспетчера серверов (Server Manager) (рис. 2.13). Интерфейс системы по сравнению с Server 2008 R2 обновлен — он основан на плитках. Диспетчер серверов и другие компоненты графического интерфейса сервера будут рассмотрены в главе 3.

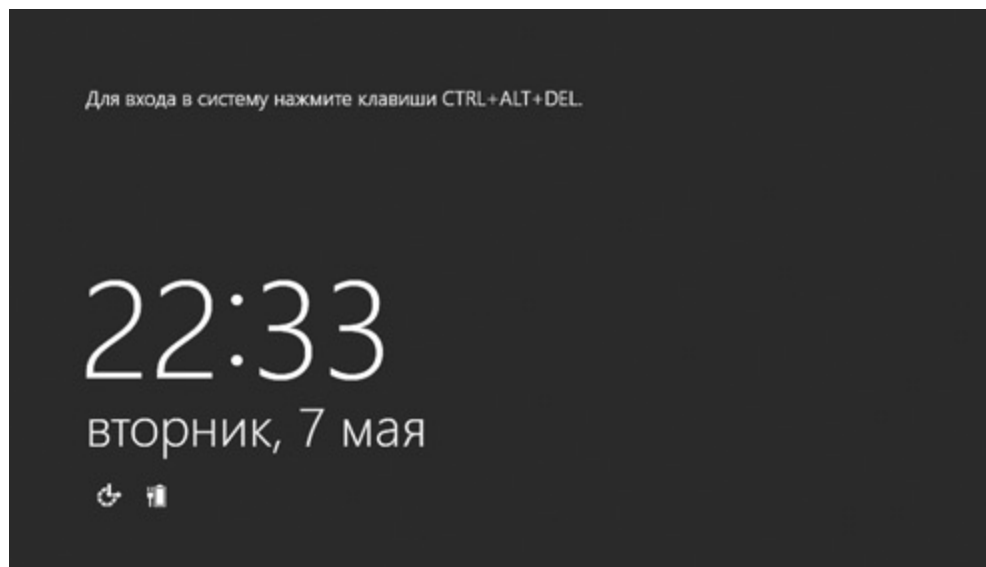


Рис. 2.11. Экран входа в систему в стиле Windows 8

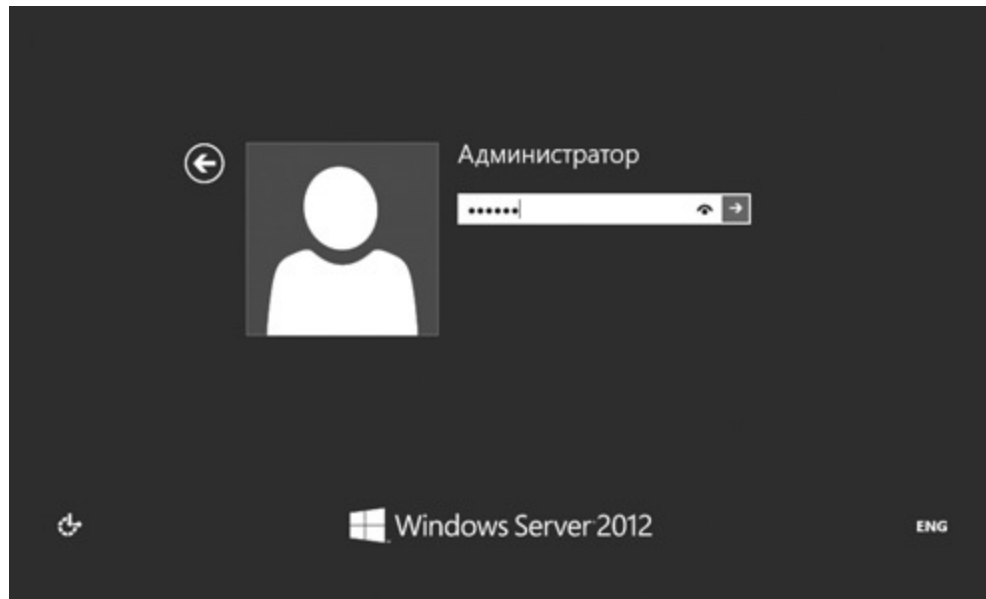


Рис. 2.12. Экран входа в систему

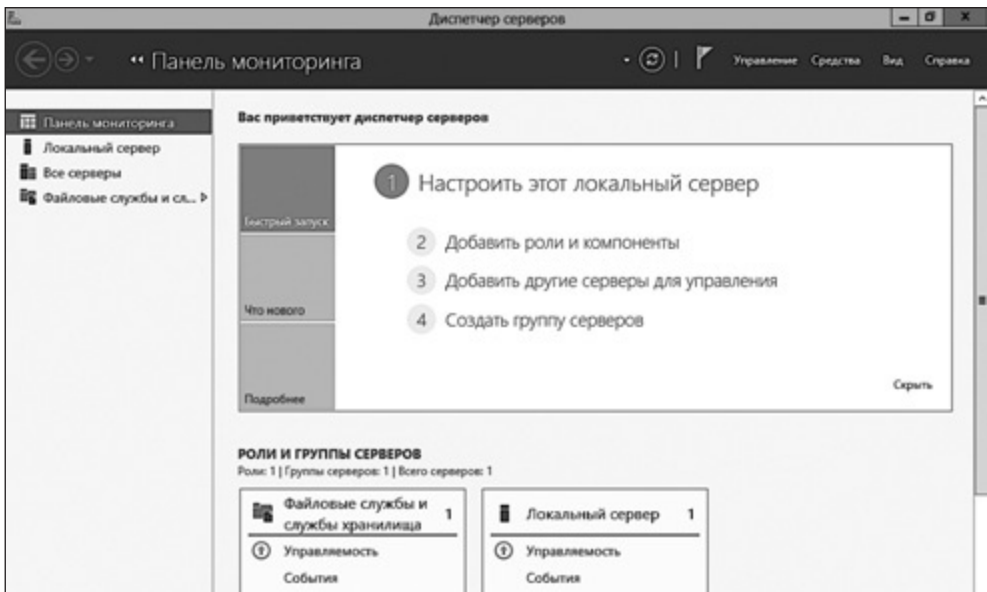


Рис. 2.13. Новая панель мониторинга диспетчера серверов

Переключение между режимами установки

Неважно, какой вариант сервера вы выбрали при установке, — благодаря гибкости Server 2012 в дальнейшем можете переключаться между режимами установки, не теряя существующей конфигурации.

Какие существуют причины для переключения между полным интерфейсом сервера и вариантом установки, содержащим лишь основные компоненты, и обратной процедуры? Одна из них заключается в том, что полная установка требует слишком больших серверных ресурсов. А возможно, вам хочется снизить риск атак на сервер, который сопутствует полному варианту установки. Или вам достаточно удобно администрировать сервер с помощью PowerShell для того, чтобы рационально управлять им и избавиться от полного интерфейса.

Какая бы причина ни являлась для вас значимой, у вас есть пара способов перехода от полного варианта установки к варианту, поддерживающему лишь основные возможности сервера. Преобразование можно выполнить

с помощью простой команды PowerShell либо путем удаления графической оболочки для того, чтобы остались лишь основные компоненты сервера.

Переход от сервера, на котором установлены лишь основные компоненты, к серверу с пользовательским интерфейсом

Для того чтобы преобразовать сервер, в котором установлены лишь основные компоненты, к серверу с графическим пользовательским интерфейсом, вам понадобится создать папку, чтобы смонтировать WIM-файл (Windows Imaging File, файл-ориентированный образ Windows). WIM-файлы — это образы операционной системы, они хранятся на установочном носителе в папке *sources*. Файл образа, который мы собираемся смонтировать, — это *install.wim*, который находится в упомянутой папке.

Начнем с выполнения из командной строки команды `mkdir` для создания папки с именем *mountdir*. Эта команда выглядит так: `mkdir c:\mountdir` (рис. 2.14).

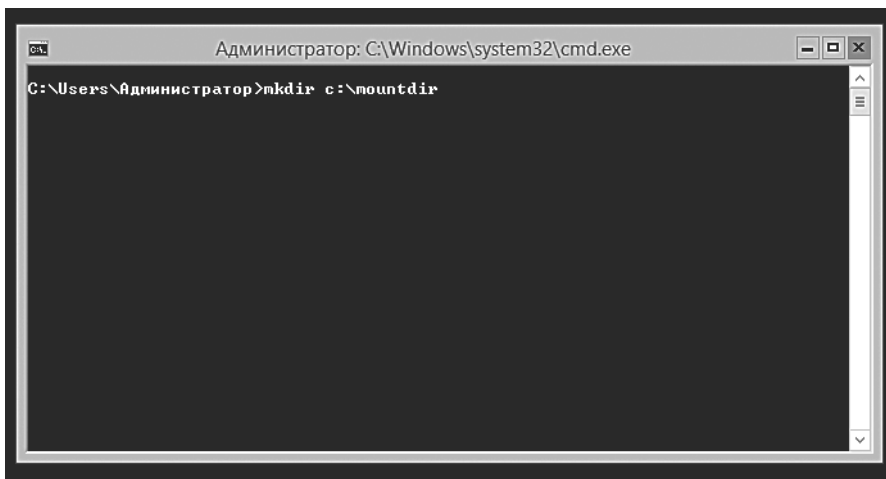


Рис. 2.14. Создание папки *mountdir* для монтирования WIM-файла

После выполнения команды `mkdir` папку *mountdir* можно будет увидеть в корневом каталоге диска *C:* (рис. 2.15).

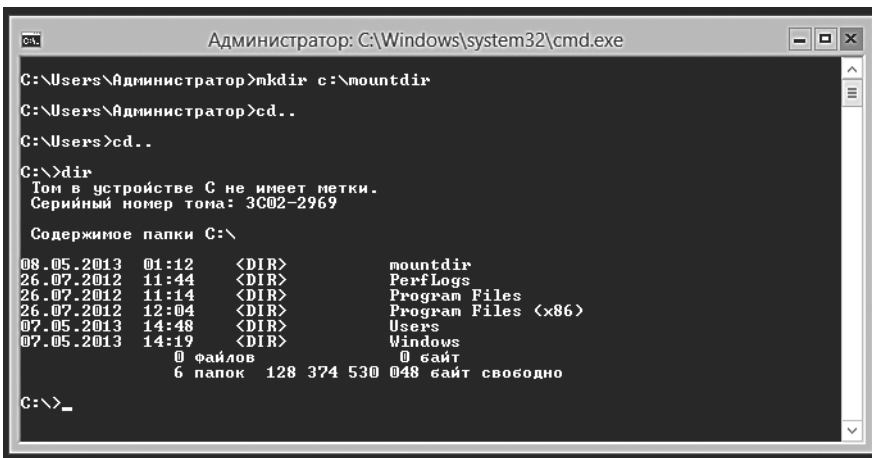


Рис. 2.15. Только что созданная папка mountdir

Далее нужно найти индекс, связанный с образом сервера с графическим интерфейсом пользователя, который вы хотите установить. Например, я конвертирую редакцию Windows Server 2012 Datacenter с установленными основными компонентами. Мне нужно найти образ сервера с графическим интерфейсом, расположенный на установочном носителе, и индекс, соответствующий этому образу. Для этого используем команду `Dism` в командной строке с повышенными полномочиями. Чтобы повысить полномочия интерпретатора командной строки, нужно выполнить команду `runas/user:administrator`. Нажмите Enter, и система предложит вам ввести пароль администратора.

Теперь, для того чтобы получить верный индекс, выполните команду следующего вида (рис. 2.16):

```
Dism /get-wiminfo /wimfile:drive
```

В нашем случае установочный носитель расположен по адресу `d:\sources\install.wim`.

После успешного выполнения данной команды загрузится система DISM (Deployment Image Servicing and Management tool, система обслуживания образов развертывания и управления ими). Найдите индекс образа сервера с графическим интерфейсом, который вы хотите использовать при установке (рис. 2.17).

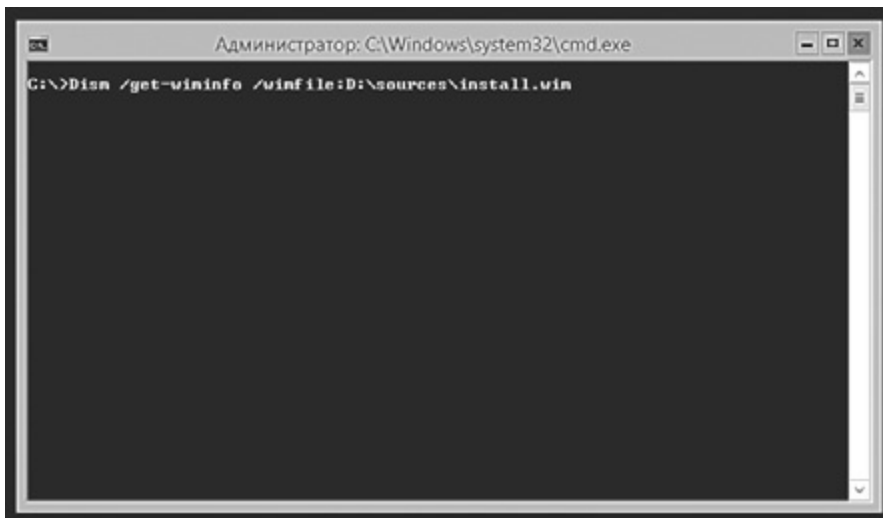


Рис. 2.16. Команда для выяснения индекса подходящего образа сервера с графическим интерфейсом

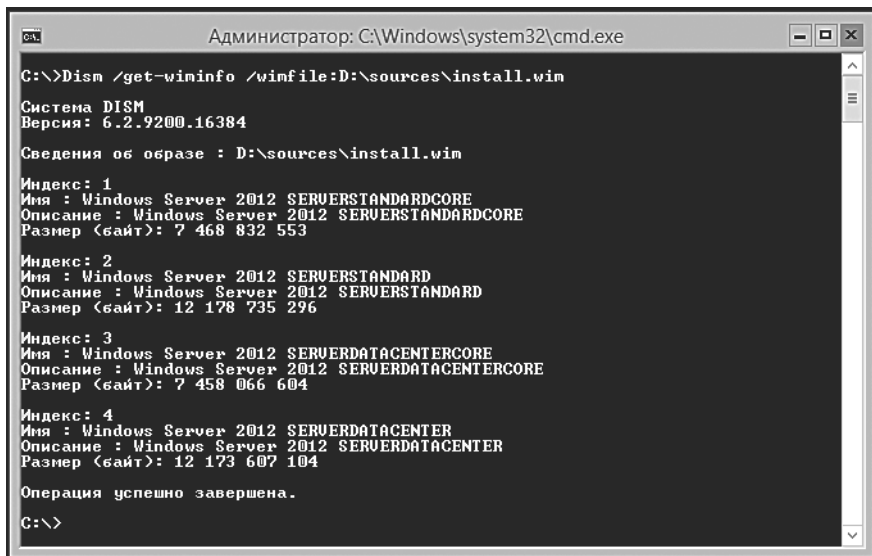


Рис. 2.17. Список файлов образов и их индексы

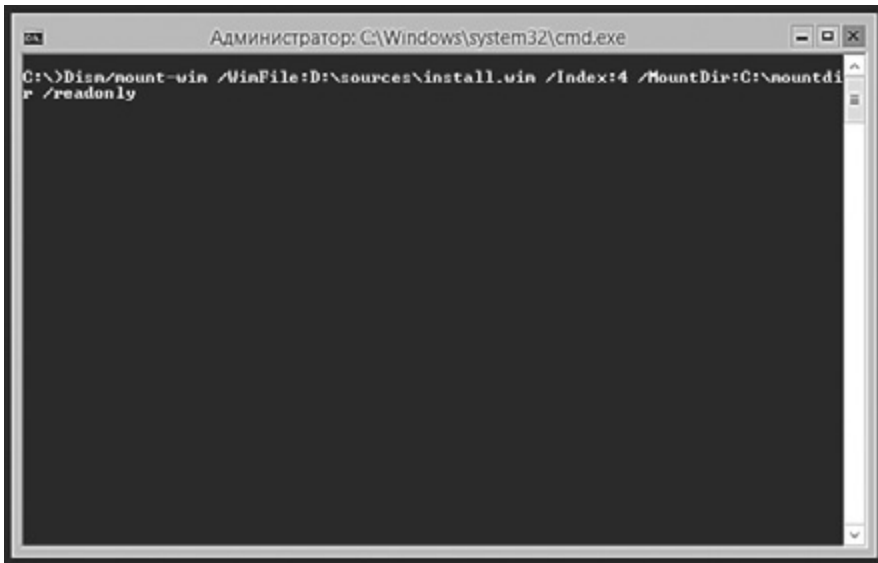


Рис. 2.18. Монтирование файла образа

Смонтируйте подходящий образ с помощью следующей команды (рис. 2.18):

```
Dism /mount-wim /WimFile:drive /Index:#_из_шага_2 /MountDir:c:\mountdir/  
readonly
```

В нашем случае установочный носитель расположен по адресу *d:\sources\install.wim*.

Эта команда снова приведет к запуску системы DISM, и начнется монтирование образа для установки сервера с графическим интерфейсом.

После того как вы увидите сообщение «Операция успешно завершена» («The operation completed successfully»), монтирование будет завершено. Последний шаг при установке сервера с графическим интерфейсом из смонтированного образа требует использования PowerShell. Запустите PowerShell, набрав команду **powershell** в командной строке. PowerShell также нужно запускать с повышенным уровнем административных полномочий, для того чтобы установка прошла успешно.

Запустите следующий командлет:

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart  
-Source c:\mountdir\windows\winsxs
```

Если командлет будет выполнен успешно, начнется установка сервера с графическим пользовательским интерфейсом с помощью PowerShell (рис. 2.19).

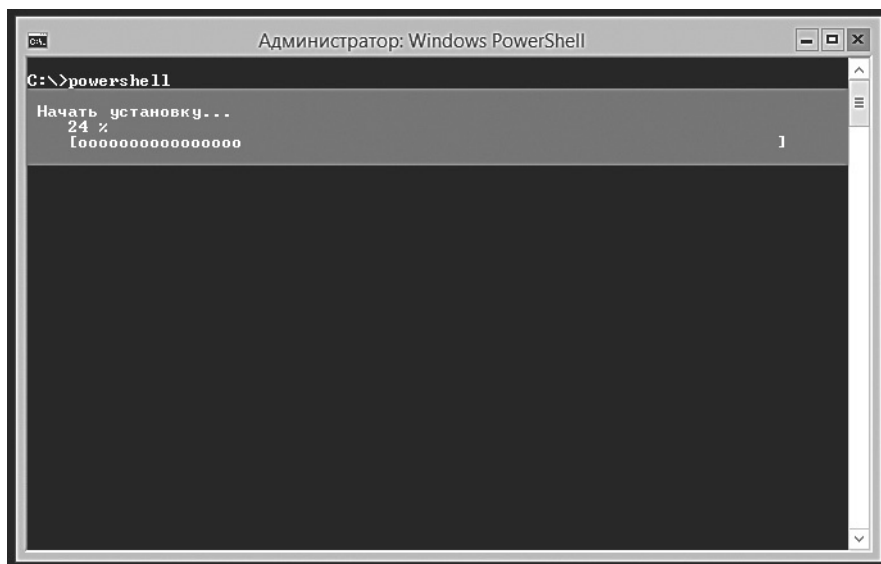


Рис. 2.19. Установка сервера с графическим интерфейсом в PowerShell

После установки сервер будет перезагружен. Когда он загрузится, отобразится экран входа в систему сервера с графическим интерфейсом, на котором нужно нажать **Ctrl+Alt+Del**. Экран ввода пароля и интерфейс сервера с основными компонентами будут заменены на полную графическую оболочку Windows Server 2012.

Кроме того, вы можете вместо WIM-файла использовать службу обновления Windows (Windows Update), используя следующий командлет Windows PowerShell (предварительно убедитесь в наличии соединения с Интернетом):

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
```

Переход от сервера с пользовательским интерфейсом к серверу, на котором установлены лишь основные компоненты

Для того чтобы преобразовать сервер с графическим интерфейсом к серверу, на котором установлены лишь основные компоненты, можно воспользоваться следующим командлетом PowerShell:

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra -restart
```

При успешном выполнении данного командлета начинается процесс удаления графической оболочки сервера (рис. 2.20).

Как только все необходимое будет сделано, сервер перезагрузится. После входа в систему вы увидите интерфейс сервера, на котором установлены только основные компоненты.

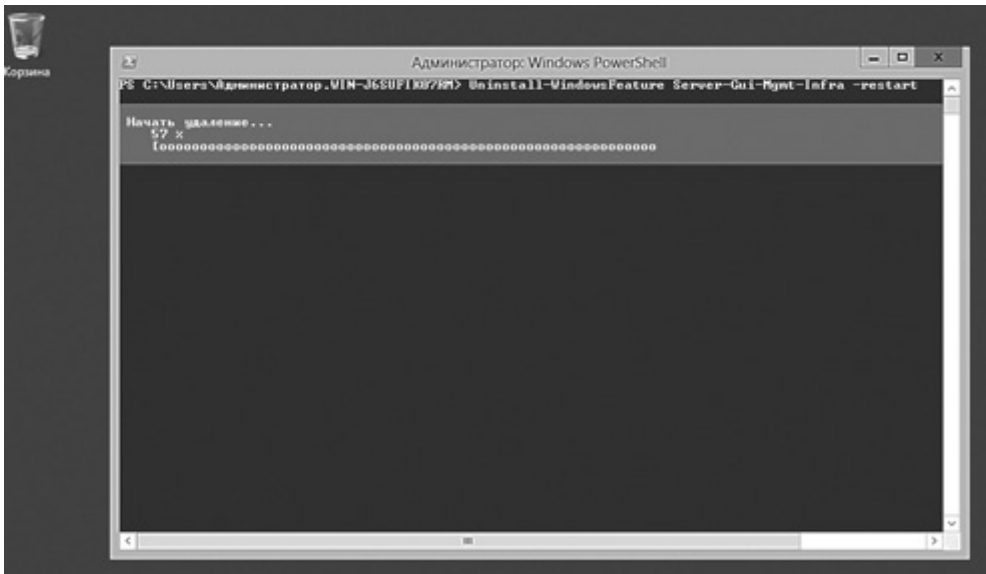


Рис. 2.20. Преобразование сервера с графическим интерфейсом к варианту установки основных компонентов сервера

Если вы изначально выполняли установку сервера с пользовательским интерфейсом и затем, используя приведенную ранее команду, преобразовали его к варианту с установкой основных компонентов, то позже сможете вернуться к серверу с графическим интерфейсом, не задавая источника для его развертывания. Это происходит потому, что необходимые файлы остаются на диске даже в том случае, если они не установлены в системе. Для того чтобы узнать подробности о том, как удалить с диска файлы, отвечающие за интерфейс, обратитесь к разделу данной главы «Настройка интерфейса с помощью компонентов по требованию».

Если вы преобразуете систему к варианту установки Server Core, компоненты Windows, серверные роли и графические инструменты для управления сервером, необходимые для варианта установки сервера с графическим интерфейсом, будут автоматически деинсталлированы. Можете задать параметр `-WhatIf` в PowerShell, для того чтобы увидеть, какие конкретно компоненты затронет преобразование.

Развертывание минимального интерфейса сервера

Windows Server 2012 помимо полного графического интерфейса сервера и сервера, на котором установлены основные компоненты, предлагает промежуточное интерфейсное решение: минимальный интерфейс сервера (Minimal Server Interface). Сервер с полным графическим интерфейсом можно преобразовать в сервер с минимальным интерфейсом с помощью диспетчера серверов. При установке минимального интерфейса сервера удаляются компоненты графической оболочки сервера (Server Graphical Shell). Среди них Internet Explorer 10, Проводник Windows (Windows Explorer), Рабочий стол и начальный экран (Start screen). Среди остающихся установленных компонентов можно отметить консоль управления Microsoft (MMC, Microsoft Management Console), диспетчер серверов (Server Manager) и набор элементов панели управления (Control Panel).

Для того чтобы от сервера с графическим интерфейсом перейти к серверу с минимальным интерфейсом, нужно запустить из диспетчера серверов мастер удаления ролей и компонентов (Remove Roles and Features Wizard). В списке Компоненты (Features) следует выбрать Графические средства

управления и инфраструктура (Graphical Management Tools and Infrastructure) (рис. 2.21).

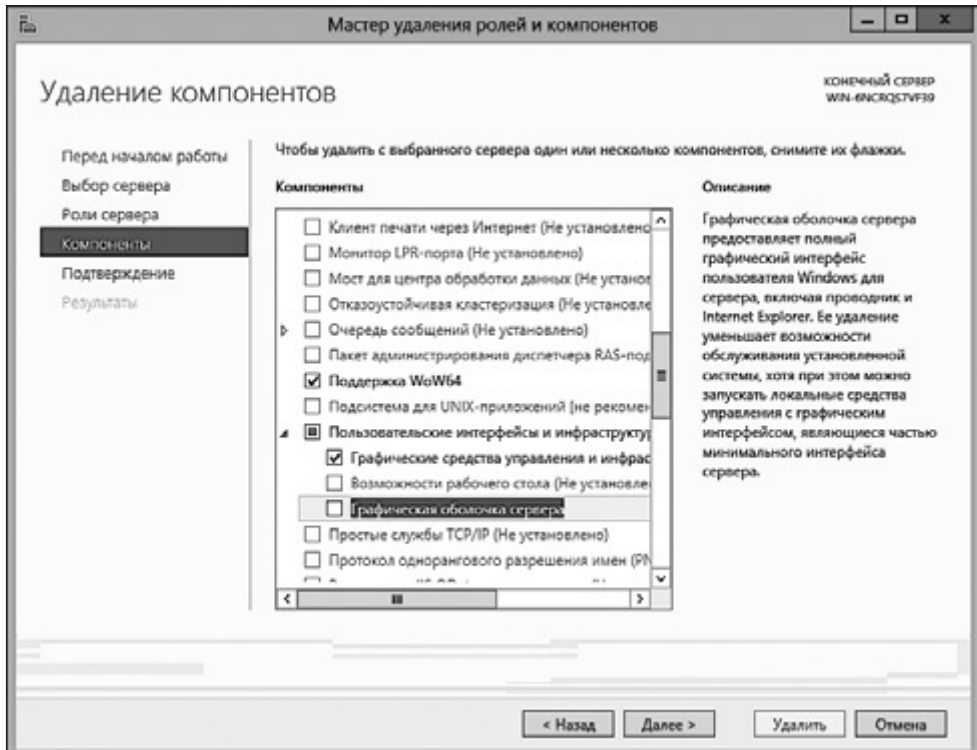


Рис. 2.21. Преобразование сервера с графическим интерфейсом к минимальному интерфейсу сервера

Щелкните на кнопке **Далее** (Next). Установите флажок **Автоматический перезапуск конечного сервера, если требуется** (Restart the destination server automatically if required). Ответьте утвердительно на вопрос о необходимости автоматической перезагрузки сервера (рис. 2.22). Нажмите кнопку **Удалить** (Remove).

В результате мы получим интерфейс, совмещающий черты сервера, установленного в конфигурации установки основных компонентов, и графических инструментов, таких как диспетчер серверов (рис. 2.23).

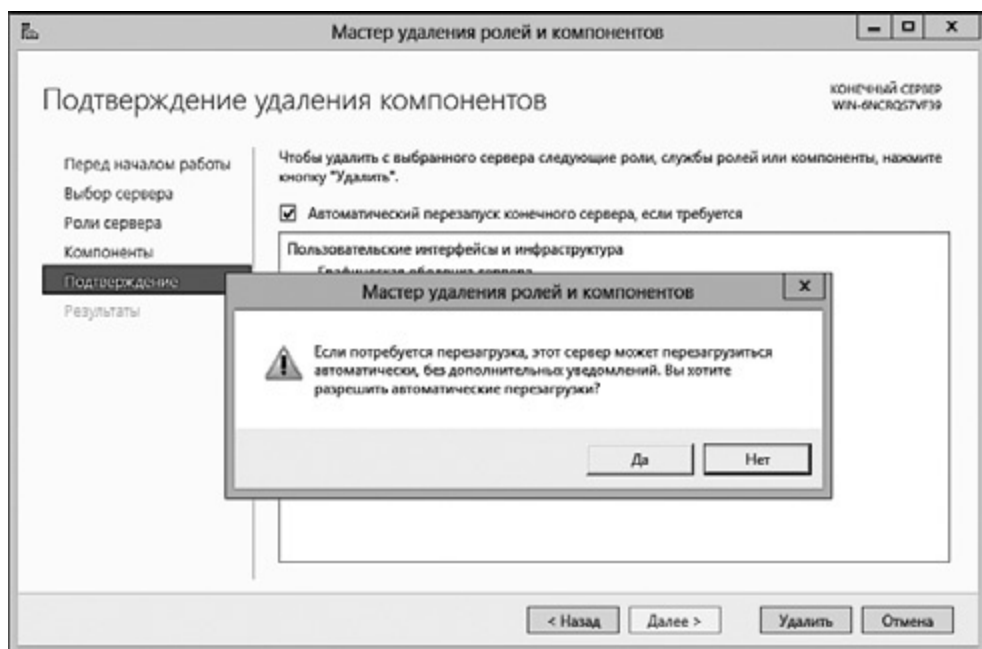


Рис. 2.22. Разрешение автоматической перезагрузки

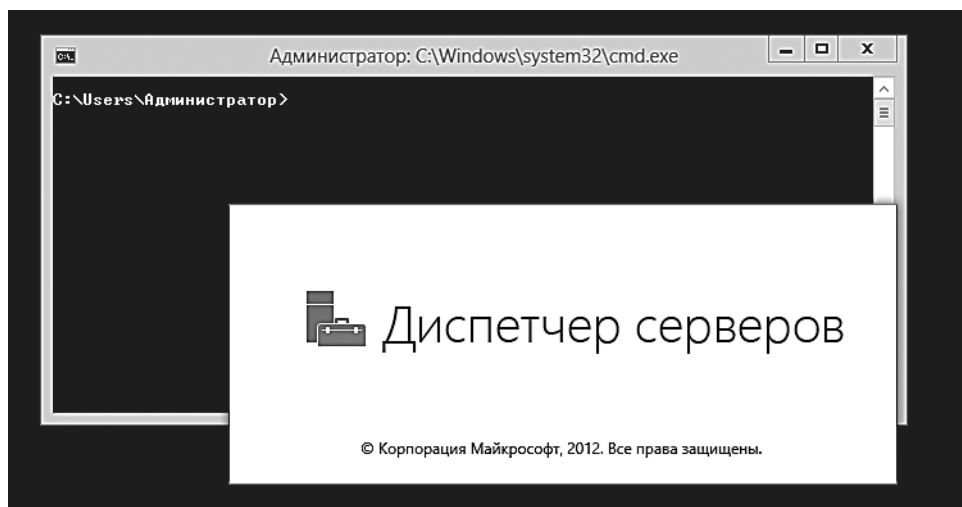


Рис. 2.23. Минимальный интерфейс сервера

Настройка интерфейса с помощью компонентов по требованию

Механизм компонентов, устанавливаемых по требованию (Features on Demand), можно использовать для удаления ненужных ролей и компонентов. Тщательно подходу к выбору компонентов, развернутых на вашем сервере, вы можете сэкономить дисковое пространство. При работе с Hyper-V такой подход уменьшает размер файлов виртуальной машины. В некоторых случаях удаление отдельных ролей и компонентов может уменьшить размер файлов виртуальной машины более чем на 1 Гбайт.

Это одна из моих любимых возможностей в Server 2012. Я не вполне понимаю, почему Microsoft не уделяет особого внимания замечательной возможности подключения компонентов по требованию (Features on Demand), предлагая администраторам пользоваться ею, вместо того чтобы рекомендовать устанавливать сервер в варианте с установкой лишь основных серверных компонентов. Минимальный интерфейс сервера гораздо лучше, чем установка только основных компонентов. Он более гибок в том случае, если вам не нужен полный интерфейс. Это настраиваемый графический интерфейс, который вы можете сконфигурировать в соответствии с вашими нуждами.

Еще одно значительное преимущество Server 2012 перед предыдущими версиями серверных ОС заключается в том, что в предыдущих версиях вы могли отключать роли и компоненты сервера, но файлы, на которых они основаны, оставались на сервере. В Windows 2012 эти файлы можно удалить. Деинсталляция файлов, связанных с серверными ролями и компонентами, приводит к тому, что эти компоненты и роли переходят в состояние Отключено с удалением полезных файлов (Disabled with payload removed).

Для удаления ролей и компонентов вы можете использовать командлет PowerShell. Например, для удаления Проводника Windows (Windows Explorer), Internet Explorer и всех зависимых компонентов можете выполнить такую команду:

```
Uninstall -WindowsFeatures Server-Gui-Shell -remove
```

Если вы удалили роль или отключили компонент с удалением полезных файлов, можете переустановить их. Для переустановки нужен доступ к установочным файлам (обычно они расположены на установочном носителе). Используйте команду PowerShell `Install-Windows Feature` с параметром `-Source`. Если вы не укажете источник (source) установленных файлов,

Windows попытается загрузить необходимые файлы с использованием службы обновления Windows (Windows Update).

Выводы

Перед установкой Server 2012 очень важно все как следует спланировать. Для того чтобы понять, какая именно редакция Server 2012 нужна вашей организации, понадобятся определенные усилия. Учет различных факторов, таких как стоимость, возможности, то, какие функции виртуализации вам нужны, поможет выбрать нужную редакцию Windows Server. Для небольшой инфраструктуры со скромными потребностями в виртуализации и развертывании облачных служб вполне подойдет редакция Standard. Небольшие организации, не нуждающиеся в работе с большими объемами данных, могут рассмотреть варианты использования редакций Essentials или даже Foundation в зависимости от того, какие именно службы им нужны, и от количества поддерживаемых пользователей. Более крупные организации с уже развернутыми (или планируемыми к развертыванию) мощными виртуализованными и облачными средами могут обратить внимание на редакцию Datacenter. Кроме того, перед установкой очень важно убедиться в том, что ваше оборудование соответствует системным требованиям. Не забудьте о том, что Hyper-V предъявляет особые требования к оборудованию, поэтому, если вы планируете устанавливать серверную роль Hyper-V, убедитесь, что аппаратное обеспечение им соответствует.

Позаботьтесь о решении задач, которые предшествуют установке Server 2012. В частности, о создании резервной копии данных. Выберите наиболее подходящий для вас вариант установки — либо сервер с основными компонентами (Server Core), либо сервер с полным интерфейсом (Server with a GUI). Выбирайте тот вариант, который соответствует вашим возможностям по управлению сервером. Если облегченная, экономящая ресурсы установка подходит для существующего серверного аппаратного обеспечения, обратите внимание на вариант с установкой основных серверных компонентов, особенно если вы имеете достаточный опыт использования PowerShell для решения повседневных задач. Если же вы предпочитаете полный пользовательский интерфейс и имеются соответствующие аппаратные ресурсы, обратите внимание на вариант установки сервера либо с полным пользовательским интерфейсом, либо с минимальным интерфейсом. А если вам нужна рабочая среда, настроенная под ваши нужды, рассмотрите возможность подключения компонентов по требованию (Features on Demand). Она позволяет выбирать только

необходимые вам графические элементы управления, которыми можно пользоваться при установке интерфейса сервера с основными компонентами.

Server 2012 гораздо более гибок в плане установки и настройки, чем предыдущие версии серверных ОС от Microsoft. Используйте эту гибкость в своих целях, для того чтобы достичь максимальной эффективности управления сервером.

3 Управление Windows Server 2012

Самое замечательное в улучшениях, выполненных в Server 2012, — это система управления. Здесь имеется расширенный интерфейс диспетчера серверов (Server Manager) и более аскетичный PowerShell. Кроме того, инструменты управления сервером можно запускать на удаленных клиентских компьютерах. Вам не обязательно управлять серверами локально. В Server 2012 просто, как никогда, управлять множеством серверов с помощью единой консоли диспетчера серверов.

Диспетчер серверов обладает обновленным интерфейсом, основанным на плитках, но если вы работали с ним в предыдущих версиях Windows Server, то без труда сможете в нем ориентироваться. Диспетчер серверов — это централизованное Рабочее место управления серверами. Слово *«централизованное»* играет здесь особую роль, так как с помощью диспетчера серверов вы можете выполнять множество задач по обслуживанию сервера. Среди них добавление серверных ролей и компонентов, настройка политик безопасности, конфигурирование удаленных Рабочих столов и т. д.

Даже в самых маленьких организациях в большинстве сетевых инфраструктур, основанных на Windows, имеется несколько серверов. И эффективное управление несколькими серверами было одной из непростых задач, которую

приходилось решать администраторам в предыдущих версиях Windows Server. Теперь же диспетчер серверов позволяет администратору добавлять в панель мониторинга диспетчера несколько серверов, для того чтобы иметь возможность контролировать их состояние и управлять всеми серверами, развернутыми в организации. Это ключевое преимущество, так как возможность управлять всеми серверами с помощью одного интерфейса сокращает нагрузку на администраторов и позволяет управлять серверами из одного места вне зависимости от того, расположены ли они неподалеку от администратора, являются удаленными или виртуальными. Возможность управлять множеством серверов, поддерживаемая диспетчером серверов, — это еще один шаг в сторону облака. Это тенденция к перемещению критически важных бизнес-служб и приложений, равно как и хранилищ данных, на поддерживаемые другими организациями онлайн-серверы, за пределы центров обработки данных. Более эффективное управление множеством серверов подразумевает большую гибкость в управлении серверами, развернутыми в облаке, облачными приложениями и службами, а также масштабировании инфраструктуры.

PowerShell предлагает даже большие возможности по управлению Windows-окружением, особенно при выполнении автоматизированных задач. Новые командлеты и другие улучшения значительно повышают эффективность использования PowerShell. Несмотря на это, многие администраторы, особенно поддерживающие небольшие и средние инфраструктуры, просто не могут расстаться с графическим интерфейсом сервера. И пусть хорошие администраторы находят время для того, чтобы изучить хотя бы основы PowerShell, давайте взглянем правде в глаза: иногда для того, чтобы что-либо сделать, гораздо легче пару раз щелкнуть мышью. Настройка параметров сети — это один из примеров.

Поэтому в данной главе я уделю особое внимание тому, как выполнять основные задачи по управлению сервером, используя преимущественно диспетчер серверов и другие подобные инструменты, например консоль управления Microsoft (MMC, Microsoft Management Console). Но несмотря на это, здесь я показываю и способы выполнения некоторых из этих задач с помощью PowerShell.

Кроме того, данная глава знакомит администраторов с пользовательским интерфейсом Server 2012 и с тем, как управлять несколькими серверами и серверами, которые работают под управлением предыдущих версий Windows. Здесь речь идет и об использовании обычных приложений и, наконец, о том, как установить на клиентском компьютере инструменты Server 2012 для управления сервером при удаленном администрировании.

Интерфейс Server 2012

После того как вы войдете в Server 2012 с графическим интерфейсом, автоматически откроется окно панели мониторинга диспетчера серверов. И хотя вы будете выполнять большинство административных действий в диспетчере серверов, что если вам понадобятся Рабочий стол и кнопка Пуск?

В интерфейсе Server 2012 кнопка Пуск, присутствовавшая в предыдущих версиях операционных систем семейства Windows, не предусмотрена. По умолчанию на Рабочем столе отображается лишь один значок — Корзина (рис. 3.1).

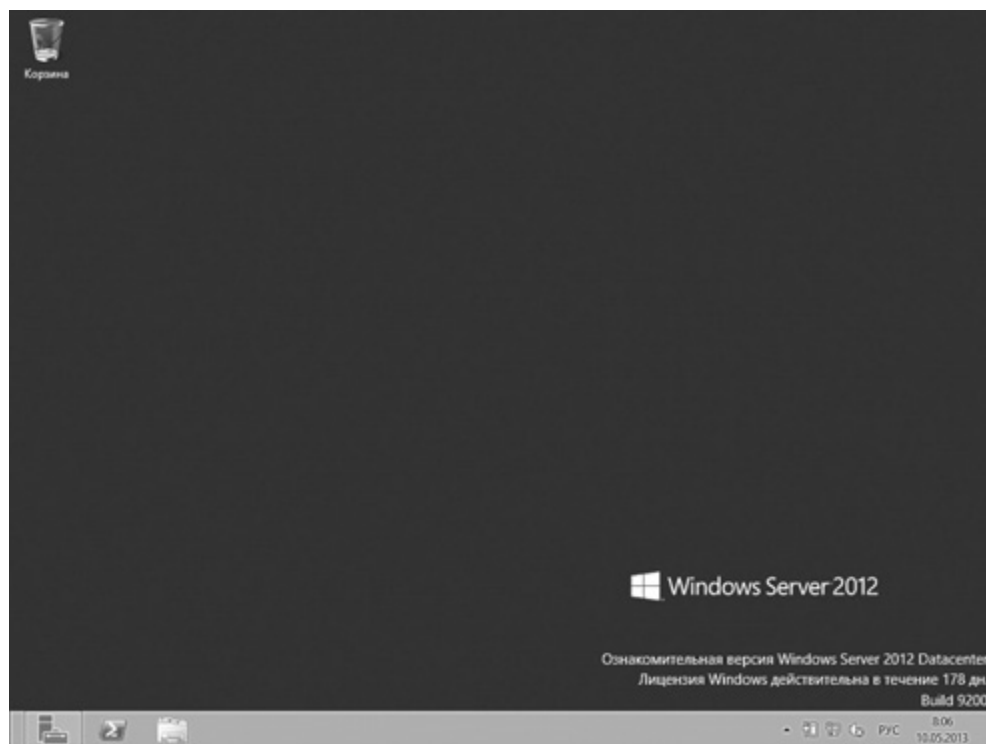


Рис. 3.1. Рабочий стол сервера с графическим интерфейсом

От интерфейса Server 2008 на Рабочем столе осталась лишь панель задач. В Server 2012 на панели задач три закрепленных ярлыка: диспетчер серверов, PowerShell и Проводник Windows.

Учтите: если вы работали с Server 2008 R2 и другими версиями серверных ОС семейства Windows, изменения в интерфейсе могут показаться вам непонятными. Когда я впервые увидела Рабочий стол Server 2012, то слегка растерялась — не знала даже, где нужно щелкнуть, чтобы выключить компьютер! После того как поработала с Server 2012 примерно неделю, я обнаружила, что те инструменты и меню, которые раньше использовались для работы с Windows Server, никуда не делись — они просто расположены в других местах. Например, у меню кнопки Пуск теперь есть собственный экран, независимый от Рабочего стола. В Server 2012 найти какую-нибудь программу или инструмент проще, чем в предыдущих версиях системы. Далее я расскажу вам, как это сделать.

На экране вы можете увидеть небольшой прямоугольник левее значка Диспетчер серверов на панели управления. Если навести указатель мыши на его левый нижний угол и щелкнуть на появившемся значке, будет открыт начальный экран (рис. 3.2).

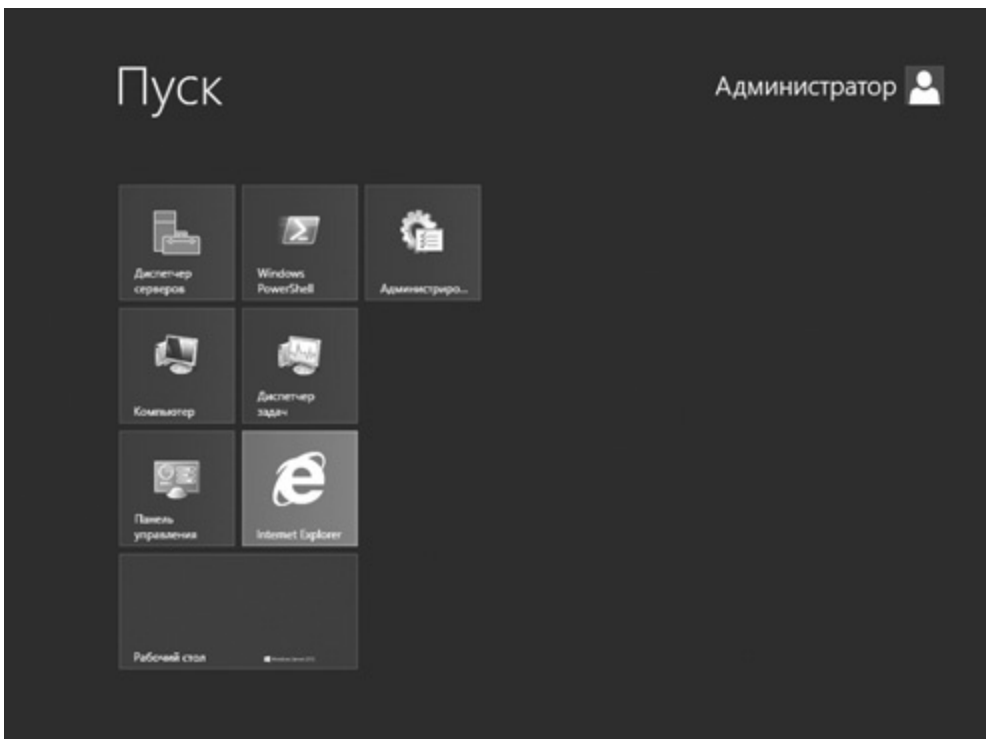


Рис. 3.2. Начальный экран Server 2012

Работа с плиточным интерфейсом

У начального экрана Server 2012 такой же плиточный интерфейс, как у клиентских систем на базе Windows 8, только плиток на нем меньше и он имеет более строгое цветовое оформление. Плитками элементы управления Server 2012 названы так из-за их внешнего сходства с теми плитками, которыми покрывают полы в ваннных комнатах или стены в кухнях. Плитки в Server 2012 — это то же самое, что значки в Server 2008. Щелчок на плитке открывает соответствующую программу.

На начальном экране администраторы обнаружат все дополнительные серверные приложения, которых, как кажется, не хватает на Рабочем столе. По умолчанию отображаются восемь плиток: Диспетчер серверов, Windows PowerShell, Администрирование, Компьютер, Диспетчер задач, Панель управления, Internet Explorer и Рабочий стол. В верхнем правом углу экрана отображается имя учетной записи пользователя, который вошел в систему.

При работе на начальном экране в правом нижнем углу появляется значок с изображением увеличительного стекла. Если навести мышь на этот значок (рис. 3.3), появится панель чудо-кнопок (Charms menu).

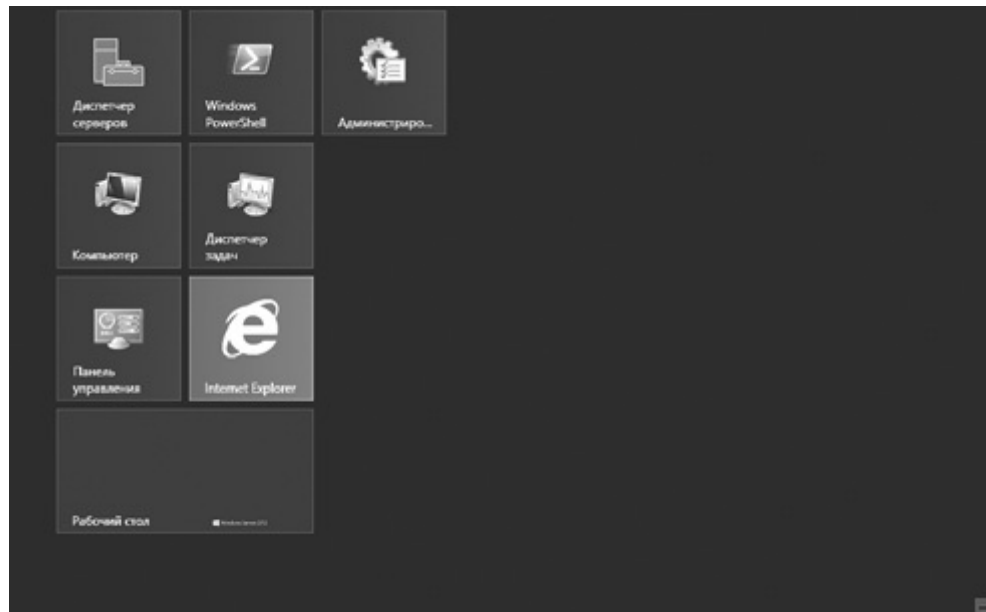


Рис. 3.3. В правом нижнем углу экрана находится значок для вызова панели чудо-кнопок



Если щелкнуть на значке, который появляется в правом нижнем углу экрана, можно уменьшить размер начального экрана.

Панель чудо-кнопок выдвигается из-за правого края экрана. Значки на ней, или чудо-кнопки, — это Поиск (Search), Пуск (Start) и Параметры (Settings) (рис. 3.4). Кроме того, на экране вместе с панелью чудо-кнопок отображается небольшое окно, содержащее сведения о дате, времени, сетевом подключении и некоторые другие данные. Подобное отображение даты и времени на экране сервера может показаться странным. Но оно очень кстати, так как на начальном экране нет, как в Server 2008, расположенной в нижнем правом углу области системных уведомлений (System Tray), в которой всегда отображаются дата и время.

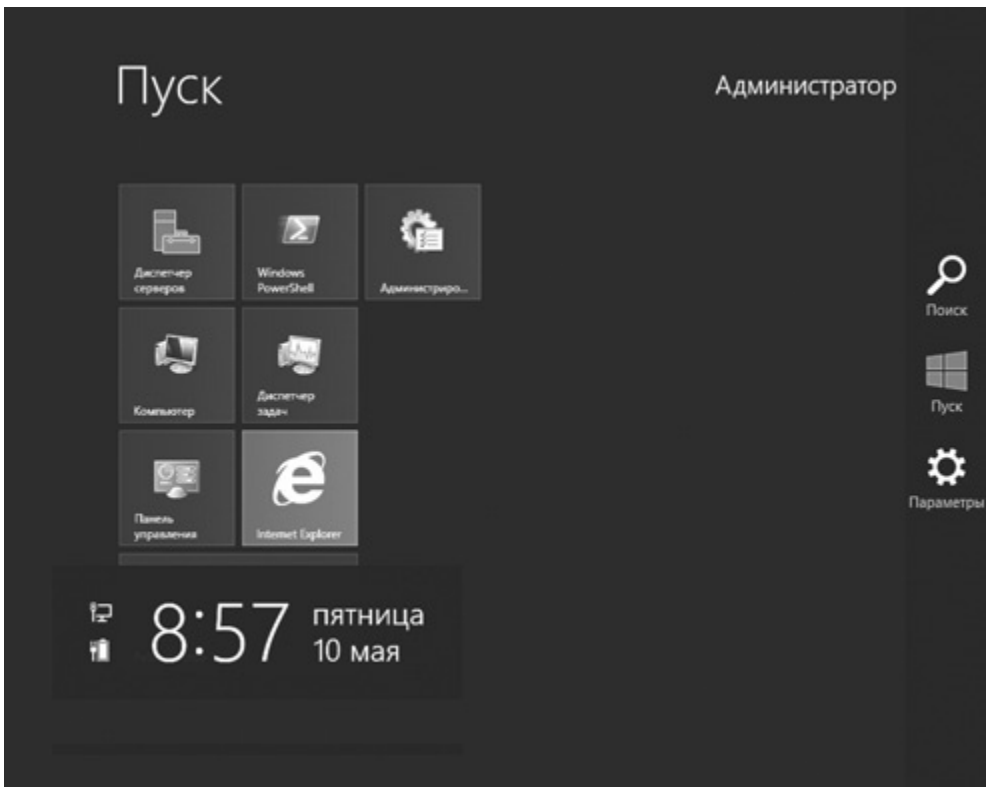


Рис. 3.4. Панель чудо-кнопок

Если щелкнуть на начальном экране правой кнопкой мыши, будет открыто еще одно меню (панель начального экрана), в котором имеется команда **Все приложения** (All apps) (рис. 3.5).



В мире высоких технологий наблюдается сдвиг от концепции ориентации на персональные компьютеры к мобильным технологиям. Поэтому программы (programs) и приложения (application) часто называют просто приложениями (apps), даже если они рассчитаны на работу на серверах или настольных компьютерах.

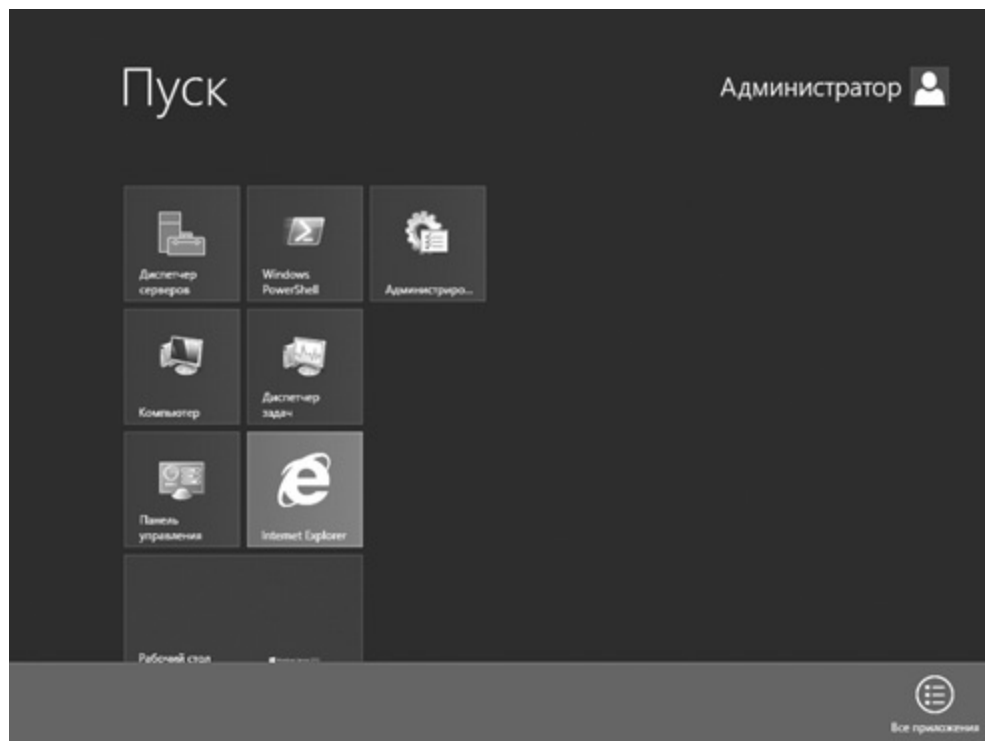


Рис. 3.5. Команда Все приложения

Если щелкнуть на значке **Все приложения**, будет отображен список всех приложений, установленных на Server 2012, в том числе Системный монитор, Блокнот, Paint, Система архивации данных Windows Server и др.

Поскольку новый интерфейс создавался в расчете на мобильные устройства, оснащенные сенсорным экраном, прокрутка списка плиток ориентирована на использование сенсорных жестов. Работая на компьютере, не оснащенном сенсорным экраном, вы можете воспользоваться полосой прокрутки, расположенной в нижней части экрана, но удобнее в данной ситуации пользоваться клавишами-стрелками на клавиатуре.

Решение Microsoft о включении интерфейса, основанного на плитках и применяемого в Windows 8-клиентах, в Server 2012 вызвало множество споров и совершенное недоумение среди многих бета-тестеров и в техническом сообществе. Помните, однако, что вы не обязаны работать с графическим интерфейсом сервера. Можете установить Server 2012 в облегченном режиме установки основных серверных компонентов или использовать минимальный интерфейс сервера и выбрать только нужные компоненты графической оболочки.



Не путайте Рабочий стол и начальный экран. В Server 2012 это разные экраны, в то время как в Server 2008 R2 меню Пуск располагалось на Рабочем столе. В Server 2012 вы можете переходить с Рабочего стола на начальный экран, и наоборот. Быстрее всего переключаться между ними, используя кнопку Windows на клавиатуре.

Использование средств управления сервером

Поскольку в Server 2012 с пользовательским интерфейсом имеются два главных экрана — начальный экран и Рабочий стол, существует несколько способов вызова средств управления сервером. В этом разделе мы поговорим о том, как можно быстро найти наиболее часто используемые приложения для управления сервером, как их запускать от имени администратора и как запускать консоль управления Microsoft.

Поиск средств управления сервером

Вот где вы можете найти наиболее часто используемые приложения для управления сервером:

- **Панель управления.** Плитка панели управления (Control Panel) — это часть стандартного начального экрана, она появляется на нем сразу после установки сервера с пользовательским интерфейсом. Панель управления можно найти и в списке **Все приложения**.
- **Windows PowerShell.** Как и в случае с панелью управления, вы найдете плитку Windows PowerShell либо на начальном экране, либо в списке **Все приложения**. Кроме того, при установке Server 2012 с пользовательским интерфейсом ярлык для вызова PowerShell закреплен на панели задач Рабочего стола.
- **Командная строка.** Значок для вызова командной строки (Command Prompt) можно найти в списке **Все приложения**.



Командная строка и PowerShell — это не одно и то же. Командная строка используется для запуска DOS-команд и создания пакетных файлов. PowerShell — это среда исполнения сценариев для администрирования Windows и выполнения сложных задач наподобие управления разрешениями.

Запуск приложения от имени администратора

Для того чтобы запустить программу от имени администратора с использованием графического интерфейса, выделите плитку приложения щелчком правой кнопкой мыши, а затем из панели, которая появится в нижней части экрана, выберите команду **Запуск от имени администратора** (Run as administrator).

Запуск консоли управления Microsoft

Для того чтобы открыть MMC, перейдите на начальный экран, наберите «MMC» и воспользуйтесь значком MMC из списка результатов поиска.

Интерфейс MMC по сравнению с имеющимся в Server 2008 R2 обновлен: хотя MMC включает в себя оснастку Локальная архивация (Local Backup), в ней нет оснастки диспетчера сервера (Server Manager) (рис. 3.6).

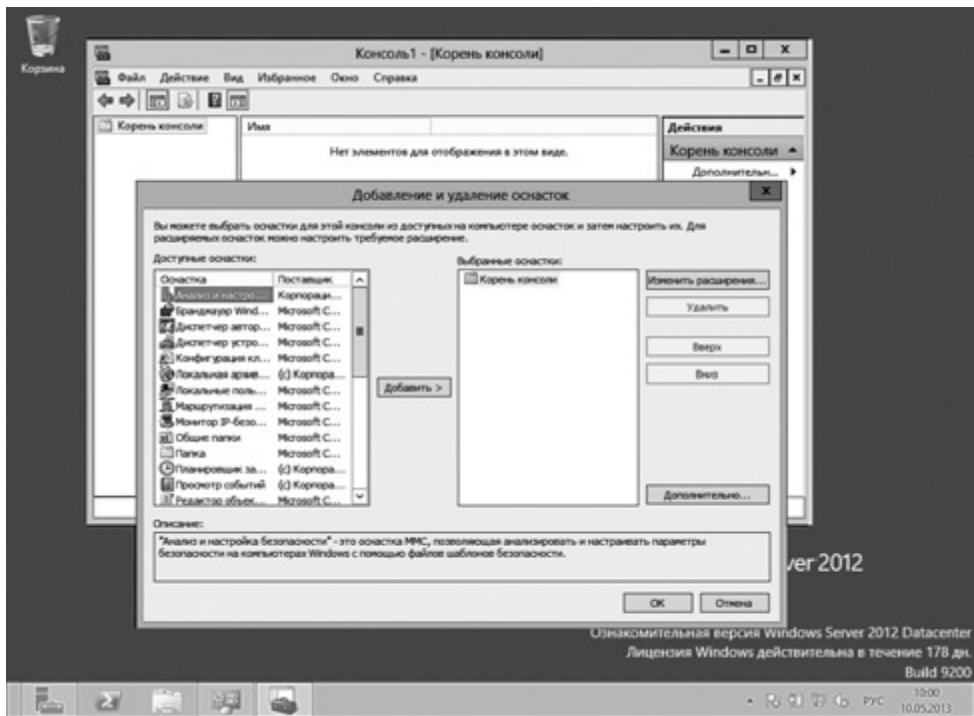


Рис. 3.6. MMC

Кроме того, вы можете настроить интерфейс Рабочего стола и начального экрана так, как вам нужно, добавить ярлыки, чтобы находить приложения гораздо быстрее. В следующем разделе я расскажу вам, как это сделать.

Настройка интерфейса

Существует немало возможностей настройки Рабочего стола и начального экрана.

Настройка Рабочего стола

Настройка Рабочего стола во многом напоминает его настройку в Server 2008 R2 или других ОС семейства Windows. Щелкните правой кнопкой

мыши на свободном пространстве на Рабочем столе для вызова контекстного меню. Выберите в этом меню пункт Разрешение экрана (Screen resolution).

В окне Разрешение экрана (Screen resolution) вы можете настраивать параметры экрана (рис. 3.7). Щелкните на ссылке Изменение размеров текста и других элементов (Make text and other items larger or smaller), в результате будет открыто окно Экран (Display) (рис. 3.8).

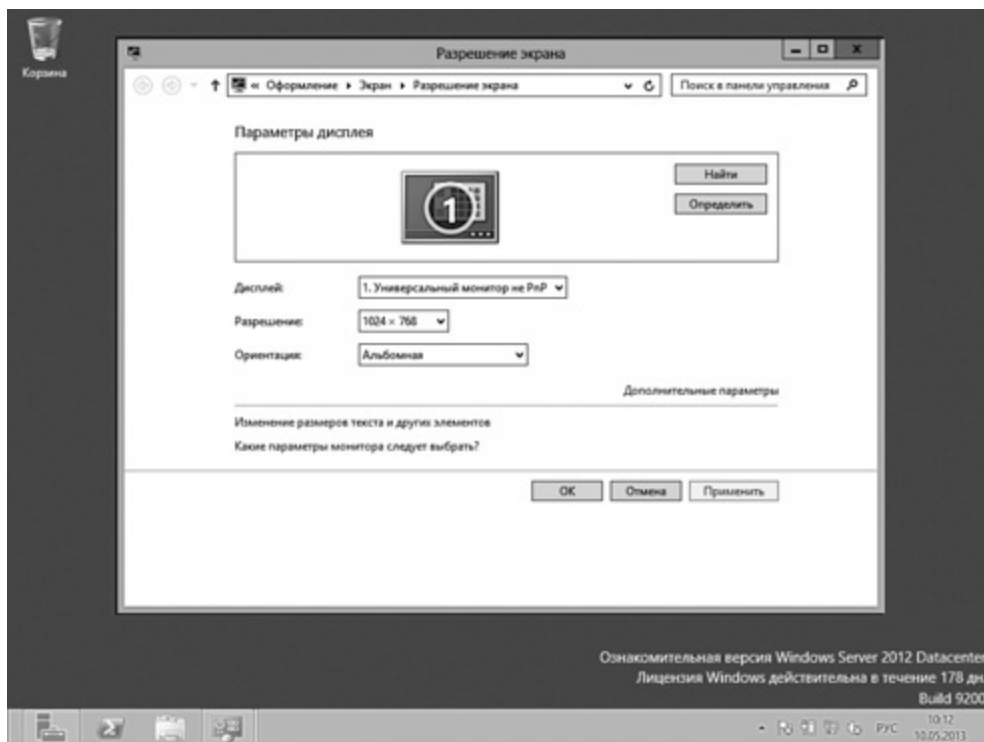


Рис. 3.7. Настройка разрешения экрана

Если вы когда-нибудь настраивали параметры экрана в Windows, это окно вам уже знакомо. Настроив Рабочий стол, вы можете изменить его фоновый рисунок, цвет окон, заставку и многое другое. Единственное, чего нет в Server 2012, — это интерфейс Aero. Вы можете сделать Рабочий стол Server 2012 больше похожим на Windows 8, установив компонент Возможности Рабочего стола (Desktop Experience). Для того чтобы сделать это, в мастере Добавить роли и компоненты (Add roles and features) нужно установить

флажок Возможности Рабочего стола (Desktop Experience), который находится в группе Пользовательские интерфейсы и инфраструктура (User Interfaces and Infrastructure).

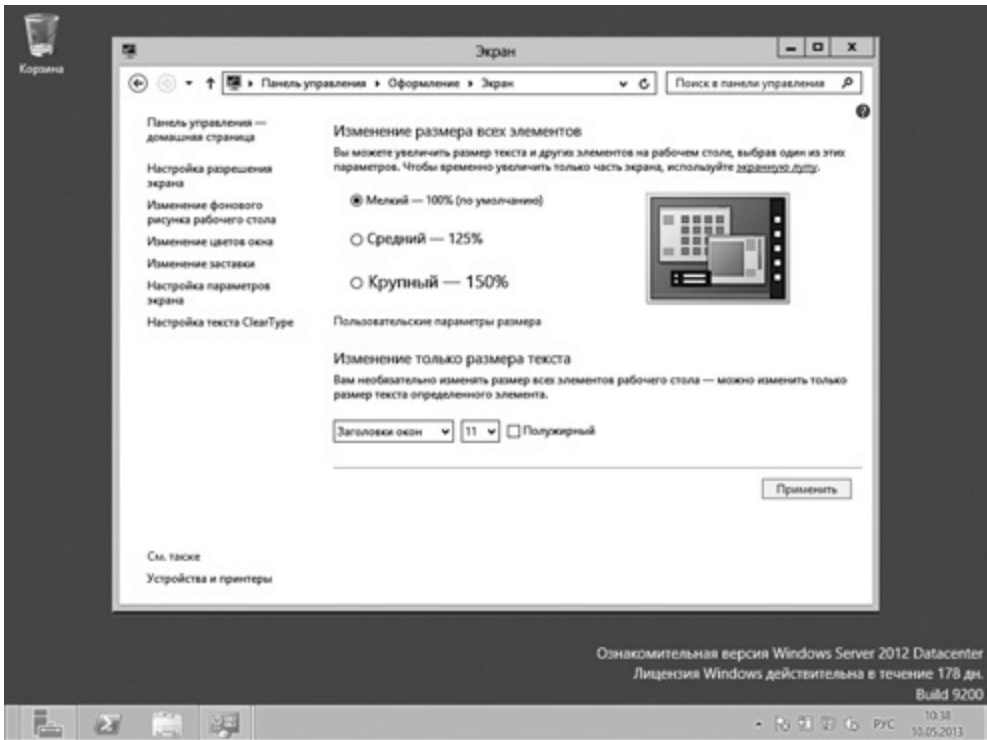


Рис. 3.8. Окно Экран

Вы можете размещать ярлыки для вызова приложений, находящихся в списке приложений начального экрана, на Рабочем столе. Например, если вам нужно добавить на Рабочий стол ярлык для вызова панели управления (Control Panel), можете щелкнуть в любом месте Рабочего стола правой кнопкой мыши, выбрать в появившемся меню команду Создать (New), в подменю выбрать команду Ярлык (Shortcut). В окне Создать ярлык (Create Shortcut) нужно ввести «Control Panel», однако вы можете нажать кнопку Обзор (Browse), для того чтобы самостоятельно найти нужную программу. Теперь нужно нажать кнопку Далее (Next), ввести имя ярлыка, например «Панель управления», и нажать Готово (Finish). Теперь на Рабочем столе есть ярлык для вызова панели управления.

Ярлыки для вызова приложений можно закреплять на панели задач. Перейдите на начальный экран, откройте окно **Все приложения**. Щелкните правой кнопкой мыши на приложении, ярлык которого хотите закрепить на панели задач, значок приложения будет выделен. В нижней части экрана откроется панель, где имеются несколько команд, которые появляются там при выделении значка приложения: **Закрепить на начальном экране (Pin to Start)**, **Закрепить на панели задач (Pin to taskbar)**, **Открыть в новом окне (Open new window)**, **Запустить от имени администратора (Run as administrator)** и **Открыть расположение файла (Open file location)**. Щелчок на команде **Закрепить на панели задач** приводит к размещению ярлыка для вызова программы на панели задач Рабочего стола. На рис. 3.9 показан список приложений с выделенным значком **Монитор ресурсов (Performance Monitor)**.

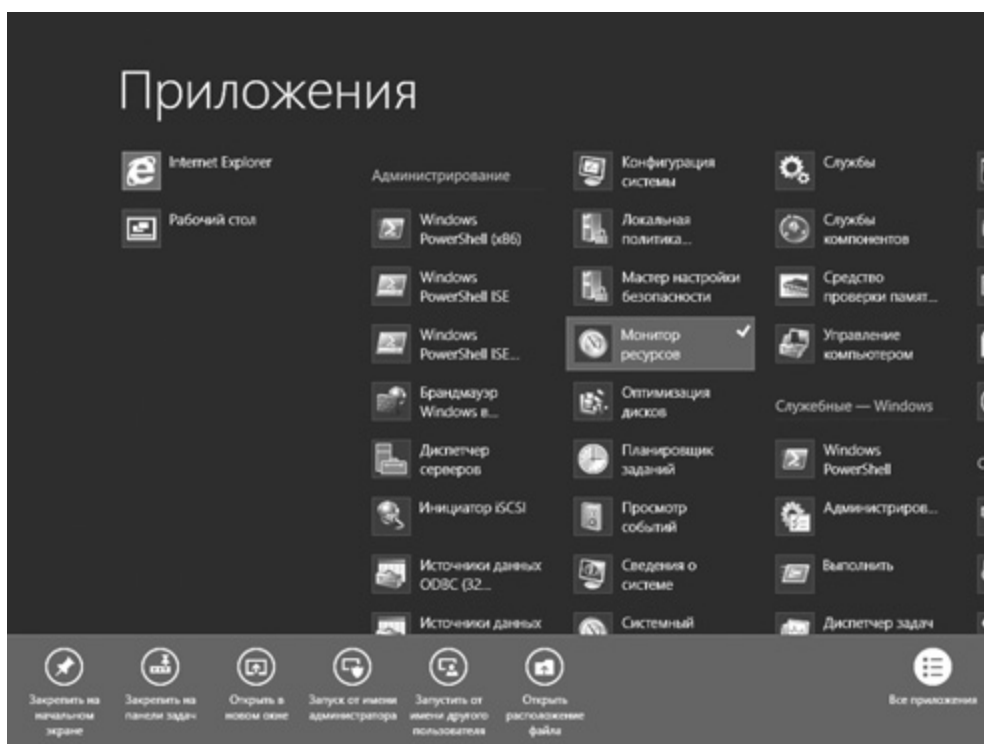


Рис. 3.9. Выделенный значок Монитор ресурсов

На рис. 3.10 показан ярлык монитора ресурсов, закрепленный на панели задач. Количество ярлыков, которые можно размещать на панели задач, не

ограничено. Когда они перестанут помещаться на ней, в ее правой части появятся кнопки со стрелками, направленными вверх и вниз. Эти кнопки позволяют прокручивать панель, просматривая закрепленные на ней ярлыки. Однако если на панели задач закрепить слишком много ярлыков, она будет выглядеть перегруженной. Прокрутка панели в поисках нужного ярлыка противоречит идее быстрого доступа к приложениям, поэтому закрепляйте здесь ярлыки только тех приложений, которыми пользуетесь часто.

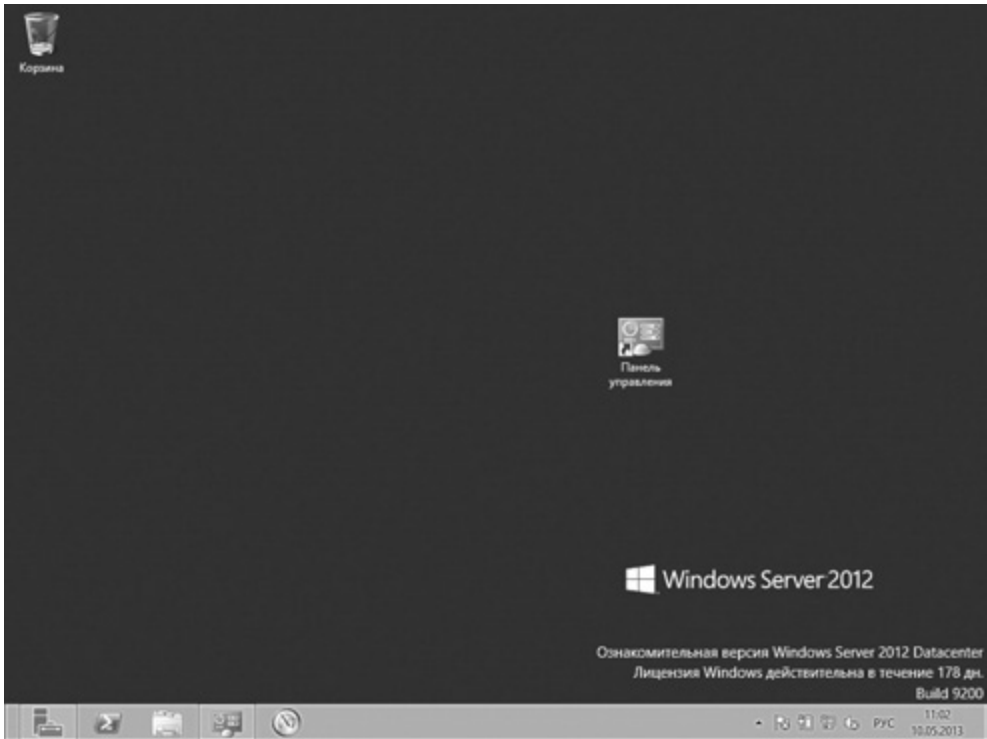


Рис. 3.10. Ярлык монитора ресурсов закреплен на панели задач

Для того чтобы удалить ярлык с панели задач, достаточно щелкнуть на нем правой кнопкой мыши и выбрать из списка команду **Изъять программу из панели задач** (Unpin this program from taskbar).

Когда ярлык приложения закреплен на панели задач Рабочего стола, его плитка остается на начальном экране. Удалить ярлык с панели задач можно и воспользовавшись средствами начального экрана.

Настройка начального экрана

Внешний вид начального экрана также поддается настройке. Хотя по умолчанию на начальном экране присутствует лишь несколько плиток, вы можете добавить на него и другие плитки. Для того чтобы сделать это, щелкните правой кнопкой мыши на начальном экране и из панели начального экрана выберите команду **Все приложения (All apps)**.

Для добавления плиток на начальный экран нужно выполнить последовательность действий, похожую на ту, которую мы выполняли для закрепления ярлыка программы на панели задач. Щелкните на значке приложения и из панели, которая появится в нижней части экрана, выберите команду **Закрепить на начальном экране (Pin to start)**.

Кроме того, вы можете скрыть с начального экрана средства администрирования. Это может быть полезно, если вы управляете сервером удаленно и не хотите, чтобы кто-либо получил доступ к этим средствам на локальном компьютере. Для того чтобы это сделать, вызовите панель чудо-кнопок, щелкните на чудо-кнопке **Параметры (Settings)**, в появившейся панели нажмите **Плитки (Tiles)**. Чтобы скрыть средства администрирования, установите переключатель **Показать средства администрирования (Show administrative tool)** в положение **Нет (No)** (рис. 3.11).

Выход из системы, перезагрузка и отключение питания

Отсутствие кнопки **Пуск** делает выполнение простых задач, таких как выход из системы, перезагрузка или выключение Server 2012, немного непривычным для тех, кто привык к предыдущим версиям ОС семейства Windows. Все это делается не так, как в Server 2008 R2.

Для того чтобы выйти из системы и войти в нее в роли другого пользователя, нужно щелкнуть на имени текущего пользователя в верхнем правом углу начального экрана. В появившемся меню следует выбрать команду **Выйти (Sign out)**. Также из этого меню вы можете заблокировать экран. Когда экран заблокирован, на нем имеется кнопка **Сменить пользователя (Switch user)**. Это еще один способ выхода из системы и входа под другой учетной записью.

Для того чтобы выключить компьютер или перезагрузиться, вызовите панель чудо-кнопок, щелкните на чудо-кнопке **Параметры (Settings)**.

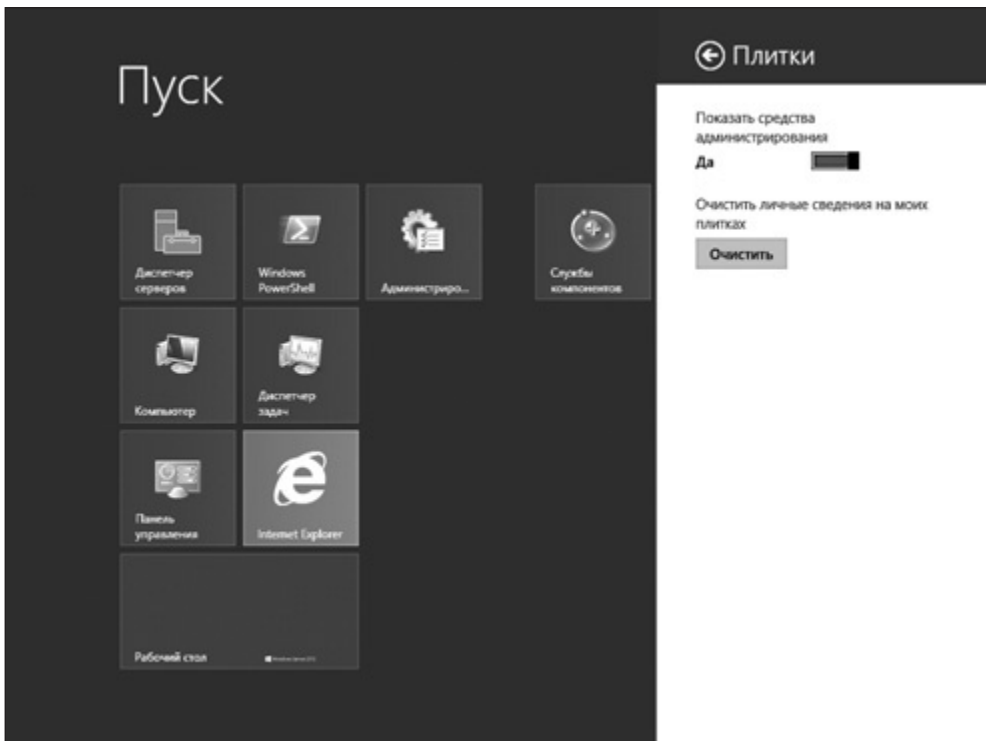


Рис. 3.11. Управление показом средств администрирования

В появившемся в нижней части экрана подменю вы увидите шесть значков, один из них называется **Выключение (Power)**. Если вы на нем щелкнете, появится меню, с помощью которого можно выключить или перезагрузить сервер.

Поиск

Поиск — одна из мощных и полезных возможностей Server 2012 с пользовательским интерфейсом. Для того чтобы найти приложение, достаточно перейти на начальный экран и начать вводить поисковый запрос. На экране результатов поиска будет отображен список найденных элементов. На рис. 3.12 показаны результаты поиска по запросу «task».

Вызвать интерфейс поиска можно и с помощью чудо-кнопки Поиск (Search). Так вы можете искать приложения, файлы и даже данные в Интернете.

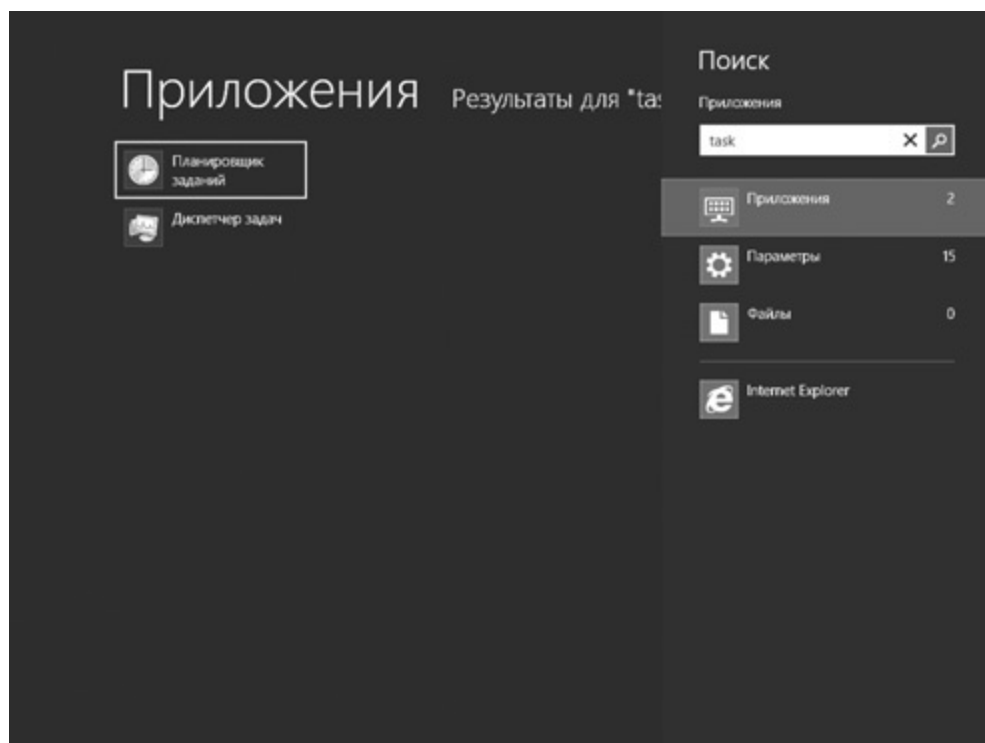


Рис. 3.12. Результаты поиска по запросу «task»

На Рабочем столе вы можете выполнять поиск так же, как в Server 2008 R2, открыв Проводник Windows с помощью ярлыка, закрепленного в панели задач, и введя запрос в поле Поиск (Search).

Диспетчер серверов

Диспетчер серверов (Server Manager) занимал важнейшее место в администрировании Windows Server с того момента, как он появился в Server 2008. Диспетчер серверов в графической оболочке сервера — это центральный узел выполнения множества административных задач.

В Server 2012 интерфейс диспетчера серверов обновлен, в него добавлено много новых возможностей. Управление несколькими серверами, в том числе возможность создания групп серверов и управления ими — одно из основных нововведений. В то время как в Server 2008 R2 вы могли подключаться

к другим серверам для того, чтобы управлять ими, в Server 2012 можете просто добавлять удаленные серверы в локальную консоль диспетчера серверов. Эта возможность упрощает управление серверами и делает его более эффективным.

Диспетчер серверов Server 2012 позволяет выполнять больше административных задач, чем в Server 2008 R2, и лучше контролировать инфраструктуру Windows. Консоль диспетчера серверов в реальном времени предоставляет сведения о развернутых серверах и серверных ролях. Управление серверами из консоли сводится к нескольким щелчкам мышью. То, что вы можете с одного взгляда оценивать состояние серверов и ролей и управлять ими, поможет уменьшить время, затрачиваемое на решение возникающих проблем.

IPAM (IP Address Management, система управления IP-адресами) — это новый компонент, доступный в диспетчере серверов Server 2012, который, в частности, рассмотрен в части сценариев развертывания в следующих главах этой книги. Сейчас, однако, наша основная задача заключается в запуске диспетчера серверов и выполнении некоторых предварительных действий, таких как развертывание серверных ролей и компонентов, использование обновленной системы BPA (Best Practice Analyzer, анализатора соответствия рекомендациям), добавление нескольких серверов и создание групп серверов.

Запуск диспетчера серверов и работа с ним

После того как вы входите в Server 2012 с пользовательским интерфейсом, автоматически запускается диспетчер серверов. Кроме того, вы можете запустить диспетчер серверов с Рабочего стола (соответствующий ярлык закреплен на панели задач) или с начального экрана (там имеется плитка Диспетчер серверов).

Интерфейс диспетчера серверов, основанный на плитках, показан на рис. 3.13. Самая большая плитка в его верхней части содержит ярлыки для вызова мастеров, которые позволяют настраивать локальный сервер.

Добавление серверных ролей и компонентов

Серверные роли — это отдельные функции, которые способен выполнять сервер. Обычные роли включают в себя DHCP, DNS, файловые службы

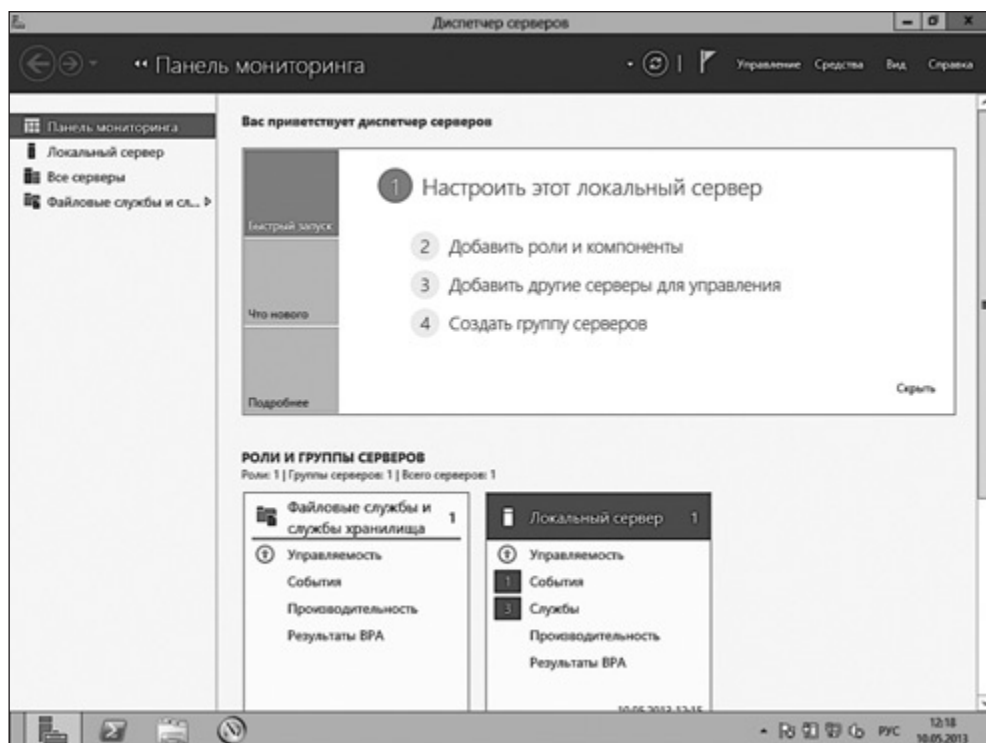


Рис. 3.13. Диспетчер серверов

(File Services) и IIS. В Server 2012 предусмотрены 19 серверных ролей. Компоненты расширяют серверные роли и часто требуются для развертывания ролей.

Для того чтобы добавить серверную роль, откройте диспетчер серверов и выберите команду **Добавить роли и компоненты** (Add roles and features), которая находится в группе **Настроить этот локальный сервер** (Configure this local server). Будет открыт мастер добавления ролей и компонентов (Add roles and features wizard) (рис. 3.14).

Щелкните на кнопке **Далее** (Next) и выберите тип установки. Здесь вы можете выбрать вариант установки либо ролей и компонентов, либо служб удаленных Рабочих столов (Remote Desktop Services) для развертывания узла сеансов удаленных Рабочих столов (Remote Desktop Session Host). Сейчас нас интересует добавление роли для отдельного сервера. Я выбрала вариант **Установка ролей или компонентов** (Role-based or feature-based installation) (рис. 3.15).

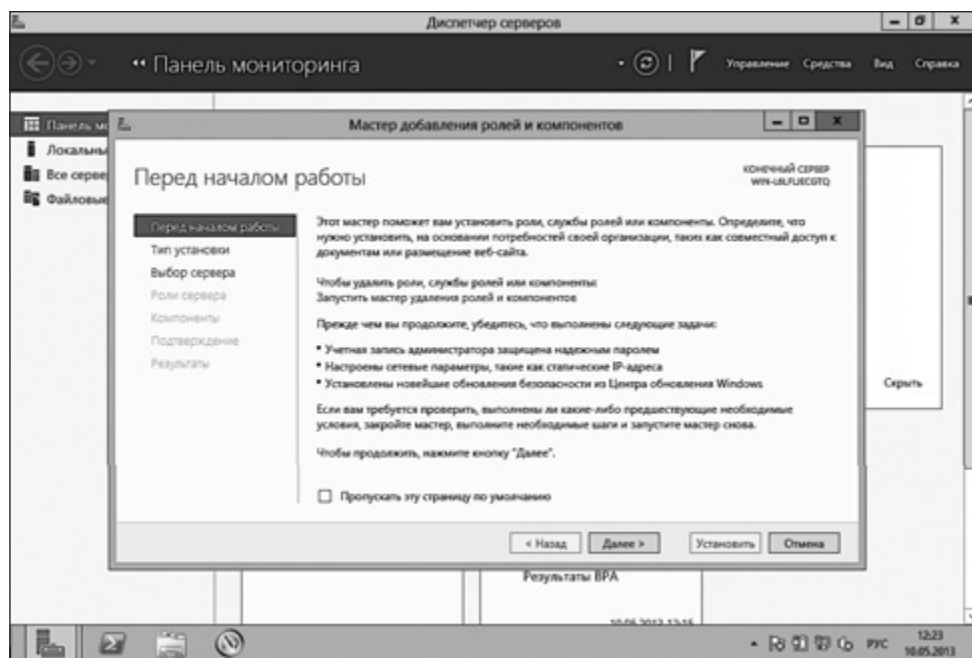


Рис. 3.14. Добавление ролей и компонентов

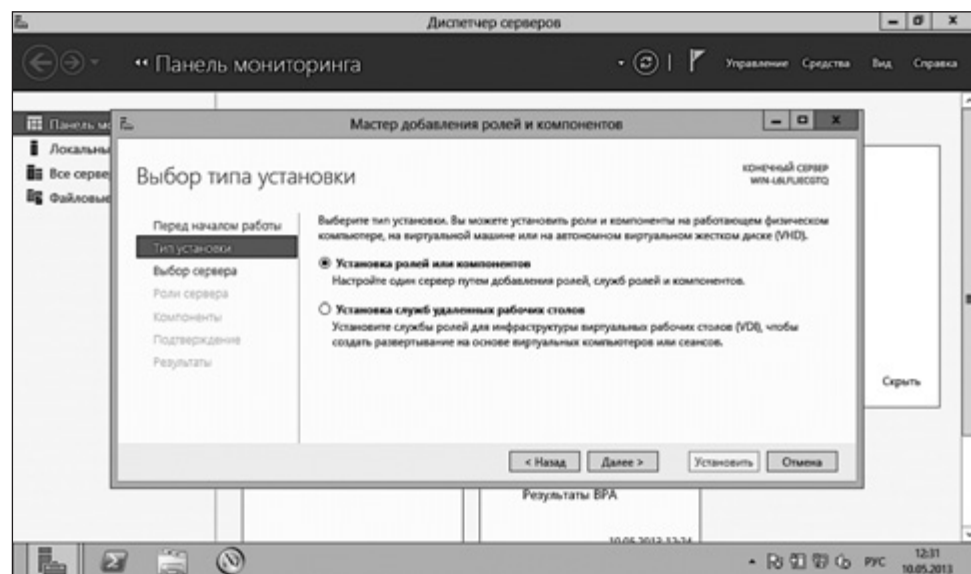


Рис. 3.15. Установка роли

Затем мастер предложит вам выбрать целевой сервер. Роли и компоненты можно разворачивать на локальном, удаленном или виртуализированном сервере. На рис. 3.16 показан выбор локального сервера в качестве целевого.

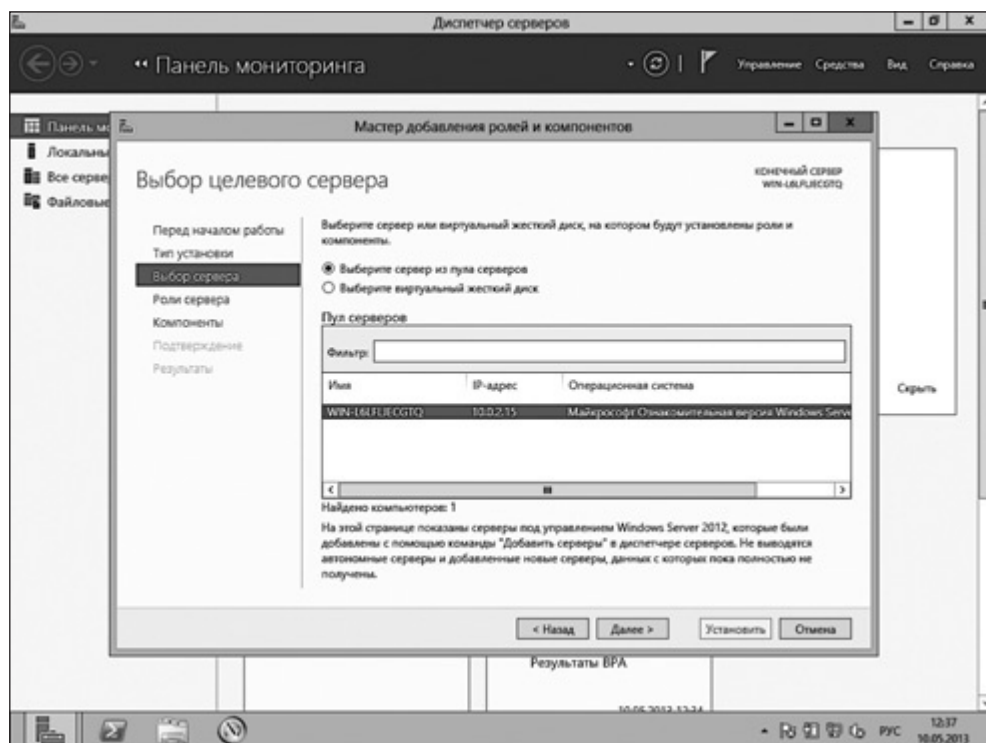


Рис. 3.16. Роль будет установлена на выбранном локальном сервере

Следующий шаг заключается в выборе роли или компонента, которые нужно установить. Я выбрала для установки на локальный сервер роль Службы Windows Server Update Services (сервер службы обновления Windows, WSUS) (рис. 3.17).

Список других компонентов и ролей, которые нужны для развертывания роли или компонента, будет автоматически показан при установке. Например, для установки роли IIS как части разворачиваемого WSUS-сервера вы должны будете установить компонент .NET Framework 4.5. Windows отобразит список компонентов, необходимых для установки роли, и позволит установить эти компоненты (рис. 3.18).

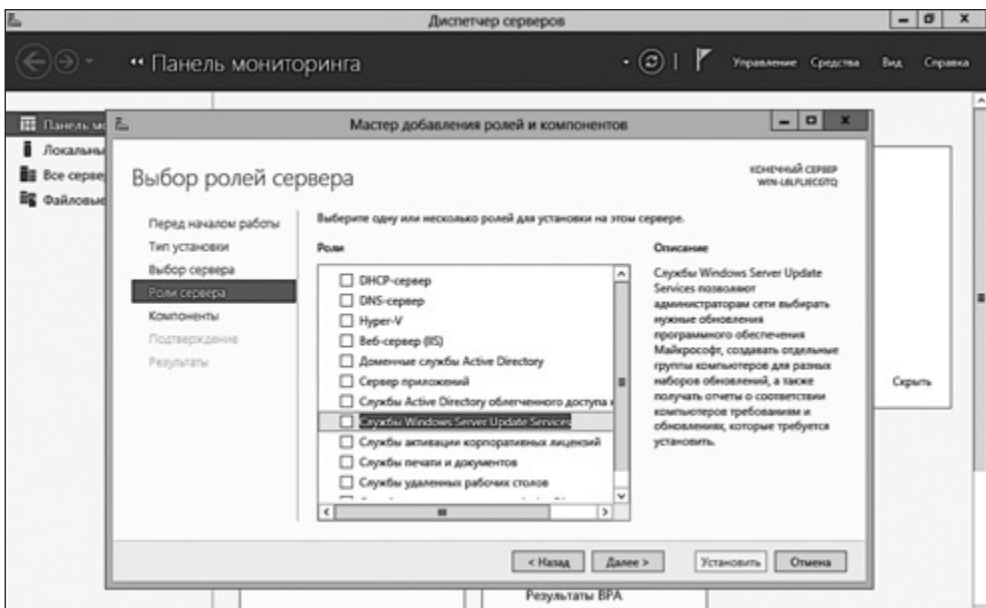


Рис. 3.17. Выбор роли WSUS

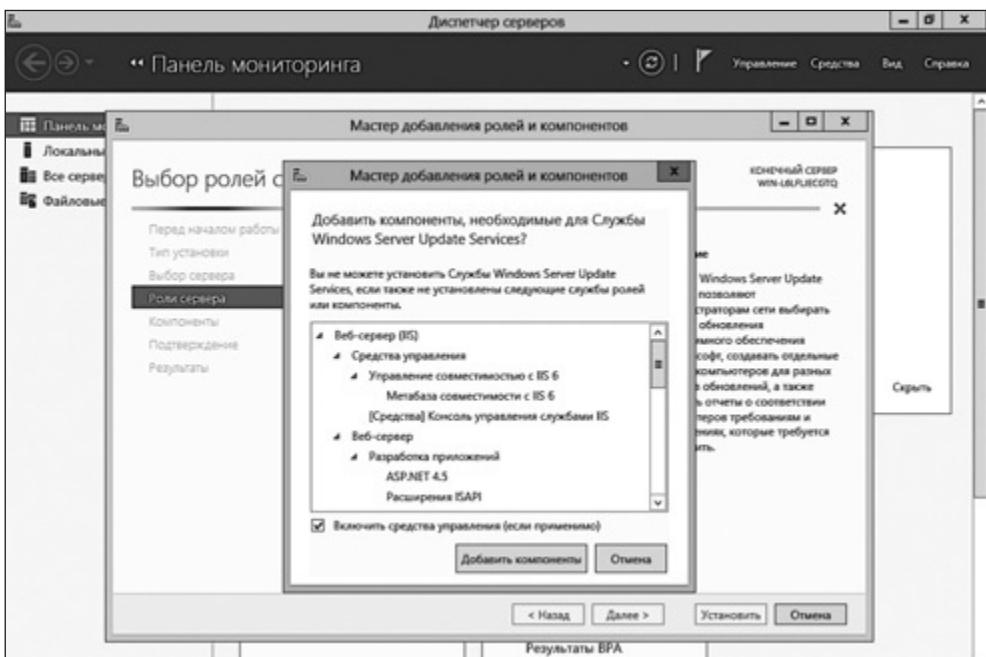


Рис. 3.18. Компоненты, необходимые для установки роли WSUS

Мастер выводит различные сведения об устанавливаемых компонентах, которые нужно знать администратору. Например, когда я добавляла серверные роли WSUS, мастер сообщил о том, что хотя бы один WSUS-сервер в сети должен иметь доступ к Интернету для загрузки обновлений Microsoft и что межсерверные, а также клиент-серверные соединения должны быть настроены с использованием SSL (Secure Socket Layer, защищенных соединений). На последнем шаге развертывания роли WSUS мне предложили выбрать, как следует хранить обновления — локально или удаленно (рис. 3.19).

Как показано на рис. 3.20, мастер предложит ознакомиться со списком устанавливаемого программного обеспечения и даст возможность установить флажок для автоматического перезапуска сервера, если это потребуется.

Нажмите кнопку Установить (Install), для того чтобы начать установку роли (рис. 3.21).

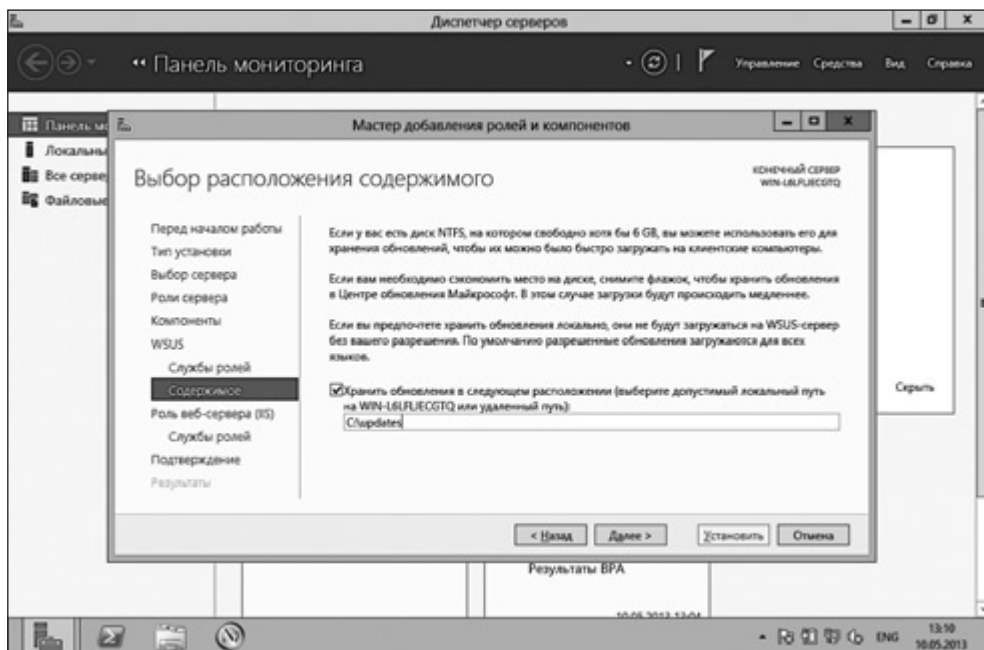


Рис. 3.19. Последний шаг настроек перед установкой роли WSUS

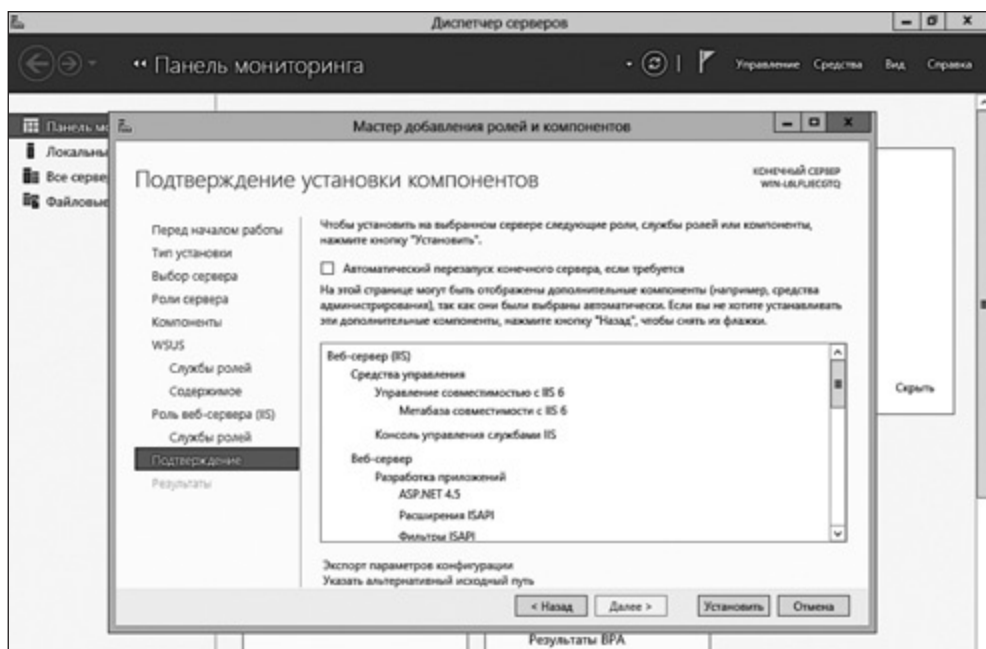


Рис. 3.20. Подтверждение

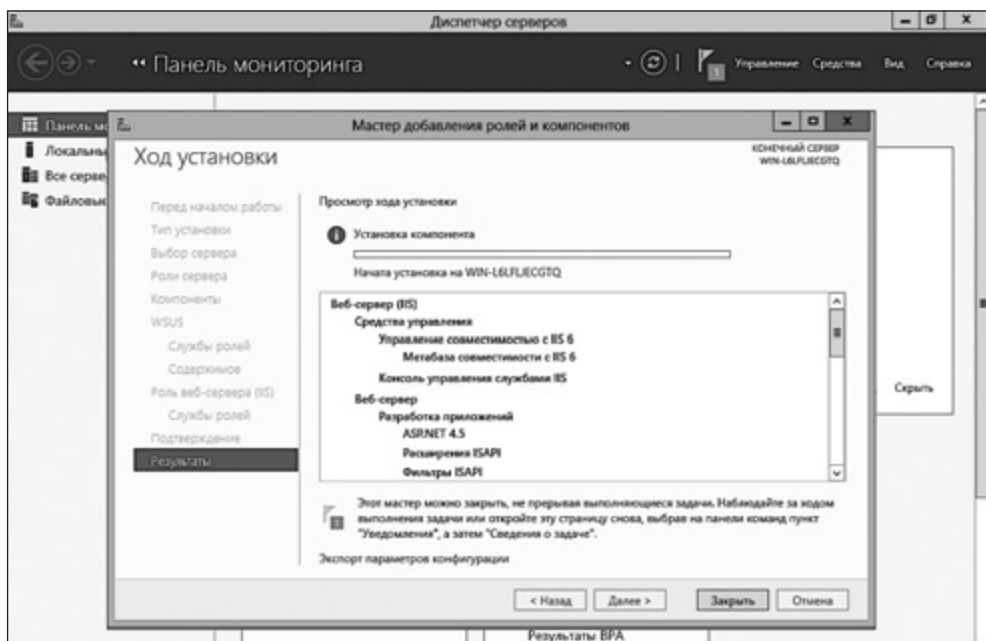


Рис. 3.21. Начало установки роли

После завершения установки в левой части консоли диспетчера серверов появятся два дополнительных элемента: IIS и WSUS (рис. 3.22).

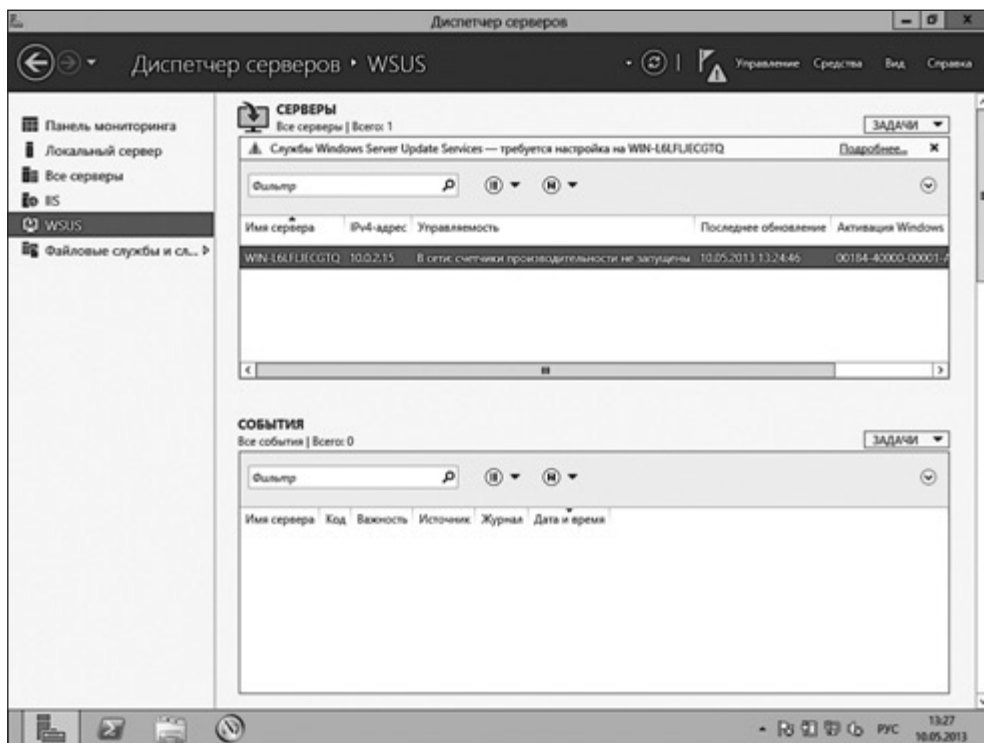


Рис. 3.22. Результат установки роли WSUS и необходимых для ее работы компонентов

Весьма полезная возможность диспетчера серверов в Server 2012 заключается в том, что он предоставляет сведения, необходимые для настройки только что установленной роли. Обратите внимание на треугольник с восклицательным знаком, что на рис. 3.22. Это уведомление указывает на то, что после установки роли WSUS нужно выполнить еще некоторые действия. Щелкнув на треугольнике, можно узнать подробности. После разворачивания роли WSUS, которую я установила, нужно выполнить некоторые настройки для обеспечения ее правильной работы. Уведомление предоставляет ссылку *Запуск послеустановочных задач* (Launch post-deployment tasks), которой можно воспользоваться для настройки только что добавленной роли.



Установленные роли добавляются в виде плиток на начальный экран для того, чтобы можно было быстро обращаться к ним вне диспетчера серверов.

Управление несколькими серверами и группами серверов

В предыдущих версиях Windows Server немало сложностей вызывало управление с одной консоли и локальным сервером, и удаленными серверами, например виртуализированными или расположенными в филиалах организации. Управление несколькими серверами — одна из заметных возможностей диспетчера серверов в Server 2012.

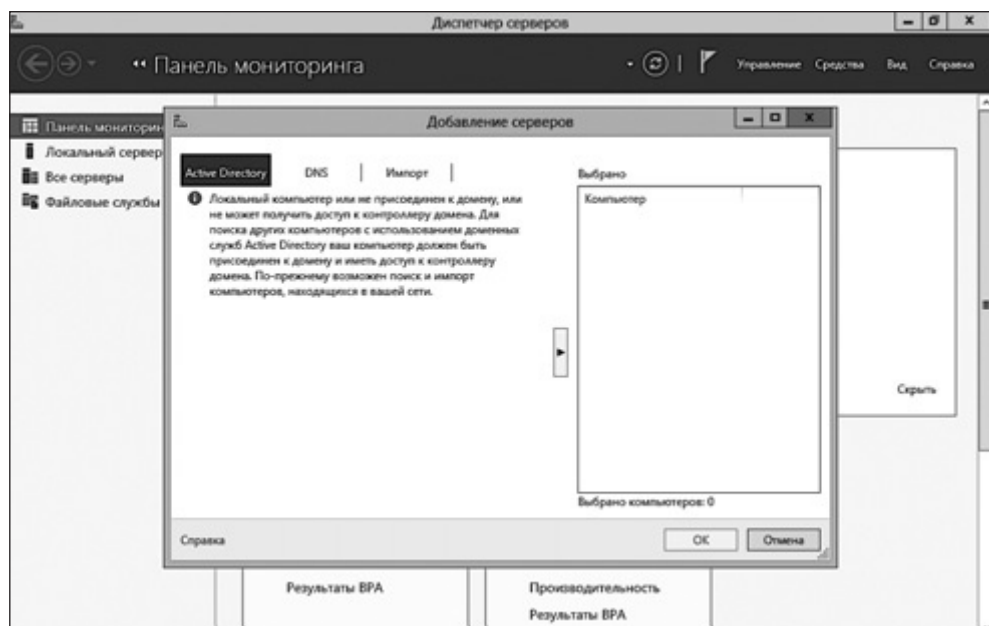
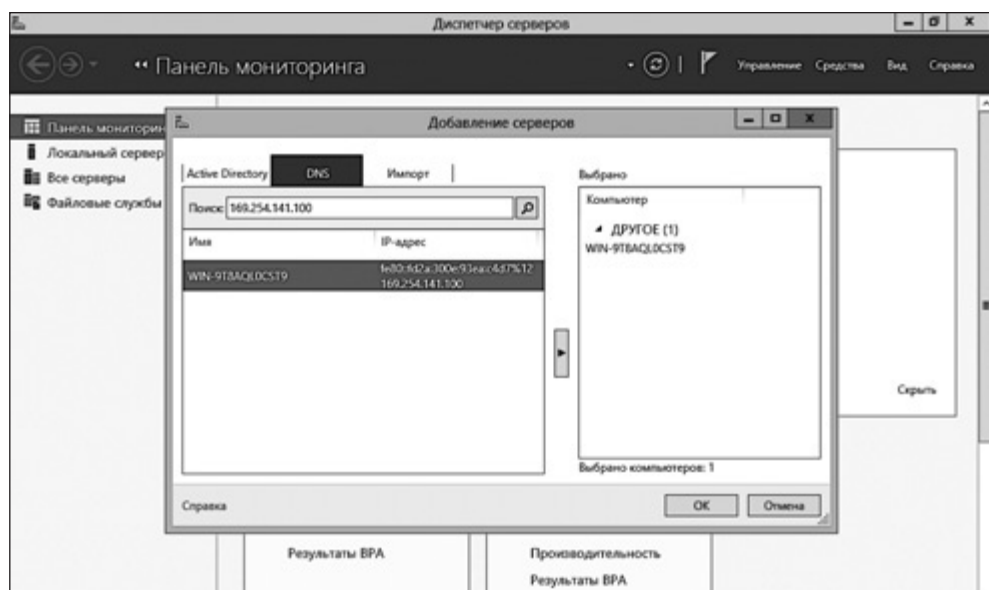
Для того чтобы добавить на панель мониторинга диспетчера серверов другие серверы, перейдите по ссылке **Добавить другие серверы для управления** (Add other servers to manage) в разделе **Настроить этот локальный сервер** (Configure this local server). Будет открыто окно мастера добавления серверов (Add Servers) (рис. 3.23).

Добавить компьютер, которым вы собираетесь управлять, можно, применив поиск по Active Directory, посредством DNS, используя сетевое имя сервера или его IP-адрес или импортировав *.txt*-файл, который содержит имена или IP-адреса серверов.

На рис. 3.24 показано добавление удаленного сервера Server 2012, развернутого на виртуальной машине. Сервер добавлен посредством DNS с использованием IP-адреса виртуального сервера. Как только сервер будет обнаружен, щелкните на кнопке со стрелкой, направленной вправо, для добавления его в список **Выбрано** (Selected). После этого нажмите **ОК**.

Добавление в диспетчер серверов предыдущих версий серверов

Компьютерами, работающими под управлением серверных ОС предыдущих версий, также можно управлять с помощью диспетчера серверов Server 2012. В частности, компьютеры под управлением ОС Server 2003, Server 2008 и Server 2008 R2 можно добавить в консоль диспетчера серверов теми

**Рис. 3.23.** Мастер добавления серверов**Рис. 3.24.** Добавление сервера под управлением Server 2012

же способами, которые мы рассмотрели ранее для Server 2012. Предыдущие версии операционных систем не поддерживают все возможности управления, которые имеются у Server 2012, однако наличие единой консоли упрощает управление серверами, на которых установлены разные версии ОС.

Удаленное управление Server 2012

Конечно, вы можете запустить диспетчер серверов локально с контроллера домена, но рекомендовано запускать графические инструменты управления с удаленного клиентского компьютера. Удаленный запуск ADAC, диспетчера серверов и других инструментов снижает нагрузку на сервер.

RSAT (Remote Server Administration Tool, средства удаленного администрирования сервера) включают в себя диспетчер серверов, оснастки MMC, консоли, командлеты Windows PowerShell и инструменты командной строки для управления ролями и компонентами, которые развернуты на Server 2012.

Вы можете использовать RSAT на Windows 8 для управления Server 2008 R2 или Server 2008, но в соответствии с рекомендациями Microsoft только в отдельных случаях. Для того чтобы избежать проблем, используйте соответствующие версии RSAT для различных версий серверов на различных клиентских системах.

Установка RSAT

RSAT для Windows 8-клиентов можно загрузить из центра загрузок Microsoft. Доступна как 32-, так и 64-разрядная версии. Прежде чем устанавливать RSAT, убедитесь в том, что любые другие версии инструментов администрирования или RSAT удалены с клиентского компьютера, если ранее они были там установлены.

Загрузите и установите файл *Windows6.2-KB2693643-x64.msu* для 64-разрядных систем или файл *Windows6.2-KB2693643-x86.msu* — для 32-разрядных (или более новые версии). После установки перейдите на начальный экран Windows 8 и щелкните на плитке **Администрирование** (Administrative tool) (рис. 3.25).



Рис. 3.25. Плитка Администрирование внизу в правом столбце

В папке Администрирование (Administrative Tools) находятся утилиты, которые необходимы для управления ОС Windows Server, в частности центр администрирования Active Directory (Active Directory Administrative Center), средство управления DNS (DNS Manager), DHCP и диспетчер серверов (Server Manager) (рис. 3.26).

На рис. 3.27 диспетчер серверов открыт на Windows 8-клиенте, который присоединен к тому же домену, что и компьютер под управлением Server 2012. Нажмите Управление (Manage) в правом верхнем углу меню диспетчера серверов, выберите в появившемся меню пункт Добавление серверов (Add servers), для того чтобы добавить в консоль серверы, которыми вы хотите управлять.

Вы можете выполнять поиск серверов с помощью Active Directory, с помощью DNS или импортируя сведения о серверах в виде файла. На рис. 3.28 показан результат поиска всех серверов домена.

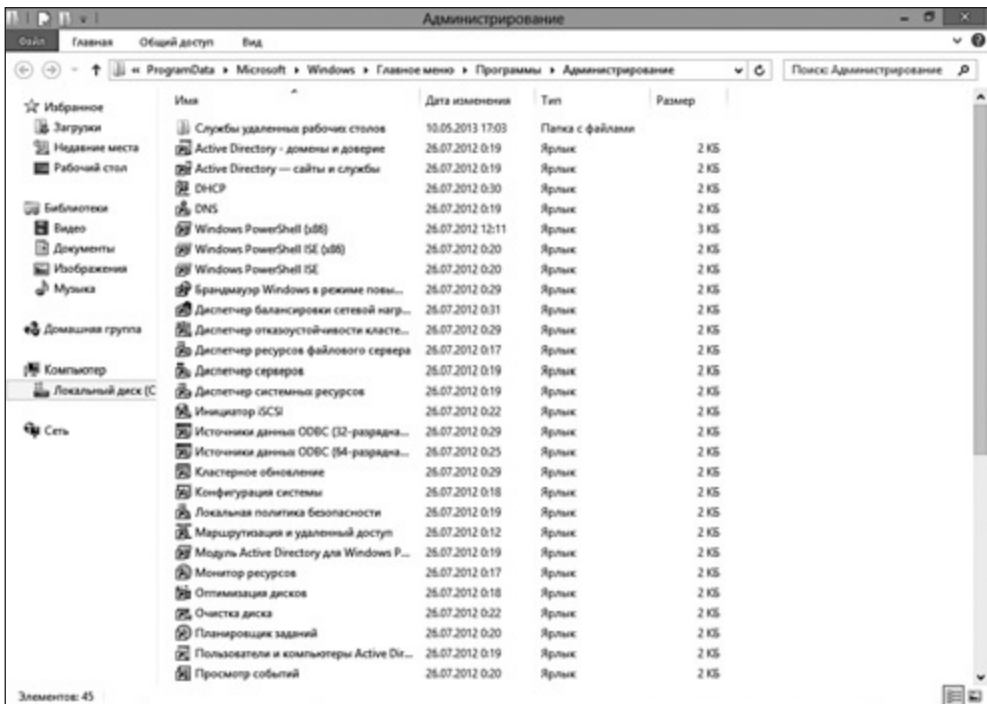


Рис. 3.26. Папка Администрирование

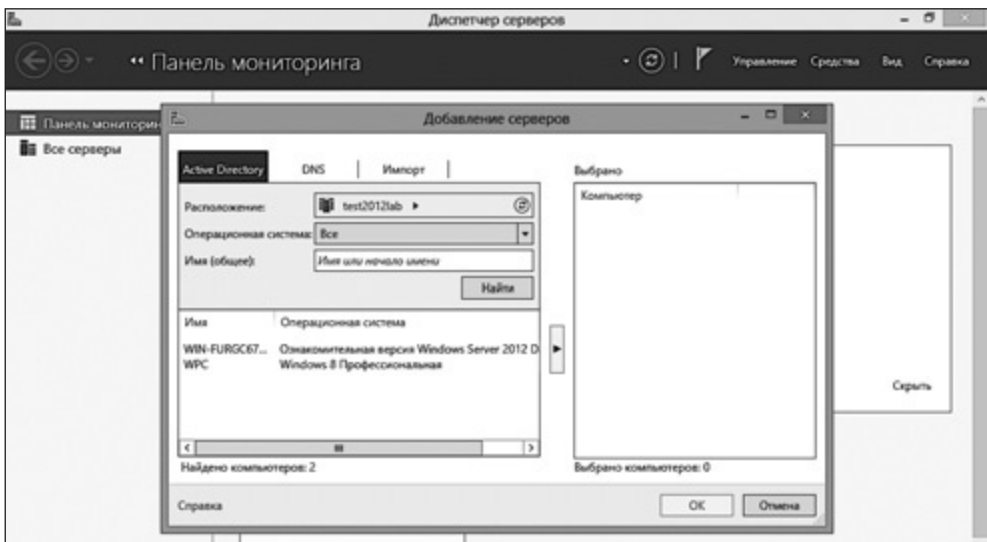


Рис. 3.27. Диспетчер серверов запущен на клиентском компьютере с установленной Windows 8

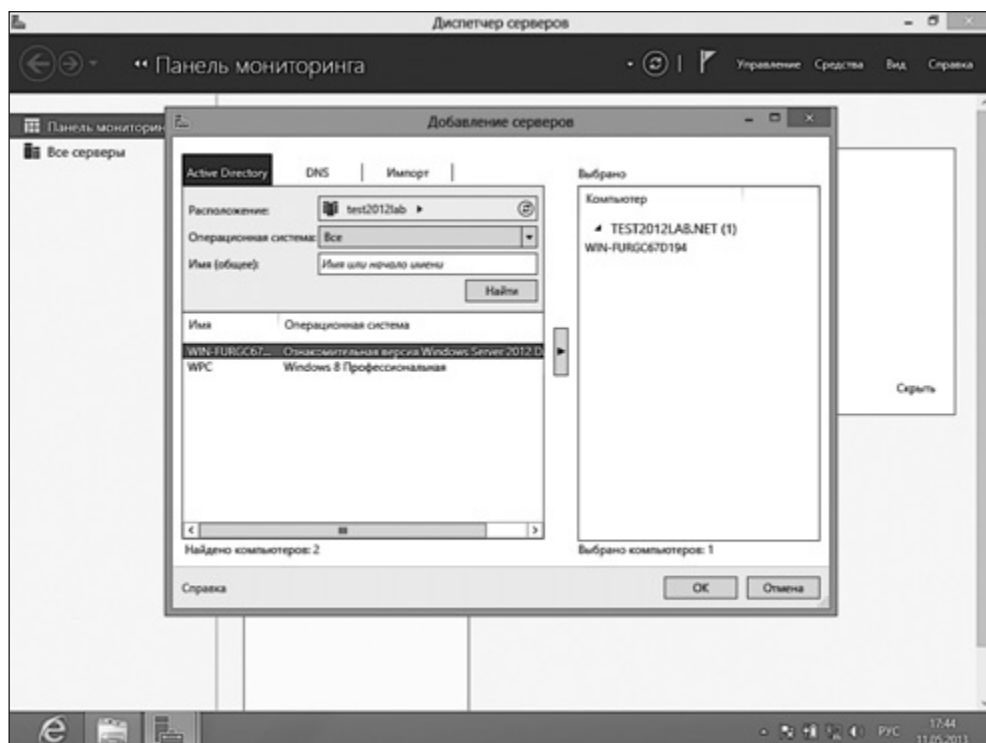


Рис. 3.28. Поиск и добавление сервера для управления

Выберите сервер и щелкните на кнопке со стрелкой, направленной вправо, для того чтобы добавить сервер (или серверы) в консоль. Как только вы добавите сервер, все роли и компоненты, развернутые на нем, отобразятся в клиентском экземпляре диспетчера серверов, как если бы вы запустили диспетчер серверов на локальном сервере.

Выводы

Диспетчер серверов — это сердце системы управления Windows Server 2012. С диспетчером серверов, обладающим понятным и современным интерфейсом, не только приятно работать. Вдобавок он дает администратору средства для управления всей инфраструктурой Windows.

Поскольку вы можете добавлять Server 2012 в существующие домены, основанные на предыдущих версиях серверных ОС от Microsoft, равно как и отслеживать состояние серверов более ранних выпусков из диспетчера серверов, самая свежая серверная ОС от Microsoft по-настоящему вписывается в реальную смешанную среду Windows, которую можно обнаружить в большинстве организаций.

Приложения для управления, созданные для Server 2012, помогают расширить возможности управления. И наконец, вы можете очень просто управлять Server 2012 с помощью инструментов, имеющих пользовательский интерфейс и запущенных на клиентских компьютерах с использованием технологии RSAT.

4

Active Directory

Возможно, ни один из механизмов Windows-окружения не вызывает столько беспокойства и разочарований, не отнимает столько времени IT-специалистов, как Active Directory (AD). Active Directory впервые была представлена в Windows Server 2000 и входила во все последующие выпуски Windows Server. В Windows Server 2012 включена самая совершенная на текущий момент версия Active Directory. Одна из важнейших причин, по которой данная версия AD может считаться лучшей, — это развертывание доменных служб Active Directory (Active Directory Domain Services, AD DS), содержащее теперь в едином интерфейсе новый мастер установки доменных служб Active Directory (Active Directory Domain Services Wizard), все шаги которого необходимы для развертывания нового контроллера домена.

Кроме того, AD DS в Server 2012 легче управлять благодаря расширенному мастеру, построенному на основе PowerShell, который интегрирован с диспетчером серверов. Проверка перед установкой, выполняемая с помощью инструмента *Adprep.exe*, и предварительная проверка системных требований являются частью процесса установки, что помогает уменьшить вероятность возникновения ошибок при развертывании AD DS.

Означают ли эти улучшения, что развертывание и управление AD в Server 2012 стало совершенно безупречным? По некоторым причинам — нет. Развертывая AD в Server 2012 впервые, я столкнулась с ошибками и предупреждениями, говорящими о необходимости добавления некоторых компонентов

или об особой настройке тех или иных механизмов, необходимых для успешной установки AD.

Однако эти уведомления и сообщения об ошибках отображались автоматически, мне не пришлось охотиться за ними, используя средство Просмотр событий (Event Viewer) для поиска предупреждений, имеющих отношение к AD, как обычно приходилось делать в Server 2008 R2 и более старых версиях Windows Server. В процессе установки в обновленном диспетчере серверов выводятся предупреждения, сообщения об ошибках и советы по подготовке сервера к запуску AD. Весь процесс развертывания AD сосредоточен в диспетчере серверов, что повышает эффективность работы и упрощает решение проблем.

В этой главе вы узнаете о новом интерфейсе центра администрирования Active Directory (Active Directory Administrative Center, ADAC). Кроме того, я расскажу о развертывании AD DS и об управлении этой службой, о том, как подключить Server 2012 к существующему домену и, наоборот, подключить компьютер под управлением Server 2012 к домену Server 2008 R2.

Эта глава посвящена также использованию новых и обновленных возможностей AD, таких как использование корзины Active Directory (AD Recycle Bin) для восстановления удаленных объектов. Кроме того, здесь мы поговорим о поиске по Active Directory, о развертывании AD с помощью PowerShell и об удаленном управлении Server 2012.

Развертывание доменных служб Active Directory

Поскольку в Server 2012 обновлен интерфейс диспетчера серверов и средств управления Active Directory, процесс установки окажется новым даже для тех, кто раньше уже устанавливал доменные службы Active Directory (Active Directory Domain Services, AD DS). Перед установкой доменных служб Active Directory убедитесь в том, что в сети функционирует DNS-сервер, иначе вам будет предложено установить его после установки AD.

Установка Active Directory

Для установки AD DS на локальном компьютере с установленным Server 2012 запустите диспетчер серверов и выберите команду **Добавить роли**

и компоненты (Add roles and features), которая находится на панели мониторинга в группе Настроить этот локальный сервер (Configure this local server).

Выберите Установка ролей или компонентов (Role-based or feature-based installation) и нажмите Далее (Next). Затем выберите в списке серверов локальный сервер (или тот сервер, на котором вы хотите развернуть AD DS) в качестве целевого. Выберите Доменные службы Active Directory (рис. 4.1).

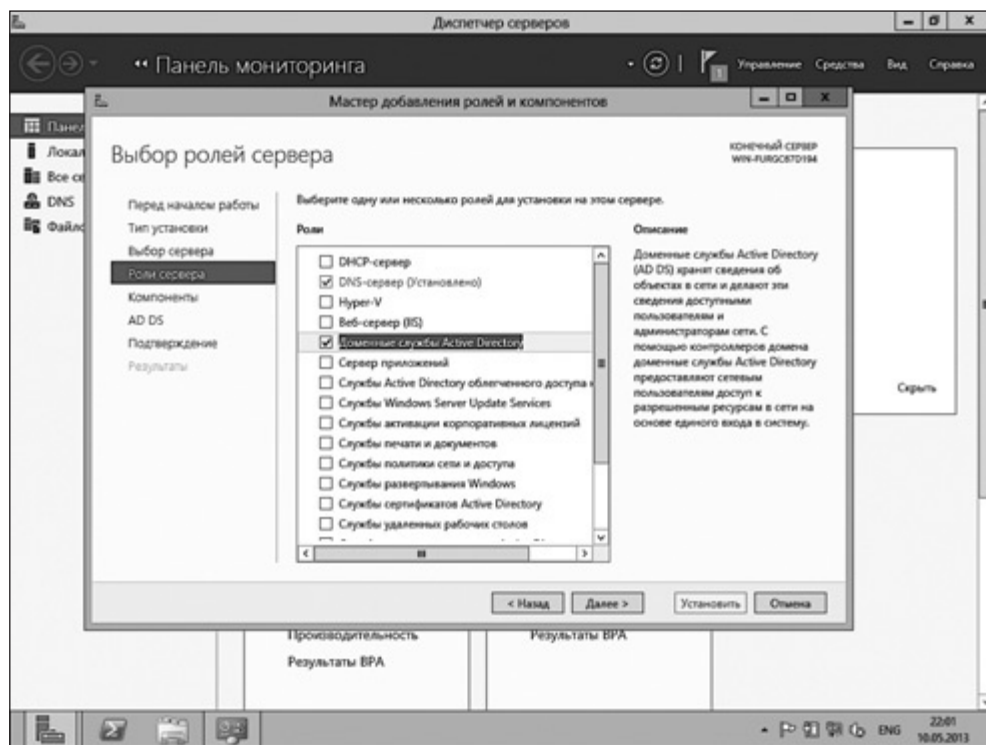


Рис. 4.1. Выбор доменных служб Active Directory

Вместе с установкой AD DS нужно установить еще некоторые компоненты. Вам будет предложен их список, можете установить и их. Для того чтобы это сделать, нажмите в появившемся окне со списком компонентов кнопку Добавить компоненты (Add features), после чего нажмите кнопку Далее (Next).

На данном этапе вы можете либо выбрать дополнительные компоненты для установки, либо просто еще раз нажать кнопку Далее (Next), для того чтобы начать установку (рис. 4.2).

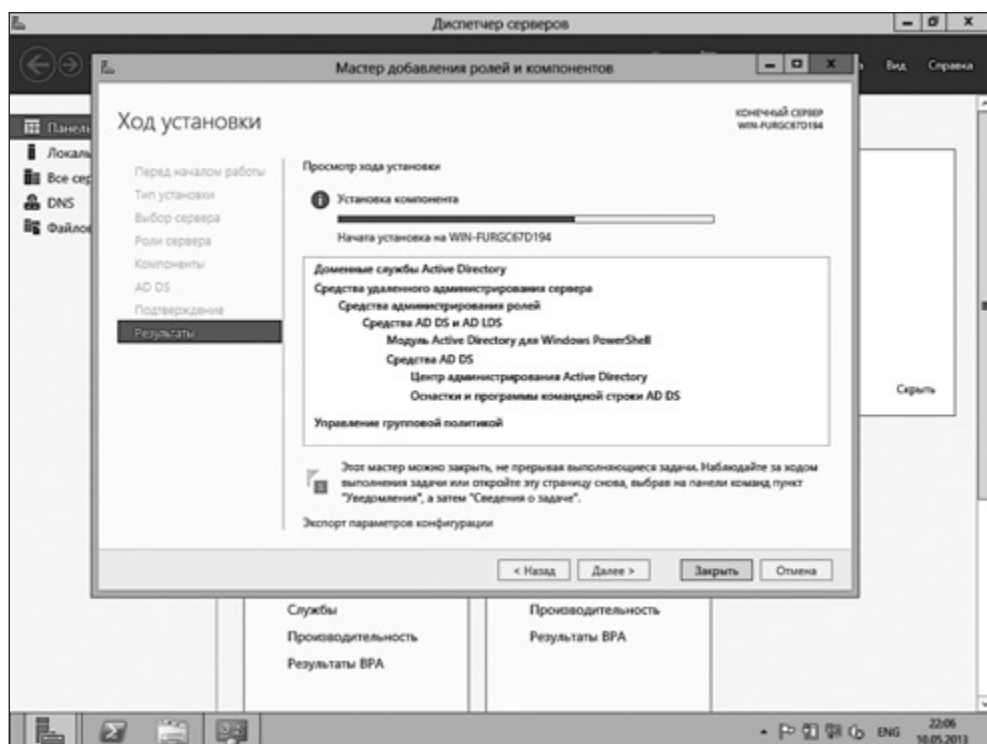


Рис. 4.2. Начало установки AD DS

После успешной установки в уведомлении диспетчера серверов вам будет предложено Повысить роль этого сервера до уровня контроллера домена (Promote this server to a domain controller) (рис. 4.3).



Конечно, вы можете не начинать работу с добавления серверов в качестве контроллеров домена (Domain Controller, DC). У большинства читателей, вероятнее всего, уже есть развернутый DC. Из соображений безопасности вы можете добавить в свою сетевую инфраструктуру сервер, работающий под управлением Server 2012, в качестве физического или виртуального DC или как DC только для чтения. Прежде чем повышать роль любого нового сервера под управлением Server 2012 до уровня контроллера домена, подумайте о существующей инфраструктуре и о том, какую роль этот сервер должен в ней играть.

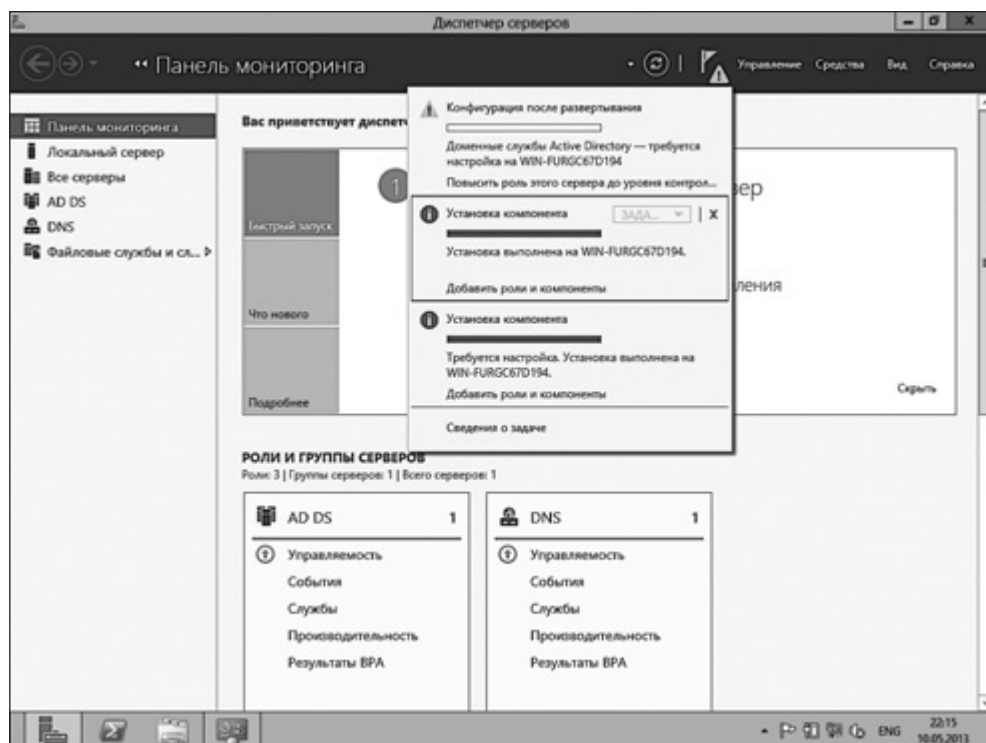


Рис. 4.3. Оповещение о необходимости повышения роли сервера до уровня контроллера домена

Есть несколько способов повышения роли сервера до уровня DC. Вы можете использовать либо инструменты с графическим интерфейсом, либо PowerShell. Существует заблуждение, что Microsoft не включила в поставку Server 2012 утилиту Dsromo, которую системные администраторы уже очень давно используют для повышения ролей серверов до уровня DC.

Dsromo можно пользоваться в Server 2012. Вы можете запустить это средство, используя команду `dsromo.exe` в командной строке и указав при этом файл ответов (answer file). Файл ответов — это текстовый файл, в который входят определенные поля, позволяющие настроить автоматическую процедуру повышения роли сервера до уровня DC на основании конфигурации, необходимой конкретной организации.

Повышение роли сервера до уровня DC с использованием Dsromo и файла ответов оправдано лишь в том случае, если в организации уже применяются подобные средства автоматизации для создания контроллеров домена либо

для инфраструктур, в которых нужно развернуть несколько контроллеров домена. В небольших организациях гораздо легче и эффективнее использовать функции установки контроллера домена и управления его полномочиями, встроенные в диспетчер серверов. При использовании этих средств снижается вероятность ошибок, в частности, тех, причиной которых являются синтаксические ошибки в файле ответов. Тот, кому удобно работать со сценариями, может воспользоваться PowerShell в качестве альтернативного инструмента для создания контроллеров домена и управления их полномочиями.

Центр администрирования Active Directory (Active Directory Administrative Center) позволяет добавить контроллер домена в существующий домен, добавить новый домен в существующий лес или создать новый лес. Для того чтобы настроить совершенно новый домен с созданием нового леса, следует в начале настройки доменных служб Active Directory выбрать в качестве операции развертывания **Добавить новый лес** (Add a new forest) (рис. 4.4).

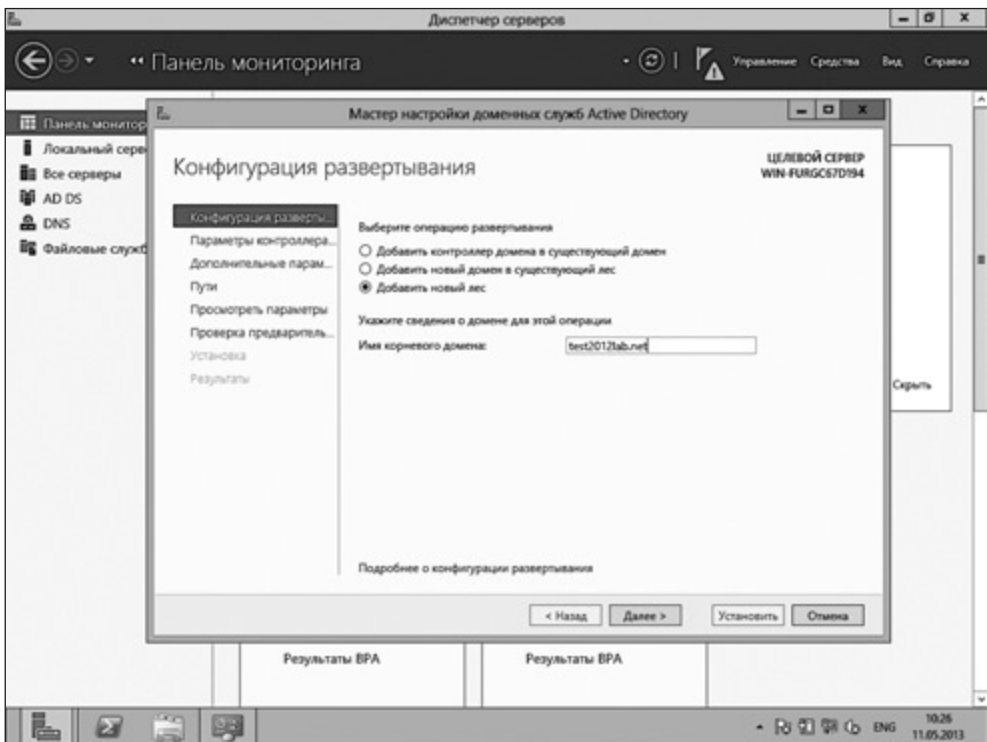


Рис. 4.4. Добавление нового леса

Здесь вы также должны указать корневое доменное имя в виде, например, <имя_домена>.com или <имя_домена>.net или любой домен верхнего уровня (top-level domain, TLD), назначенный вашей организации.

Далее нужно указать режим работы леса и домена. Режим работы, который вы выберете, зависит от того, имеется ли у вас другой контроллер домена или лес, и от того, какие серверы вы используете. Например, если в вашей инфраструктуре есть серверы, работающие под управлением ОС Server 2003, можете остановиться на режиме работы леса или домена Windows Server 2003 до тех пор, пока все контроллеры домена не будут обновлены до Server 2008 или 2008 R2.

В частности, режим работы Server 2012 может быть установлен как Server 2012, Server 2008 R2, Server 2008 или Server 2003. Если к тому же планируется, что контроллер домена будет выполнять роль сервера глобального каталога или контроллера домена только для чтения, можете указать на данном шаге

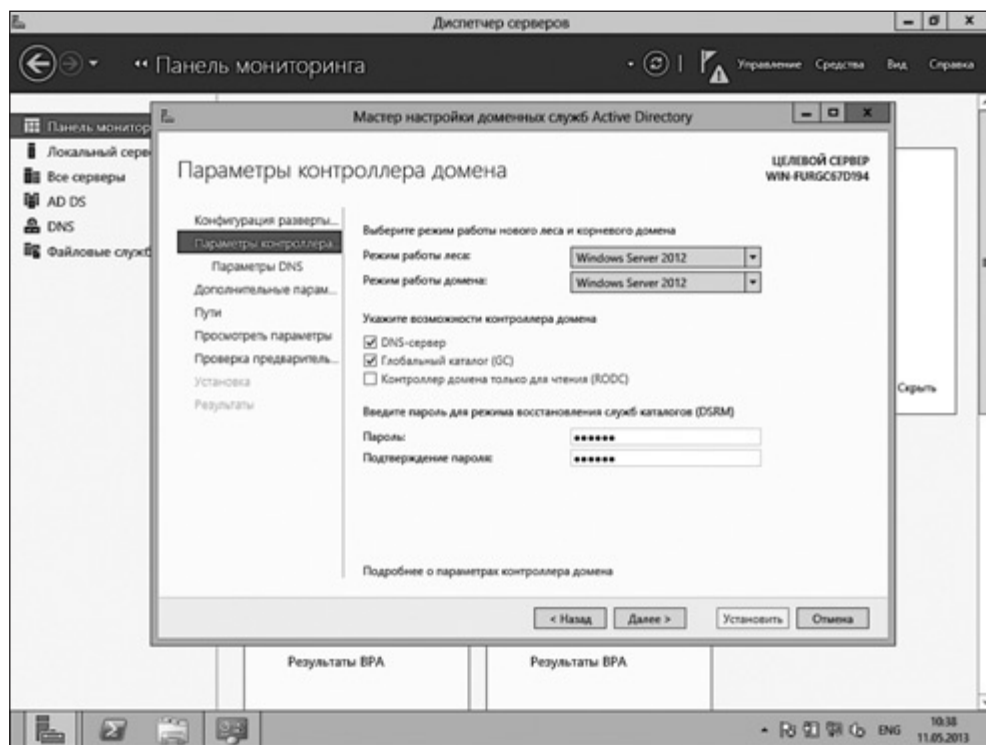


Рис. 4.5. Настройка режима работы домена

эти настройки. Важно, чтобы при добавлении нового контроллера домена не произошло незапланированного обновления существующего домена. Поэтому, если вы присоединяете сервер к существующему домену, внимательно читайте инструкции, предоставляемые мастером.

На следующем экране (рис. 4.5) нужно задать пароль для режима восстановления служб каталогов (Directory Service Restore Mode, DSRM).

Перед завершением установки будет автоматически выполнена проверка предварительных требований к системе, для того чтобы при установке AD не возникло проблем (рис. 4.6).

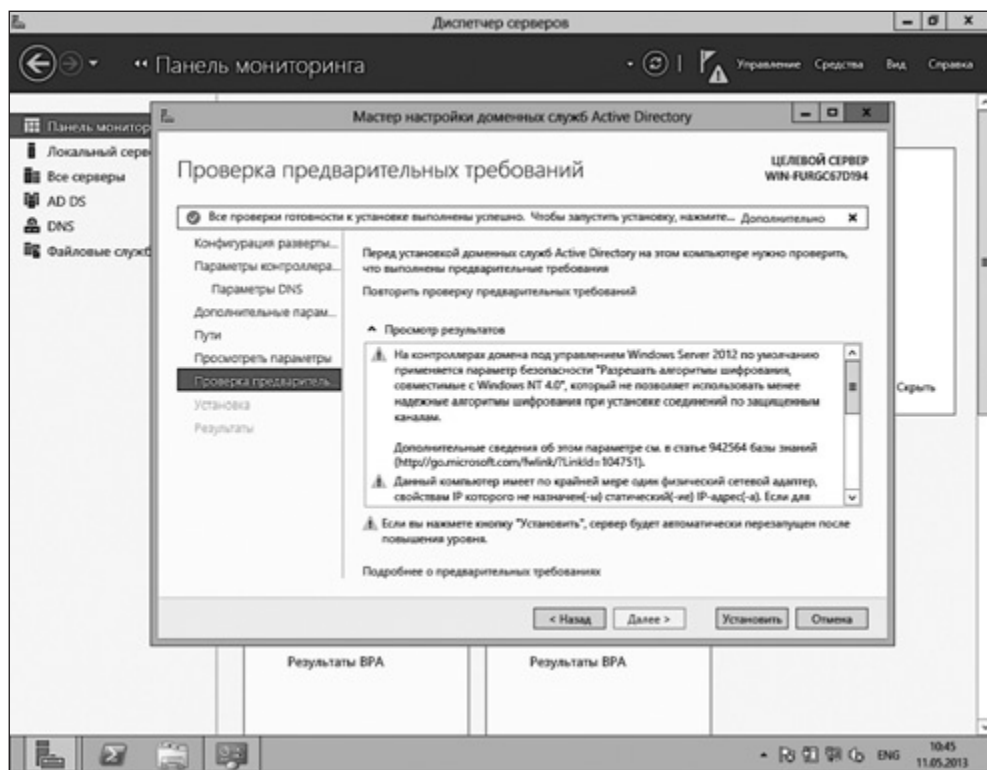


Рис. 4.6. Результаты проверки предварительных требований

После успешной установки AD DS будет доступна на панели мониторинга (рис. 4.7).

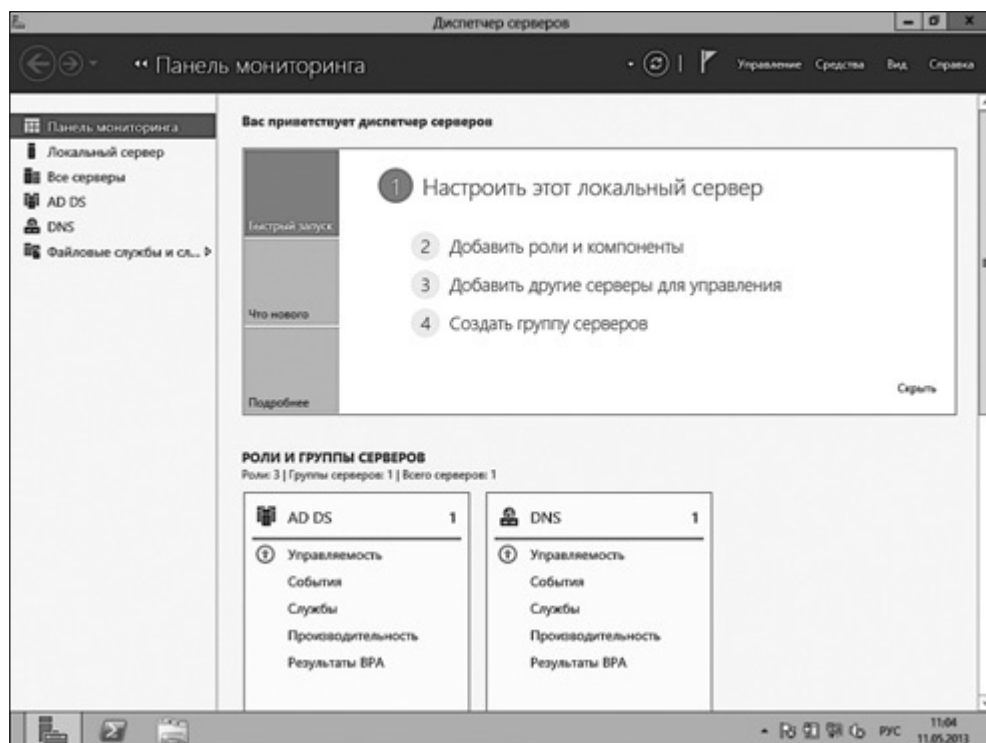


Рис. 4.7. Успешная установка AD DS

Добавление компьютеров к домену Server 2012

Обычно IT-специалисты сначала обновляют серверы, а уже потом — клиентские компьютеры или просто заменяют устаревшие машины новыми, на которых установлены последние версии клиентских ОС Windows. Вполне возможно, что в некоторых организациях к доменам Server 2012 будут подключать не только компьютеры под управлением Windows 8, но и системы с установленной Windows 7 (а иногда и с Windows XP).

В крупных организациях клиентские компьютеры и серверы можно присоединить к домену с использованием автоматизированных методов, таких как

использование сценариев и пакетных файлов. В этом разделе сосредоточимся на подключении к домену с применением интерфейса клиентской системы. Обычно этот метод используют в небольших сетях. Данная методика работоспособна и на виртуальных машинах.

Подключение к домену Server 2012 компьютера, работающего под управлением Windows 7

В панели управления (Control Panel) Windows 7 в разделе Система (System) откройте окно Свойства системы (System properties), перейдите в нем на вкладку Имя компьютера (Computer Name) и нажмите кнопку Изменить (Change) (рис. 4.8).

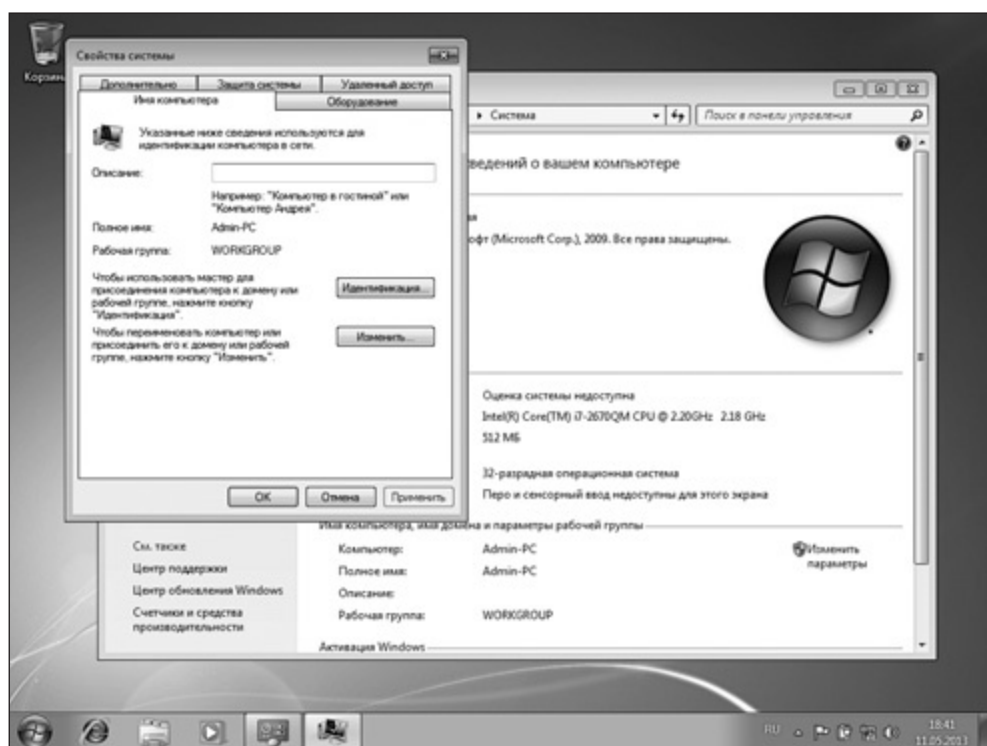


Рис. 4.8. Окно Свойства системы в Windows 7

Введите имя домена в поле домена (Domain) переключателя Является членом (Member of) (рис. 4.9).

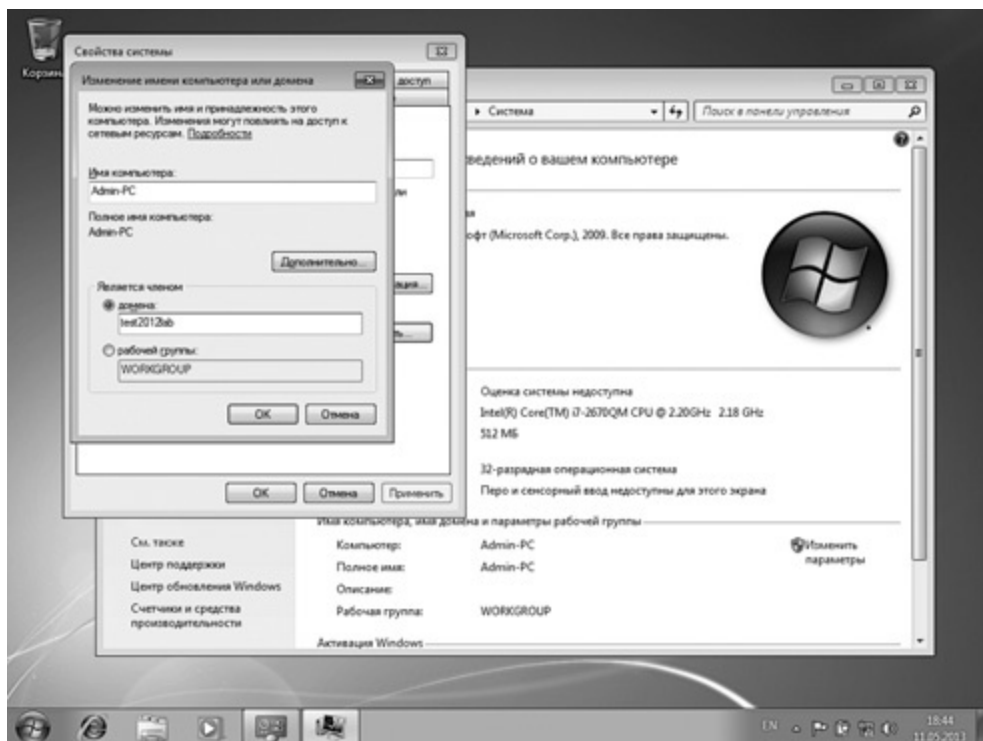


Рис. 4.9. Ввод имени домена

Введите учетные данные пользователя, имеющего разрешение на подключение компьютеров к домену. После того как компьютер будет успешно подключен к домену, появится соответствующее сообщение (рис. 4.10).

Как только клиентский компьютер присоединится к домену, вы сможете найти его в контейнере Computers (Компьютеры) центра администрирования Active Directory (ADAC) (рис. 4.11).

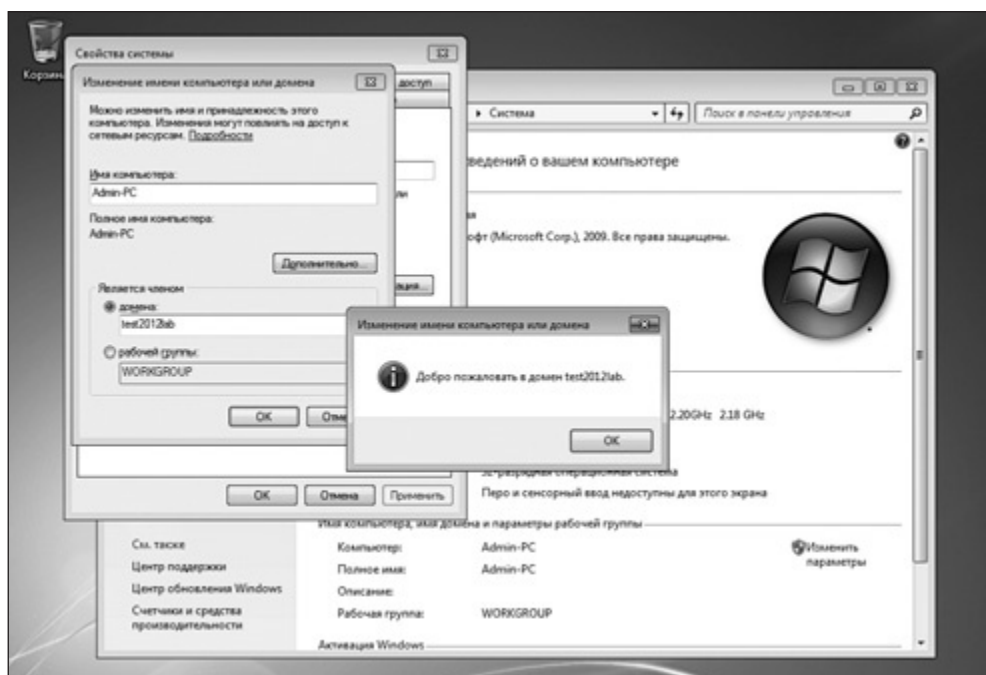


Рис. 4.10. Успешное присоединение к домену



Рис. 4.11. Запись о компьютере, подключившемся к домену, появилась в ADAC

Добавление компьютеров под управлением Windows 8 к домену Server 2012

С тех пор как была выпущена версия Windows 8 Consumer Preview, вокруг клиентских систем на Windows 8 возникает множество споров, их подвергают критике. Многим кажется, что эта операционная система больше похожа на платформу мобильных устройств для обычных пользователей, чем на систему, ориентированную на бизнес-цели. Однако приход Windows 8 в корпоративную среду неизбежен, и в первую очередь благодаря ее новым возможностям. Я помню себя администратором Windows Server, пытающимся подключить последнюю версию клиентской операционной системы к домену только потому, что некоторые руководители высшего звена хотели попробовать поработать с новой ОС!

У меня есть для вас и хорошие новости о подключении Windows 8 к корпоративным доменам, и не очень хорошие. Мобильные устройства, оснащенные ARM-процессорами, на которые установлена Windows 8, так называемая Windows RT, официально не могут быть присоединены к домену Windows. Это не означает, что вы не можете подключать мобильные устройства на Windows RT к сетевой инфраструктуре организации. Для этой цели можно использовать как собственные возможности ОС, так и средства сторонних разработчиков для управления мобильными устройствами (Mobile Device Management, MDM).

Однако вы можете подключать к доменам компьютеры и виртуальные машины с установленной Windows 8. Для того чтобы подключить компьютер с установленной Windows 8 к домену уровня Server 2012, достаточно выполнить те же действия, которые выполняются при подключении к домену Windows 7-клиентов. Откройте панель управления (Control Panel), войдите в раздел Система и безопасность (System and Security). Далее перейдите в раздел Система (System) и щелкните на ссылке Дополнительные параметры системы (Advanced system settings).

В появившемся окне перейдите на вкладку Имя компьютера (Computer Name) и нажмите кнопку Изменить (Change). Введите имя домена в соответствующее поле. Как только компьютер будет подключен к домену, его можно будет найти в контейнере Компьютеры (Computers) в ADAC.

Для подключения к домену Sever 2012 систем, работающих под управлением Server 2003, 2008 и 2008 R2, в качестве обычных серверов можно

воспользоваться той же процедурой, которая используется для подключения клиентских Windows-систем.

Обновленный интерфейс диспетчера серверов в Server 2012 позволяет вам быстро добавлять в домен компьютеры под управлением Server 2012. Для того чтобы это сделать, достаточно открыть диспетчер серверов, щелкнуть на ссылке Настроить этот локальный сервер (Configure this local server). В группе параметров Свойства (Properties) нужно щелкнуть на пункте WORKGROUP (рис. 4.12).

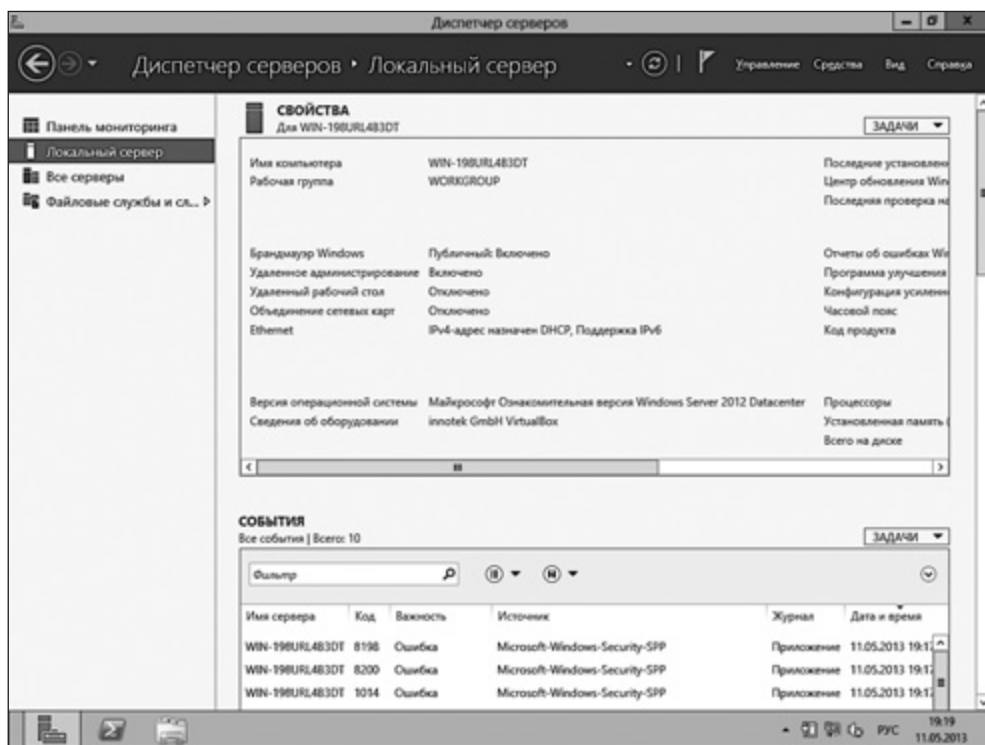


Рис. 4.12. Щелкните WORKGROUP для добавления компьютера под управлением Server 2012 к домену

Щелчок WORKGROUP приведет к открытию окна Свойства системы (System Properties), с помощью которого вы можете добавить сервер к домену (рис. 4.13).

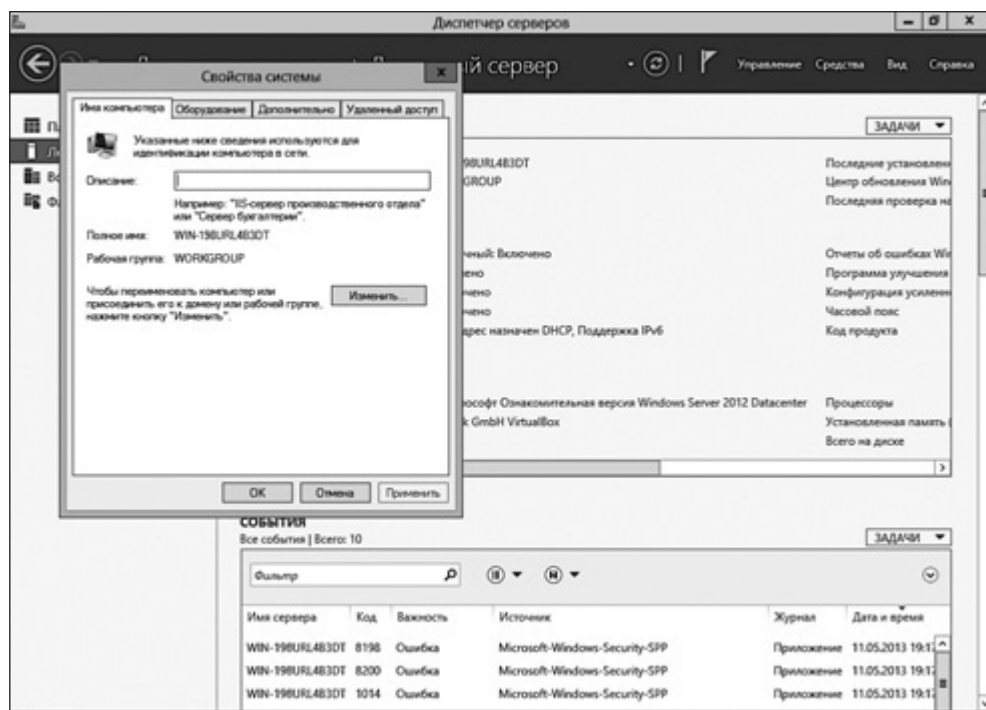


Рис. 4.13. Нажмите Изменить для добавления сервера к домену

Добавление систем под управлением Server 2012 к домену уровня функциональности Server 2008 R2

Вы можете добавлять компьютеры под управлением Server 2012 к доменам Active Directory другого уровня функциональности, хотя подобное смешанное окружение не обладает преимуществами Server 2012-доменов.

Для того чтобы добавить компьютер под управлением Server 2012, например, к домену Server 2008 R2, откройте диспетчер серверов (Server Manager), нажмите Настроить этот локальный сервер (Configure this local server). В группе параметров Свойства (Properties) щелкните на пункте WORKGROUP. В окне свойства системы (System Properties) добавьте сервер к домену 2008 R2 (рис. 4.14).

После добавления к домену компьютер, работающий под управлением Server 2012, появится в контейнере Computers (Компьютеры) в Server 2008 R2.

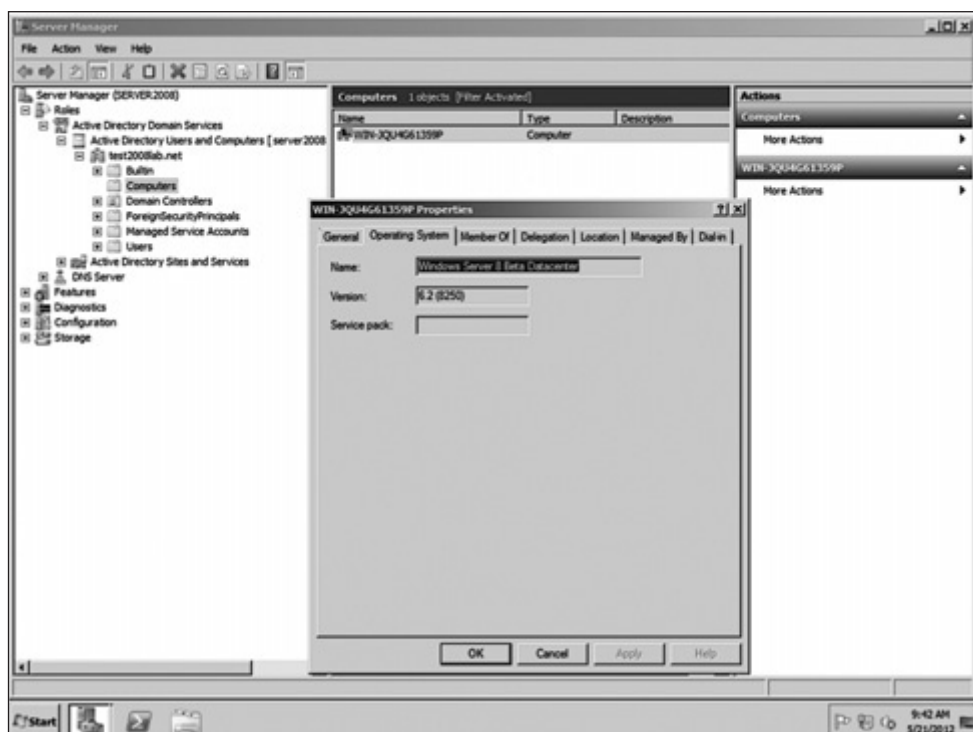


Рис. 4.14. Добавление компьютера под управлением Server 2012 к домену Server 2008 R2

Управление Active Directory

Центр администрирования Active Directory (Active Directory Administrative Center, ADAC) — это инструмент, который используется для управления AD. Вы можете запустить его из диспетчера серверов, воспользовавшись меню Средства (Tools).

Работа с ADAC

ADAC имеет такой же плиточный интерфейс, что и диспетчер серверов. Здесь представлен обзор возможностей, приведены полезные ссылки, справоч-

ные сведения по AD, средство для развертывания динамического контроля доступа (Dynamic Access Control), речь о котором пойдет в главе 5.

На рис. 4.15 представлен начальный экран ADAC. Здесь вы можете переустановить пароль администратора домена и выполнять глобальный поиск по AD. В левой части экрана можете выбрать контроллер домена, с которым хотите работать.

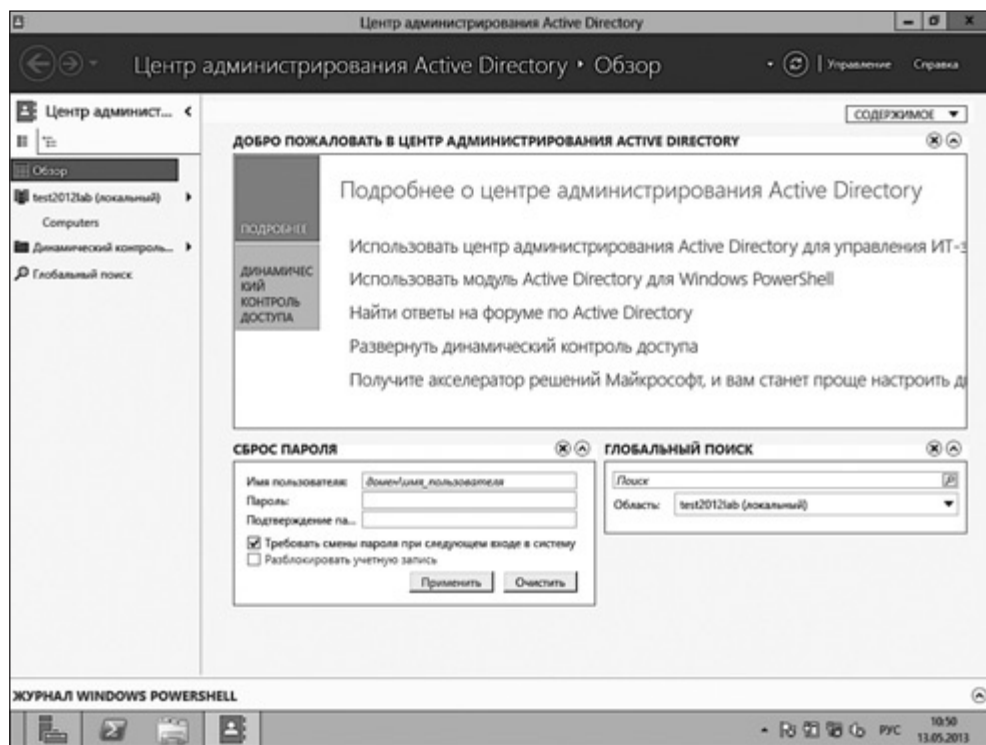


Рис. 4.15. Начальный экран ADAC

Когда вы выбираете контроллер домена, отображается список объектов AD, в том числе контейнеры и подразделения (organizations units, OU). В правой части экрана находится меню для выполнения различных задач, имеющих отношение к AD, таких как добавление и удаление новых объектов, выполнение поиска, просмотр свойств контейнеров (например, разрешений).

Интерфейс создания объектов в AD претерпел некоторые изменения. Сначала мы проходим через операцию создания новой группы.

Для того чтобы создать новую группу, нужно открыть диспетчер серверов. В панели мониторинга в левом меню нужно щелкнуть **AD DS**. Далее щелкнуть правой кнопкой на имени локального сервера (или сервера, на котором развернута AD) и выбрать команду **Центр администрирования Active Directory (Active Directory Administrative Center)** (рис. 4.16).

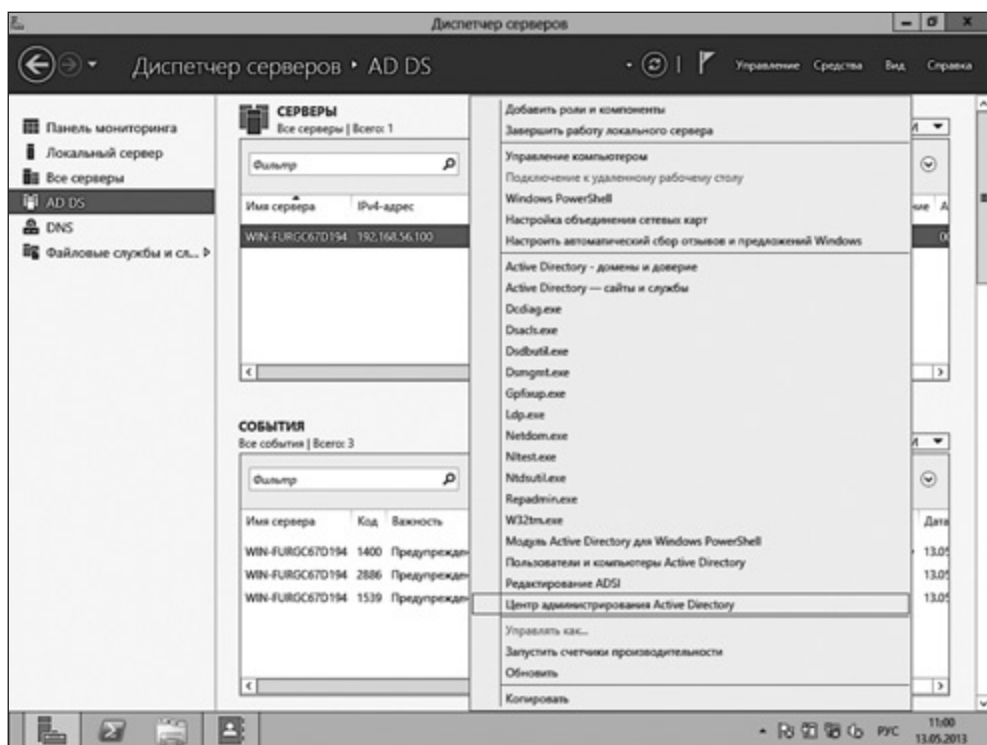


Рис. 4.16. Запуск центра администрирования Active Directory

В ADAC в меню, расположенном слева, нужно щелкнуть на строке, соответствующей серверу. Будут отображены все объекты контейнеров AD. В меню **Задачи (Tasks)**, которое появляется справа при выделении контейнера **Program Data**, нужно выбрать пункт **Создать (New)**, а затем пункт **Группа (Group)** (рис. 4.17).

Будет открыто окно Создать Группа (Create Group) (рис. 4.18). Поля, отмеченные красными звездочками, обязательны для заполнения. Я назвала свою группу *Human Resources NY*. Когда вы введете имя группы, автоматически будет заполнено поле Имя группы (SamAccountName) (Group Name

(SamAccountName)), которое находится непосредственно под полем Имя группы (Group Name).

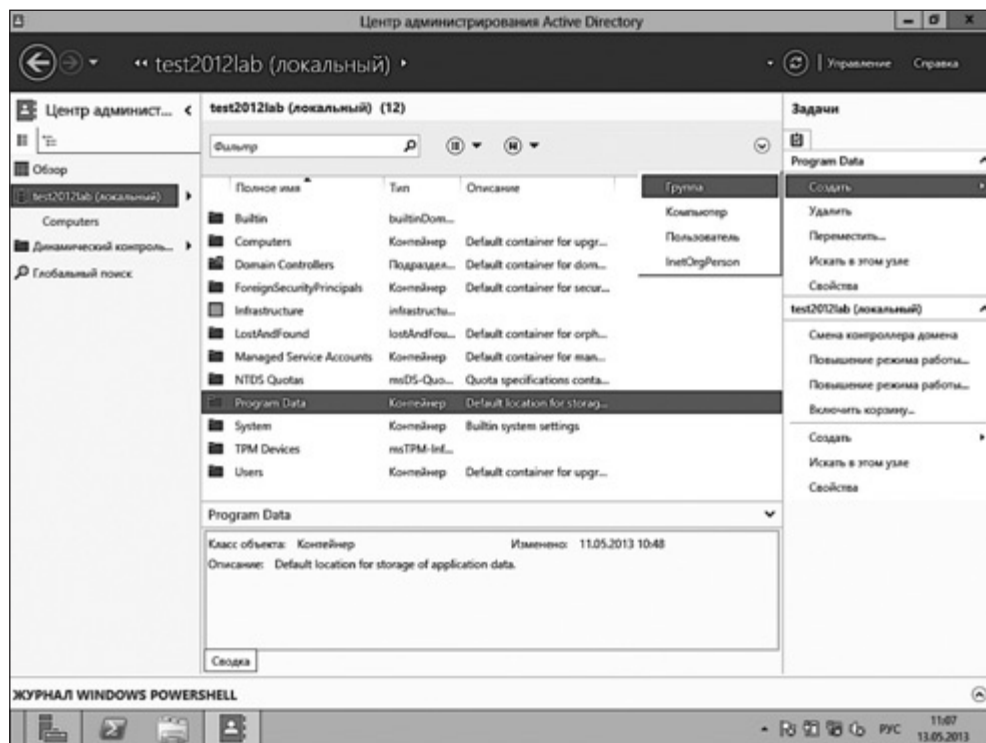


Рис. 4.17. Меню Задачи



В поле Имя группы (SamAccountName) (Group Name (SamAccountName)) находится альтернативное имя, используемое клиентскими операционными системами, которые были созданы до появления AD, таких как Windows 95.

Теперь нужно выбрать тип группы. По умолчанию это будет Безопасность (Security), но вы можете настроить группу, например, в качестве списка рассылки сообщений электронной почты. Следующий шаг заключается в выборе области группы. Значение по умолчанию — Глобальная (Global), но мы можем сделать ее локальной группой в домене или универсальной (то есть она будет использоваться в нескольких лесах Active Directory).

Рис. 4.18. Создание группы

Можно добавить в группу членов группы либо назначить группу членом родительской группы. Делается это в группах параметров Члены группы (Members) и Член групп (Member of) соответственно. Оставшиеся поля позволяют задать дополнительные сведения о группе: кто управляет этой группой, описание группы, заметки о ней и т. д.

Если вам не нужно работать со всей информацией, которая по умолчанию отображается в окне Создать Группу (Create Group), можете скрыть некоторые разделы этого окна. Например, в небольшой организации, где в IT-разделе работают несколько сотрудников, сведения о том, кто управляет группой, могут быть попросту не нужны. Для того чтобы настроить интерфейс данного окна, нужно нажать кнопку с выпадающим списком Разделы (Sections), которая расположена в верхнем правом углу окна Создать Группу (Create Group). В окне отображаются лишь выбранные в данном списке разделы (рис. 4.19). Для того чтобы скрыть раздел, достаточно снять флажок у его названия.

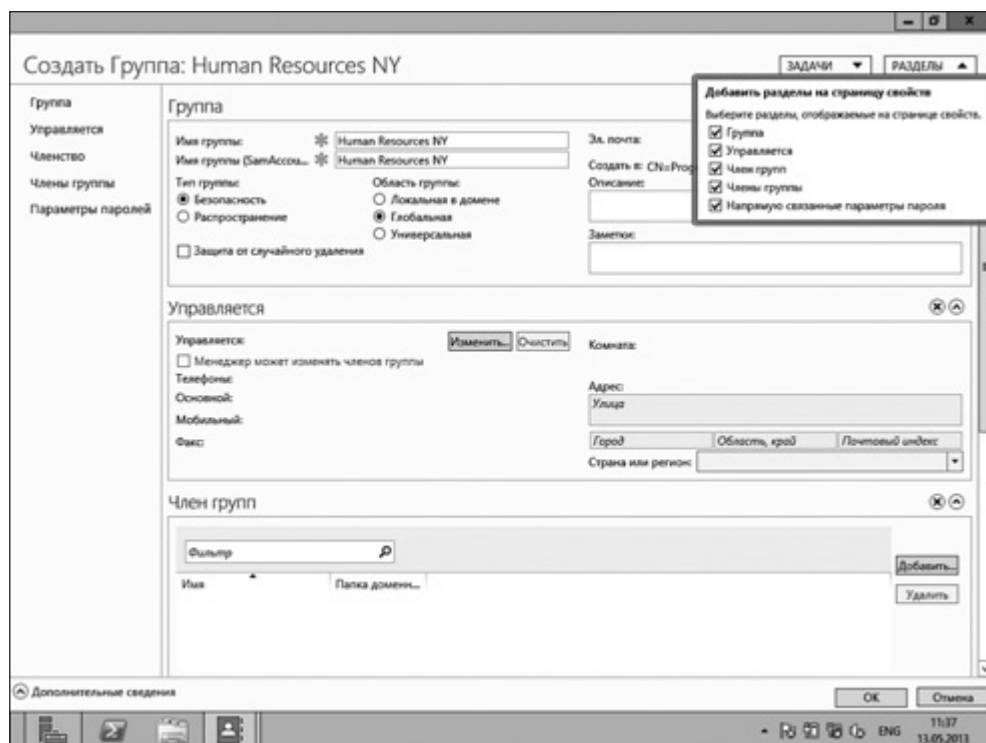


Рис. 4.19. Управление составом разделов

Кроме того, вы можете закрывать разделы с помощью кнопки со значком «X», расположенной в правом верхнем углу.

Если вы используете отдельные разделы лишь время от времени, можете просто свернуть их, когда они не нужны, вместо того чтобы закрывать. Для сворачивания раздела щелкните на кнопке со стрелкой, которая расположена около кнопки со значком «X».

Похожий интерфейс применяется при создании любых объектов AD в ADAC, хотя набор полей может различаться в зависимости от типа создаваемого объекта (например, таким объектом может быть новая учетная запись компьютера или пользователя). Подробнее о создании учетных записей пользователей и об управлении ими мы поговорим в главе 5.

ADAC позволяет также выполнять задачи, имеющие отношение к домену в целом, например менять контроллер домена или повышать уровень функциональности леса или домена.

Корзина AD

Корзина Active Directory (Active Directory Recycle Bin) — это механизм, который позволяет восстанавливать удаленные объекты AD без потери атрибутов этих объектов. Например, если вы удалили учетную запись пользователя и затем восстановили ее с использованием корзины AD, сохранятся разрешения, назначенные этой учетной записи, и заданное ей членство в группах.

В ADAC для Server 2012 корзину включить довольно просто. Для этого достаточно воспользоваться командой Включить корзину (Enable Recycle Bin), которая расположена в правой части экрана ADAC в меню Задачи (Tasks) (рис. 4.20).

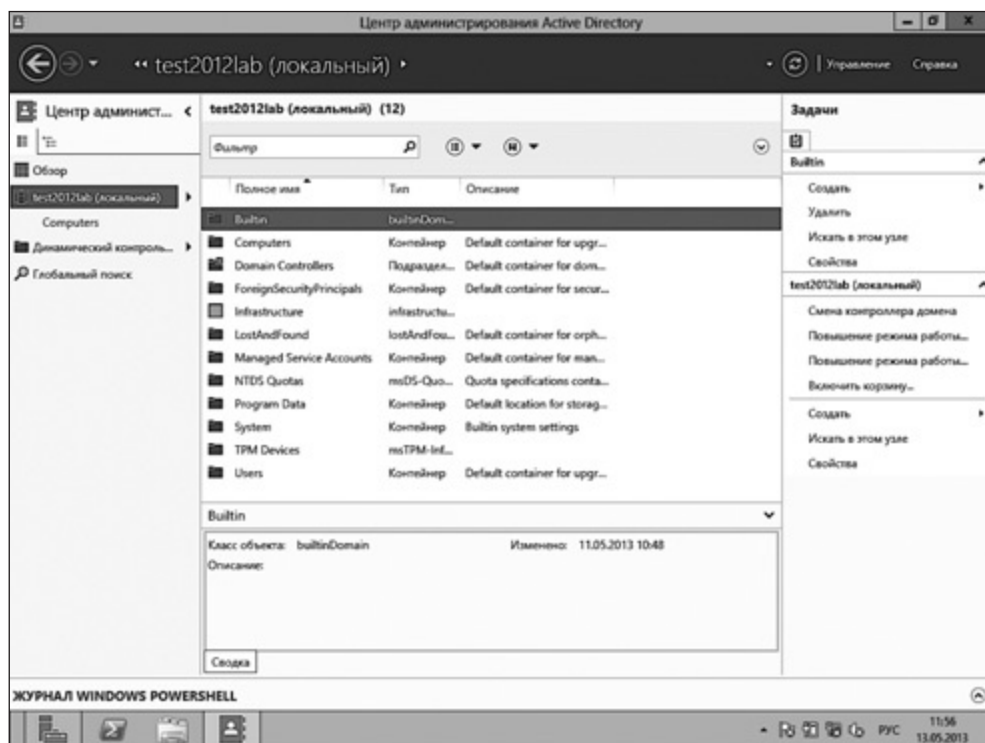


Рис. 4.20. Команда для включения корзины

Нажмите ОК во всплывающем сообщении, для того чтобы подтвердить включение корзины (рис. 4.21). Обновите экран — и вы увидите новый контейнер Удаленные объекты (Deleted Objects).



Создавая новый объект AD, вы можете защитить его от случайного удаления, установив флажок **Защита от случайного удаления** (Protect from accidental deletion) в окне создания объектов.

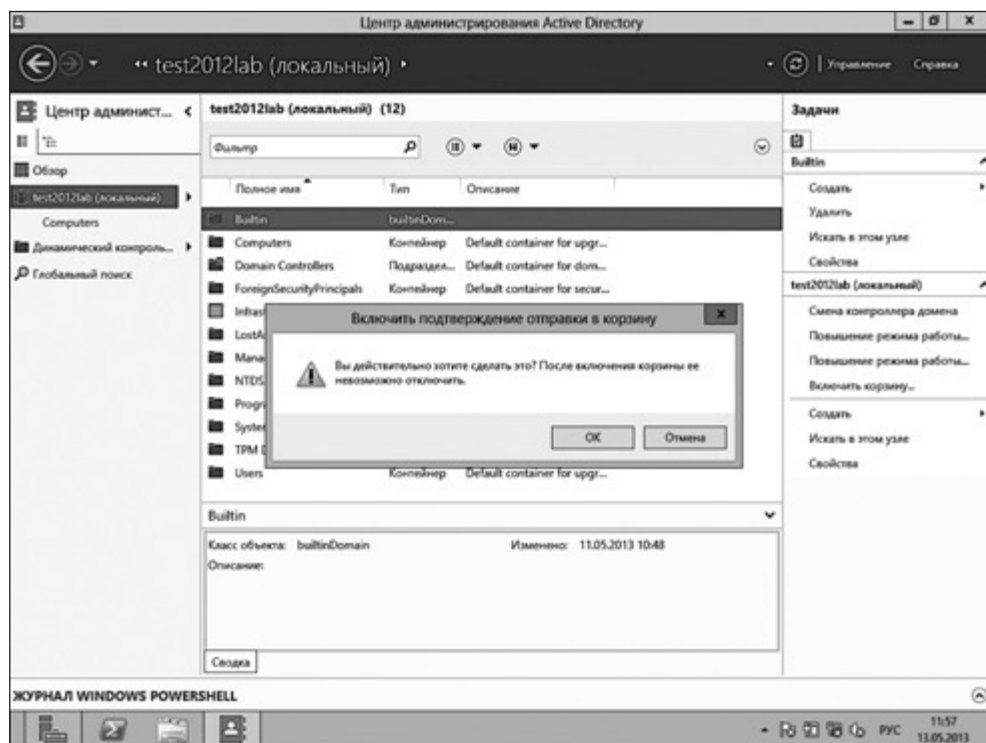


Рис. 4.21. Подтверждение включения корзины

Для того чтобы восстановить удаленный объект, откройте контейнер Deleted Objects (Удаленные объекты) и либо щелкните правой кнопкой мыши на контейнере и выберите команду **Восстановить** (Restore) для восстановления объекта там, где он находился ранее, либо выберите команду **Восстановить в (Restore to)**, для того чтобы задать для него новое расположение (рис. 4.22). Эти же команды доступны и в меню **Задачи** (Tasks).

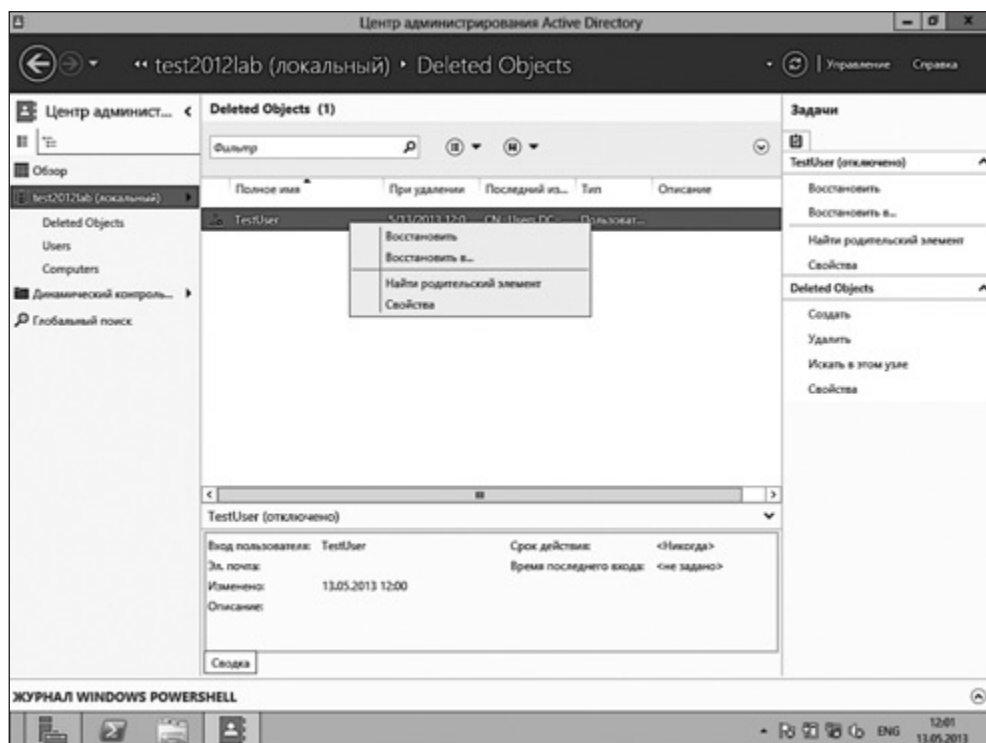


Рис. 4.22. Восстановление удаленных объектов

Поиск с помощью ADAC

Иногда вам нужно что-либо сделать с конкретным объектом AD, например отключить учетную запись пользователя, который больше не работает в вашей организации. Прокрутка списков объектов Active Directory в поиске этой учетной записи может быть довольно утомительным занятием, особенно в крупных организациях, в которых имеется множество объектов AD.

В подобной ситуации как нельзя кстати придутся поисковые возможности ADAC. С помощью ADAC вы можете производить глобальный поиск по локальной AD или по всей инфраструктуре Active Directory.

Для того чтобы начать поиск, воспользуйтесь пунктом **Глобальный поиск** (Global Search), который можно найти в левом меню ADAC. Вы можете сразу

же ввести поисковый запрос или создать более сложный запрос для более сложной операции поиска.

Начните создавать подобный запрос щелчком стрелки, расположенной в правой части окна поиска, для того чтобы отобразилось выпадающее меню с командой + Добавить условие (+ Add criteria) (рис. 4.23).



Рис. 4.23. Добавление параметра запроса

Раскрывающийся список этой команды содержит поля, позволяющие формировать сложные поисковые запросы. На рис. 4.24 показан запрос, созданный с использованием полей Имя (Name), Город (City) и Область, республика, край, округ (State).



После того как запрос готов, нажмите **Enter** или щелкните на значке увеличительного стекла, чтобы выполнить поиск.

Запросы можно сохранять, щелкая на значке с изображением диска в правой части окна поиска (рис. 4.25).

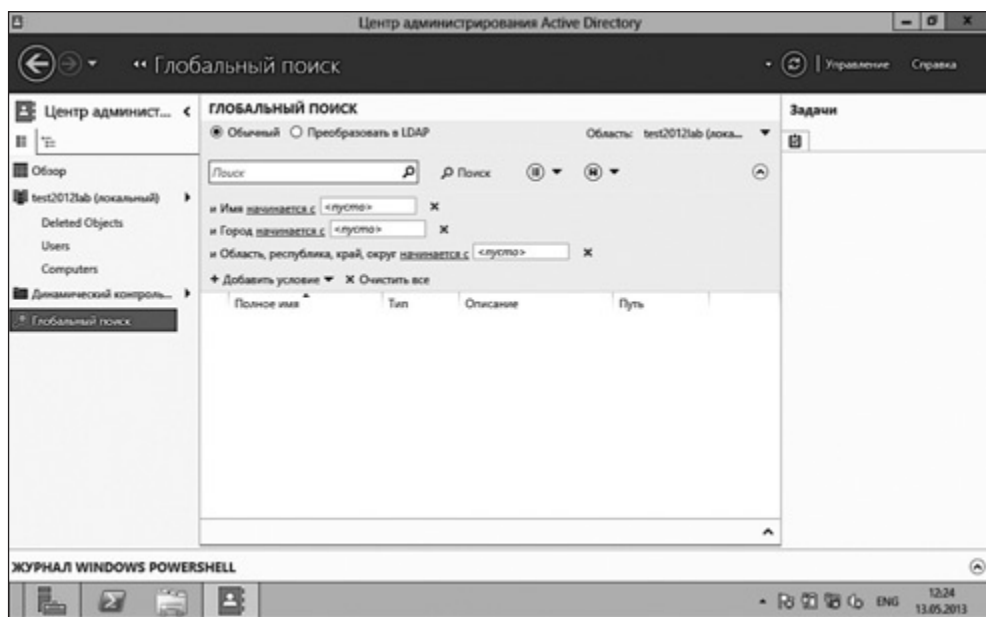


Рис. 4.24. Создание поискового запроса

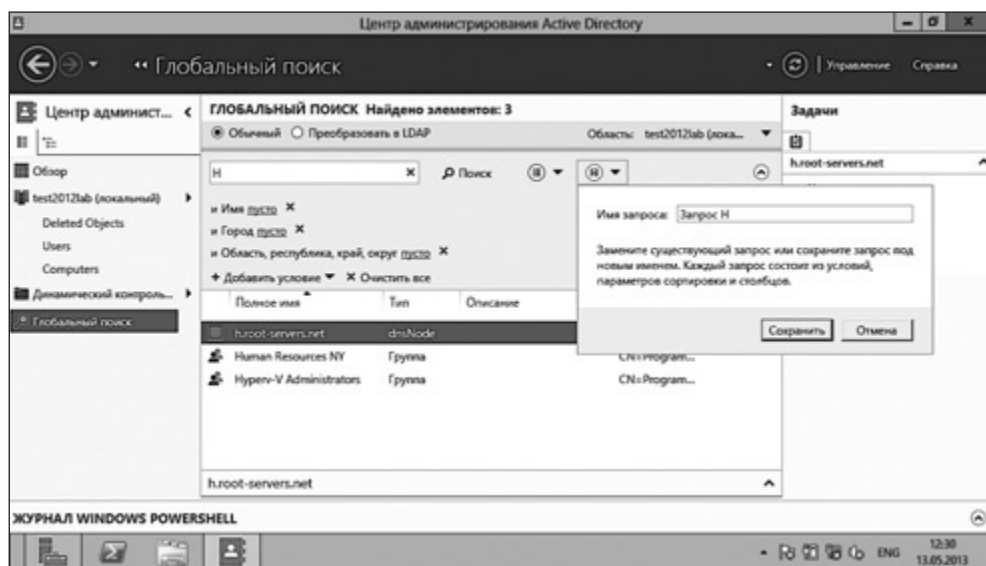


Рис. 4.25. Сохранение запроса

Сохранив запрос, вы можете быстро открыть его снова, щелкнув на значке списка запросов (рис. 4.26).

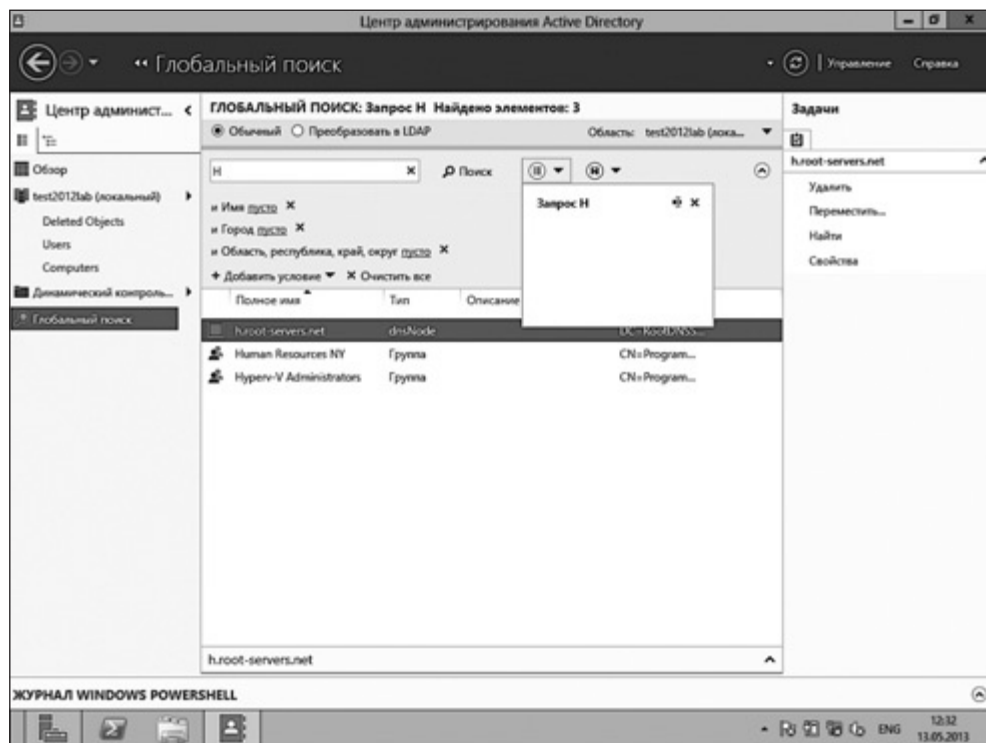


Рис. 4.26. Список запросов

Журнал Windows PowerShell

В нижней части окна ADAC расположен раздел Журнал Windows PowerShell (Windows PowerShell History), по умолчанию свернутый. Его можно развернуть, щелкнув на кнопке со стрелкой, направленной вверх, которая расположена в его правой части.

Здесь отображаются все команды PowerShell, связанные с задачами, которые вы выполняете с помощью графического интерфейса ADAC. И это отличное место для знакомства с синтаксисом PowerShell. Команда Копировать (Copy) позволяет скопировать выделенную строку в буфер обмена, после чего ее можно сохранить для последующего использования.

Выделите время, чтобы разобраться с тем, как задачи, которые вы выполняете, реализуются с использованием PowerShell. Возможно, Microsoft в Server 2012 не упростил подход к PowerShell, который облегчает выполнение повседневных задач. Однако, когда вам нужно выполнить большой объем работ, можете воспользоваться сценариями, для того чтобы избежать серьезных затрат времени на работу с графическими средствами управления.

Использование PowerShell для развертывания ActiveDirectory

Задачи, которые администратору приходится решать с помощью ADAC, могут быть выполнены и с использованием PowerShell. Хотя в этой книге и не преследуется цель изучения PowerShell, неплохо будет ознакомиться с PowerShell при выполнении основных административных действий, таких как развертывание AD.

Для того чтобы запустить процесс развертывания AD с использованием PowerShell, введите в консоль PowerShell (рис. 4.27) следующую команду:

```
Install-windowsfeature -name AD-Domain-Services -IncludeManagement Tools
```

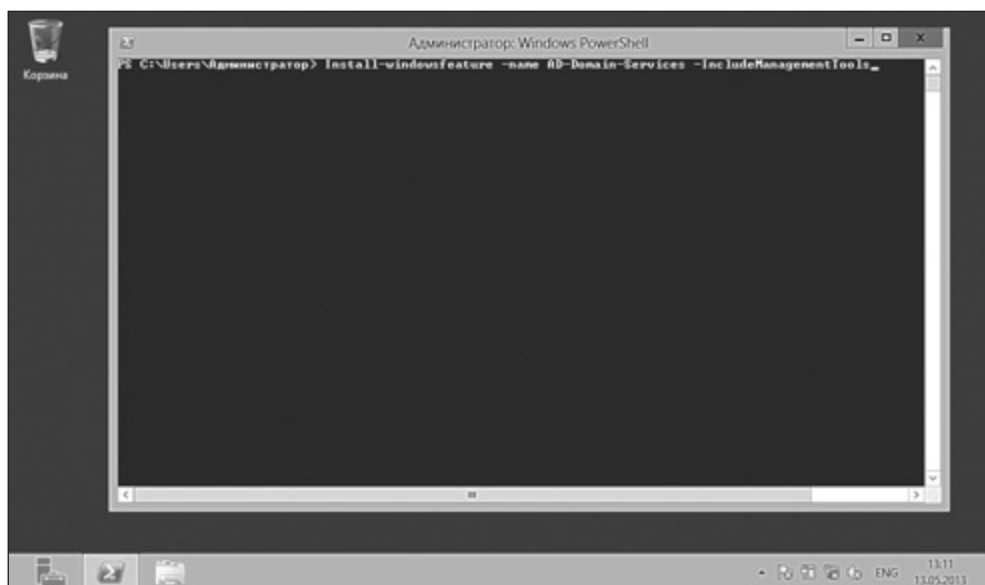


Рис. 4.27. Развертывание AD с использованием PowerShell

При успешном исполнении данной команды начнется установка (рис. 4.28).

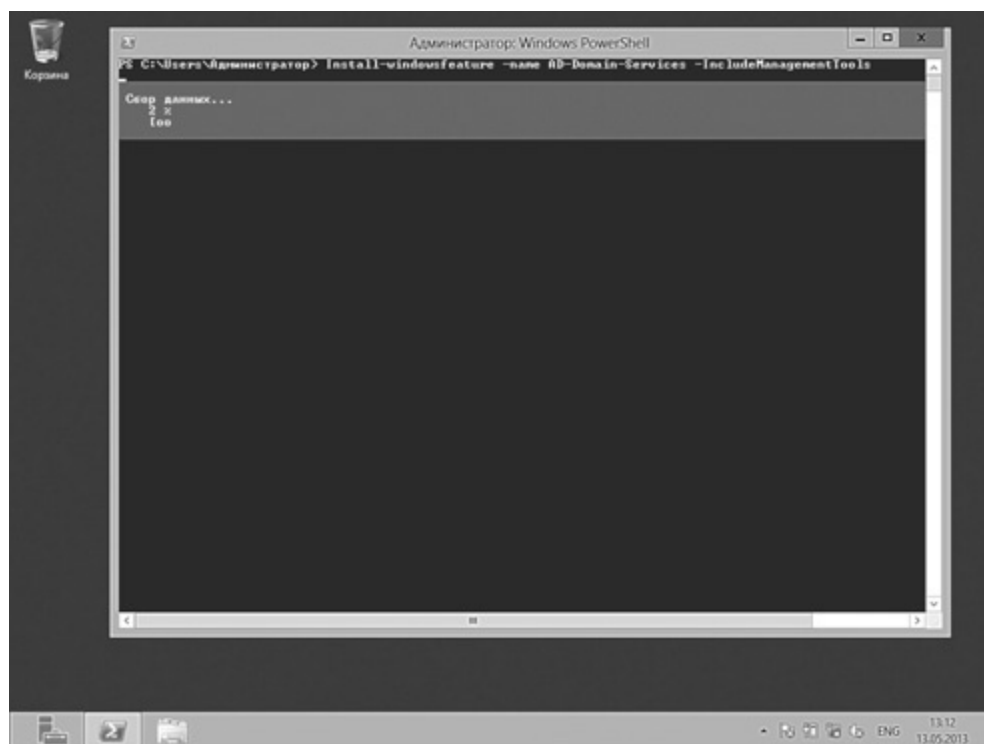


Рис. 4.28. Установка AD в PowerShell

После развертывания AD будут показаны подтверждение, а также сообщения о действиях, необходимых для успешного развертывания AD.



Практически все задачи, которые можно решить с помощью графического интерфейса ADAC, можно выполнить и в PowerShell. Например, для того чтобы включить корзину ADAC (ADAC Recycle Bin), можно воспользоваться следующим командлетом:

```
Enable-ADOptionalFeature -Identity 'CN=RecycleBinFeature,  
CN=OptionalFeatures,CN=DirectoryService,CN=WindowsNT,  
CN=Service,CN=Configuratio,DC=xyz,  
DC=local' -Scope ForestOrConfigurationSet -Target 'xyzlocal'
```

Выводы

В Server 2012 управление доменными службами Active Directory реализовано эффективнее, чем в предыдущих версиях этой ОС. Здесь имеются централизованные средства управления, в которые интегрированы инструменты проверки системы перед установкой, что вместе с интеграцией *Adprep.exe* означает упрощение процедуры установки.

Возможность быстрой и простой настройки AD DS очень важна для обеспечения эффективной работы сервиса каталога для таких замечательных механизмов, как управление идентификацией пользователей, управление безопасностью и авторизацией, управление устройствами.

Хотя центр администрирования Active Directory обладает возможностями, которые уже присутствовали в предыдущих версиях серверных ОС семейства Windows, такими как поиск и корзина, его интерфейс серьезно изменен, поэтому важно ознакомиться с ним, для того чтобы знать, где искать нужные компоненты и как ими пользоваться. Кроме того, интерфейс поддается настройке. Например, при создании объектов Active Directory разделы могут быть свернуты или скрыты.

Active Directory в Server 2012 может работать на уровне функциональности Server 2012 либо ее можно интегрировать в AD-домены, работающие на уровне функциональности более старых версий Windows Server. Однако при этом часть новых возможностей теряется.

Хотя на первый взгляд использование PowerShell для решения задач, которые могут быть решены с помощью нескольких щелчков мыши в графическом интерфейсе, может показаться слишком хлопотным делом, весьма полезно ознакомиться с системой команд PowerShell. В частности, это касается тех команд, которые имеют отношение к Active Directory. Знакомство с ними позволяет управлять AD быстро и эффективно. Лучший способ оценить потенциал PowerShell заключается в том, чтобы представить себе задачу по изменению некоторых параметров всех учетных записей пользователей в Active Directory. С использованием графического интерфейса выполнение подобной задачи может длиться целую вечность. Потратив немного времени на изучение PowerShell, вы сможете быстро и легко решать подобные задачи, кажущиеся непосильными при обычном подходе к ним. А простота и эффективность администрирования системы — это именно то, на что ориентированы все механизмы Server 2012.

5

Динамический контроль доступа при управлении пользователями и данными

Без сомнения, одна из основных новых возможностей Server 2012, с которой вы рано или поздно ознакомитесь независимо от размеров вашей сетевой инфраструктуры, — это динамический контроль доступа (Dynamic Access Control, DAC).

DAC предлагает мощные средства централизованного управления данными и правами пользователей. Среди них — условия доступа, основанные на выражениях (то есть если выполняется условие *x*, доступ предоставляется), централизованные политики доступа и централизованный аудит.

DAC — это крайне полезный набор инструментов, который упрощает решение проблем, возникающих в ходе развертывания системы разрешений в лесу или домене Windows. С его помощью легче управлять системой разрешений и отслеживать ее состояние. Управление разрешениями Windows, как знают многие из нас, легко может выйти из-под контроля.

Разрешениями обычно управляют с помощью средств NTFS, Active Directory и использования групп. Во многих случаях пользователь, не являющийся членом какой-либо группы, нуждается в доступе к файлу, который находится

в общей папке, принадлежащей данной группе. В подобных ситуациях дело нередко заканчивается созданием групп, которые, в сущности, не нужны в инфраструктуре управления разрешениями. Управлять разрешениями NTFS для родительских и дочерних папок неудобно, а проверка того, к каким данным есть доступ у тех или иных пользователей, может превратиться в кошмар. Мало того, что вы сталкиваетесь с путаницей с членством в группах. Когда управление правами доступа начинает выходить из-под контроля, оказывается перегруженной и система управления маркерами безопасности. По мере роста компании при добавлении в систему новых пользователей (сотрудников) часто возрастает и количество групп. Увеличение числа групп и пользователей неизменно приводит к разрастанию размеров маркеров безопасности Kerberos. Маркеры создаются для пользователей и содержат сведения обо всех группах, к которым принадлежат пользователи. При увеличении размеров маркеров Kerberos пользователи могут столкнуться с замедлением процесса входа в систему и сбоями при проверке подлинности. Возможности DAC помогают уменьшить и сложность групп, и чрезмерное разрастание маркеров.

Возможность аудита доступа к данным и отслеживания изменений, которые пользователи вносят в данные, полезна в любой инфраструктуре, но иногда она имеет особую важность. Речь идет об организациях, которые обязаны соблюдать определенные законодательные нормы, такие как закон Сарбейнза—Оксли (Sarbanes—Oxley, SOX) и закон «О перемещаемости и подотчетности страхования здоровья» (Health Insurance Portability and Accountability, HIPAA). Это законы, которые задают набор требований к работе с цифровыми данными в сфере финансов и здравоохранения соответственно. Среди этих требований — возможность надежного аудита и учета полномочий, доступная IT-персоналу, руководителям и сотрудникам, ответственным за обработку персональных данных. В итоге они получают в виде отчетов сведения о том, кто работал с той или иной информацией.

Политики доступа и возможность аудита существовали и в предыдущих версиях Windows Server, но динамический контроль доступа — это совершенно новая функция. DAC поддерживает сложные выражения, близкие к используемым в естественном языке. На них и основаны политики доступа и аудита.

Кроме того, в DAC есть расширенные возможности классификации данных. Документы могут быть автоматически классифицированы на основании их содержимого. Это означает, что как администратор сервера вы можете создать правило, на основании которого может быть классифицирован любой файл, содержащий заданные вами параметры. Например, любой файл, который содержит слово «конфиденциально», может быть классифицирован как

важный и автоматически зашифрован с использованием системы управления правами (Right Management Services, RMS).

Даже при наличии новых и улучшенных средств управления разрешениями, которые предоставляет DAC, возможны ситуации, когда пользователям может понадобиться доступ к файлам или общим папкам, на работу с которыми у них нет прямого разрешения. Могут возникать проблемы и тогда, когда существующие разрешения NTFS не соответствуют недавно развернутой системе DAC. Для отработки этих сценариев Microsoft включила в DAC компонент Помощь при ошибке «Отказано в доступе» (Access Denied Remediation). Пользователи могут запрашивать разрешение на доступ к данным, к которым у них нет доступа, у владельца данных или администратора. Это не полностью автоматизированная система. При ее реализации пользователь отправляет запрос по электронной почте, а затем сотрудник ИТ-подразделения или владелец данных выполняет соответствующие настройки. Однако применение системы помощи при ошибке «Отказано в доступе» позволяет уменьшить число обращений пользователей, которым нужен доступ к некоторым закрытым для них данным, в службу поддержки.

Составные части DAC

В основе системы динамического контроля доступа лежат два базовых компонента: утверждения (claims) и свойства ресурсов (resource properties).

Если я заявляю: «Я живу в Нью-Йорке», — я делаю *утверждение*. В Server 2012 утверждения интегрированы с системой аутентификации Kerberos. С помощью утверждений вы можете определять и настраивать разрешения для пользователей и устройств, основываясь не только на группах безопасности, к которым они принадлежат, но и на заданных вами утверждениях. Например, таких, как: «У этого пользователя высокий уровень допуска к секретной информации».

Свойства ресурсов — это настраиваемые метки, которые можно назначать данным для их классификации. Вы можете создать свойства ресурсов, определяющие файлы как секретные (Sensitive), конфиденциальные (Confidential), данные только для персонала (Human Resources Group Only) или задавать любые другие свойства, которые могут понадобиться для обеспечения безопасности данных в вашей организации.

Утверждения и свойства ресурсов — это строительные блоки DAC, компоненты, на которых построены централизованные политики управления

доступом и аудита. Вы можете выполнить очень сложную, детальную настройку DAC, но помните: успешное развертывание этой системы начинается с соответствующим образом установленных утверждений и свойств ресурсов. В следующем разделе я подробно расскажу о том, как настроить DAC, для того чтобы вы смогли воспользоваться всеми преимуществами этой новой мощной возможности Server 2012.

Предварительные требования и советы

Прежде чем приступать к развертыванию и тестированию DAC, вам понадобится учесть некоторые рекомендации. Хотя Microsoft и продвигает DAC как спасение от множества ИТ-напастей, даже при развертывании DAC могут возникнуть некоторые неожиданности.

Самое большое ограничение заключается в том, что DAC функционирует только на Server 2012 и клиентских системах, работающих под управлением Windows 8 и Windows RT (это версия Windows 8, которая предустанавливается производителями на планшетные устройства). Конечно, в большинстве компаний, использующих платформы от Microsoft, уже имеются серверы, Active Directory, NTFS-разрешения и полная Windows-экосистема. Так что же делать?

Ожидается, что в большинство подобных инфраструктур будут добавлены контроллер домена, работающий под управлением Windows Server 2012, и файловые серверы. Это позволит применять утверждения о пользователях и другие компоненты DAC в пределах существующего Windows-окружения. Это не обязательно аппаратные серверы — DAC можно развернуть и на виртуальных машинах.

Кроме того, Microsoft предлагает набор инструментов для классификации данных (Data Classification Toolkit), который упрощает развертывание DAC на нескольких серверах. Этот набор инструментов позволяет реализовать некоторые возможности DAC на Server 2008 R2.

Предметом наибольшего беспокойства системных администраторов могут быть потенциальные конфликты между NTFS-разрешениями и DAC. Даже если вы переносите данные, например, с файлового сервера, работающего под управлением Server 2008 R2, на новый сервер, работающий под управлением Server 2012, NTFS-разрешения, соответствующие этим данным, никуда не денутся. У каких же разрешений будет приоритет? У тех, которые назначены в рамках NTFS или DAC?

Разворачивая DAC в существующей Windows-сети, полезно помнить важное правило: NTFS-разрешения не дадут больших прав доступа, чем позволяют правила, основанные на утверждениях. В свою очередь, правила, основанные на утверждениях, не дадут большего уровня разрешений, чем установлено в NTFS. На бумаге это может выглядеть довольно запутанным, но когда DAC развернут и настроен с учетом разрешений NTFS, это правило довольно легко наблюдать в действии.

Кроме того, я рекомендую разворачивать DAC в тестовой среде, содержащей копии ваших файловых серверов. Это могут быть и виртуальные машины. Выделите время на то, чтобы проверить, как DAC повлияет на текущие параметры безопасности и повлияет ли вообще. Когда придет время разворачивания DAC, начните с наименее важных данных. Идея использования DAC заключается в постепенном встраивании его возможностей в существующие инфраструктуры.

И наконец, DAC может быть сложным в настройке. Этот процесс предусматривает множество шагов, которые придется предпринять администраторам Windows-серверов предыдущих поколений. В работе с DAC используется немало новых понятий, которые придется освоить. Далее показан очень простой пример разворачивания DAC, его цель — ознакомить вас с новыми понятиями и процессом разворачивания. Помните о том, что DAC позволяет создавать очень сложные и тщательно продуманные выражения и конфигурации для управления доступом.

Развертывание DAC

В разворачивании DAC можно выделить несколько основных шагов. Ключевой компонент DAC — это централизованная политика доступа (Central Access Policy). Создание централизованной политики доступа начинается с настройки утверждений. Как уже было сказано, это свойства, которые используются для сопоставления учетных записей пользователей и файлов для того, чтобы определить, соответствует ли учетная запись требованиям, необходимым для доступа к файлу. Эти свойства, или утверждения, добавляются в список свойств ресурсов.

На следующем шаге создается централизованная политика доступа. Список свойств ресурсов применяется в виде политики. Затем политика публикуется в домене.

Затем мы можем развернуть DAC на файловых серверах, и централизованная политика доступа будет применена к общим папкам.

Последний шаг заключается в проверке конфигурации DAC. Описанный процесс проиллюстрирован на рис. 5.1.

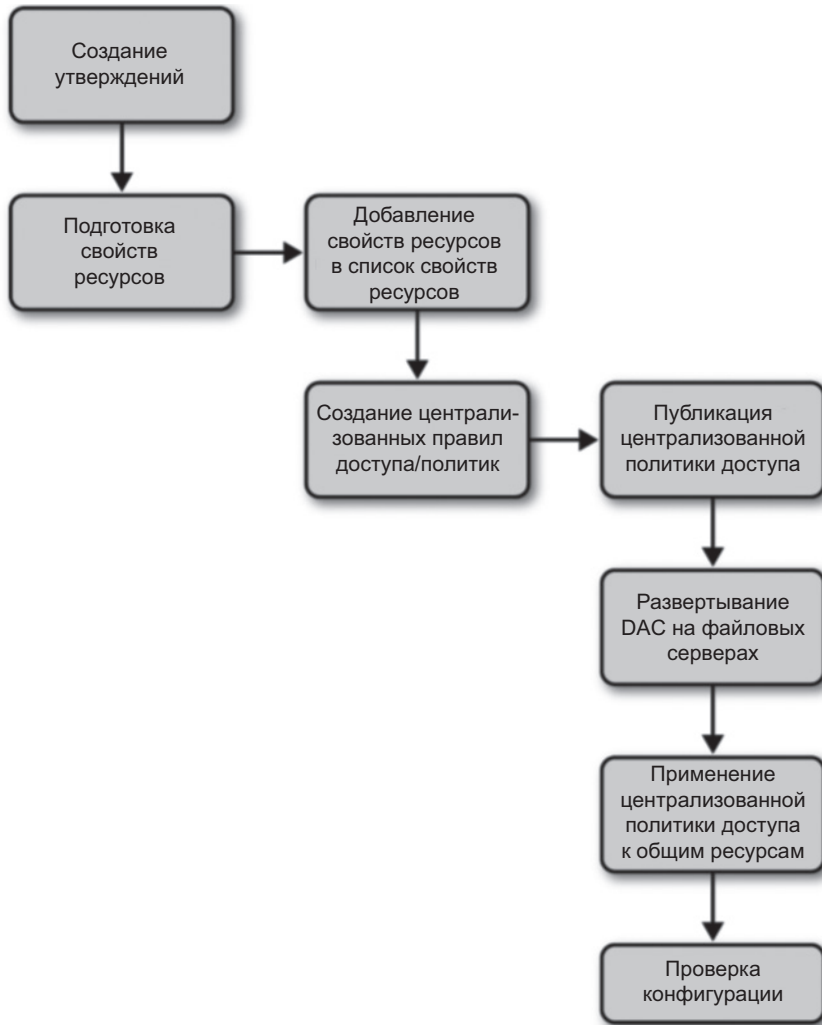


Рис. 5.1. Стандартный процесс развертывания DAC

Подготовка утверждений

Настраивая типы утверждений для пользователей, вы добавляете существующие атрибуты Active Directory в список атрибутов. Эти списки используются

для того, чтобы определять права доступа пользователей к конкретным объектам.

В нашем примере развертывания название отдела (department) Payroll, к которому относятся пользователи, используется как часть выражения, применяемого для определения того, имеет ли пользователь доступ к файлам в общей папке Payroll.

В диспетчере серверов (Server Manager) выполним команду Средства (Tools), из появившегося меню выберем Центр администрирования Active Directory (Active Directory Administrative Center). В появившемся окне щелкнем на разделе Динамический контроль доступа (Dynamic Access Control). Выберем в открывшемся окне Claim Type (Типы утверждений). Из списка команд, соответствующего данному элементу, выберем команду Создать ► Тип утверждения (New ► Claim Type).

В списке Атрибут источника (Source Attribute) найдем пункт department (отдел). Затем нужно щелкнуть на данном атрибуте и убедиться в том, что его параметр Тип значения (Value Type) установлен в значение Строка (String). Здесь мы используем существующий атрибут department в новом типе утверждения, который собираемся создать.

В поле Отображаемое имя (Display name) введем «Department» и нажмем ОК (рис. 5.2).

После выполнения описанных действий вы должны увидеть новый тип утверждения в центре администрирования Active Directory.



На рис. 5.2 вы можете видеть параметр Защита от случайного удаления (Protect from accidental deletion). Для объектов, создаваемых в DAC, эта установка включена по умолчанию. Если вы хотите удалить объект, данный флажок следует снять.

Настройка свойства ресурса для файлов

На следующем шаге мы должны добавить свойство ресурса, которое соответствует созданному утверждению. Свойства ресурсов используются файловыми серверами для классификации данных. По умолчанию есть несколько предопределенных свойств ресурсов, но можно создавать и новые.

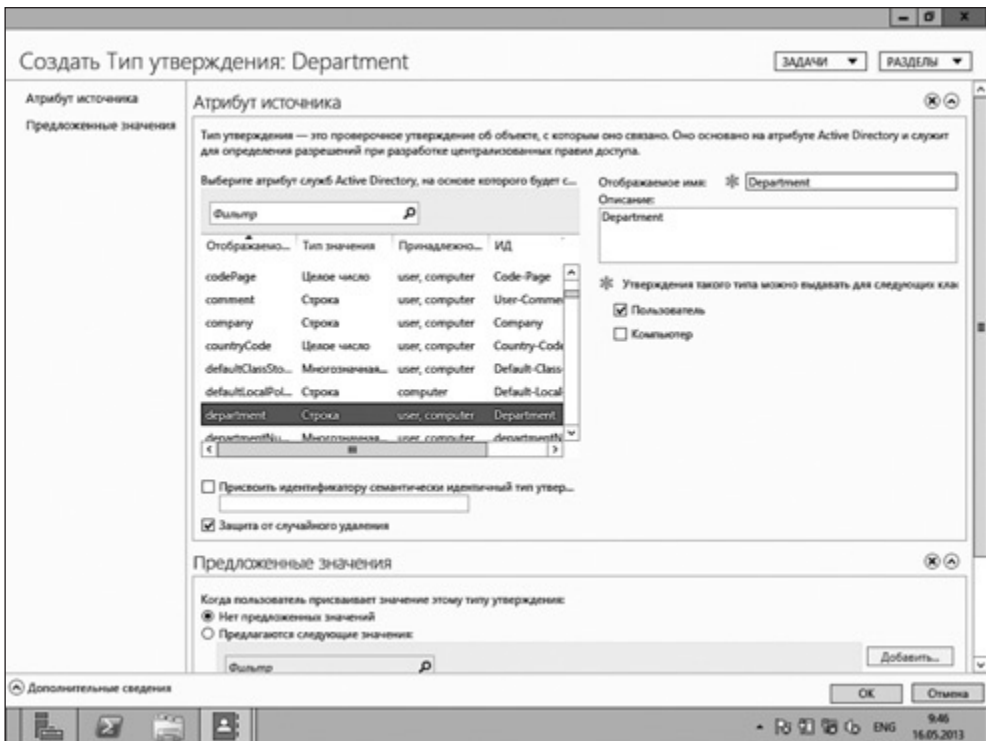


Рис. 5.2. Настройка нового типа утверждения

Для того чтобы создать новое свойство ресурса, в ADAC нужно выделить объект Resource Properties (Свойства ресурсов) и выполнить для него команду Создать ► Свойство ресурса (New ► Resource Property).

В поле Отображаемое имя (Display Name) введем «Department Payroll», добавим к свойству ресурса значение «Payroll». Подтвердим нажатиями кнопки OK операции создания значения свойства ресурса и свойства ресурса. Теперь в списке Resource Properties (Свойства ресурсов) можно найти только что созданное свойство (рис. 5.3).

Добавление свойства ресурса в глобальный список свойств ресурсов

Каждое свойство ресурсов, которое планируется использовать, следует добавить в список свойств ресурсов. Благодаря этим спискам свойства ресурсов

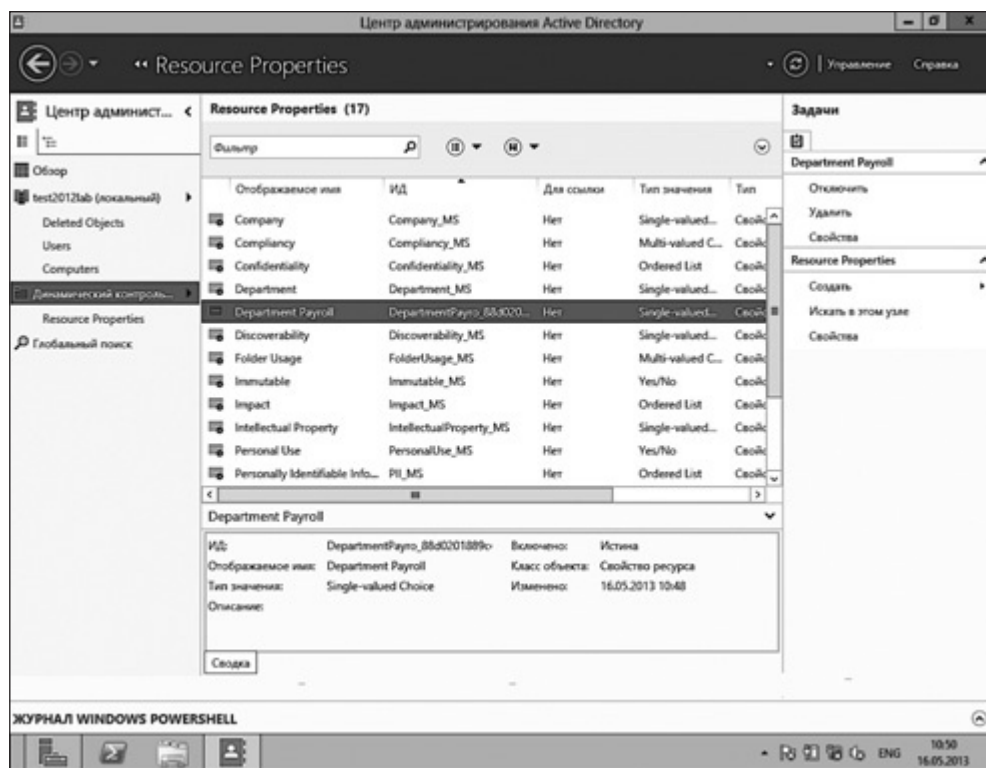


Рис. 5.3. Настройка нового свойства ресурса

становятся доступными файловым серверам. Ресурсы DAC могут быть включены в отдельные списки, рассчитанные на конкретные файловые серверы, но в данном случае мы собираемся добавить свойство ресурса в глобальный список свойств ресурсов (Global Resource Property List).

В ADAC перейдем к объекту Динамический контроль доступа (Dynamic Access Control), затем к контейнеру Resource Property Lists (Списки свойств ресурсов) и для списка Global Resource Property List (Глобальный список свойств ресурсов) выполним команду **Добавить свойства ресурса** (Add Resource Property). В появившемся окне выбора свойств ресурса найдем только что созданное свойство **Department Payroll** и с помощью кнопки со стрелками добавим его в список, после чего закроем данное окно нажатием кнопки **OK**.

Теперь свойство ресурса Department Payroll станет пунктом глобального списка свойств ресурсов (рис. 5.4).

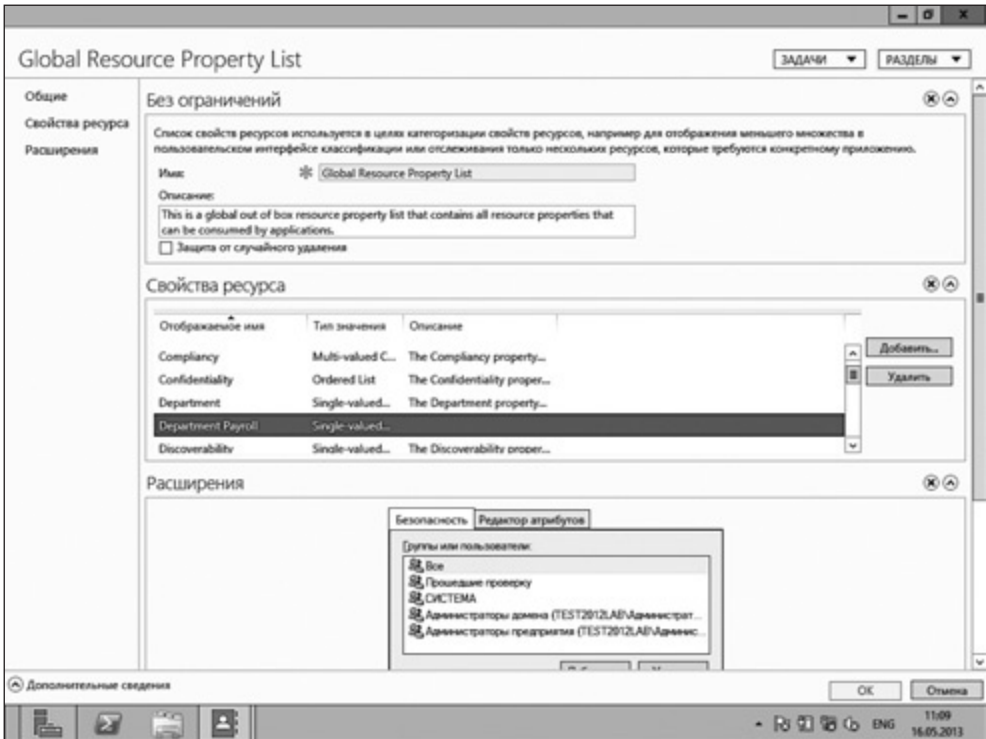


Рис. 5.4. Добавление свойства ресурса в глобальный список свойств ресурсов

Создание нового централизованного правила доступа

Централизованное правило доступа (central access rule) похоже на список контроля доступа (Access Control List, ACL). В случае с правилом вы можете задавать для пользователей условия доступа к данным. Например, можно задать такое правило: «Если выполняется условие *x*, доступ предоставляется».

В данном примере нам требуется правило, в соответствии с которым значение атрибута `department`, назначенное пользователю, должно совпадать со значением атрибута `department`, назначенного общей папке.

Откроем ADAC, перейдем в раздел Динамический контроль доступа (Dynamic Access Control), выделим объект Central Access Rules (Централизованные правила доступа) и выполним команду Создать ► Централизованное правило доступа (New ► Central Access Rules).

В появившемся окне в поле Имя (Name) введем «Department-Payroll-Match-Required». Вы можете назвать правило любым именем, главное, чтобы данное имя позволяло сразу понять смысл правила. В разделе данного окна Целевые ресурсы (Target Resources) щелкнем на кнопке Изменить (Edit). В окне, которое появится в результате этого, воспользуемся ссылкой Добавить условие (Add a condition).

Теперь добавим два условия. Первое — Ресурс Department Payroll Существует (Resource Department Payroll Exists), второе — Ресурс Department Payroll Равно Значение Payroll (Resource Department Payroll Equals Value Payroll) (рис. 5.5). Нажмем ОК.

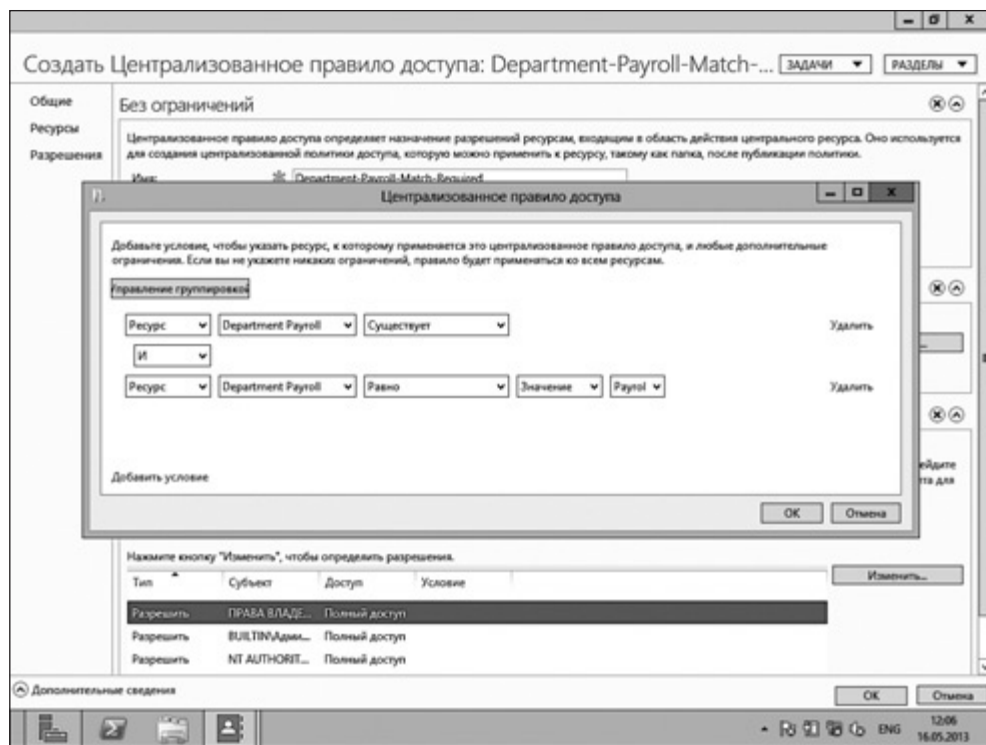


Рис. 5.5. Создание централизованного правила доступа

В разделе Разрешения (Permissions) выберем Использовать следующие разрешения как текущие (Use following permissions as current permission) и щелкнем на кнопке Изменить (Edit), для того чтобы задать разрешения. Например, вы можете дать здесь пользователям, принадлежащим к группе Payroll Department, полный доступ к данным, к которым применимо создаваемое правило. Для того чтобы протестировать разрешения, не применяя их, можно воспользоваться вариантом Использовать следующие разрешения как предложенные (Use following permissions as proposed permissions).

Создание централизованной политики доступа

Теперь нужно добавить новое централизованное правило доступа в централизованную политику доступа. К файлам и папкам в DAC можно применять единую централизованную политику доступа.

В ADAC выберем объект Динамический контроль доступа (Dynamic Access Control), затем выделим объект Central Access Policies (Центральные политики доступа), после чего выполним команду меню Создать ► Централизованная политика доступа (New ► Central Access Policy).

Назовем нашу политику «Domain File Server Policy» и нажмем кнопку Добавить (Add) для добавления нового централизованного правила доступа. В политику можно добавить только что созданное правило Department-Payroll-Match-Required. Его нужно выделить, нажать кнопку со стрелками для добавления в политику и нажать ОК.

Публикация централизованной политики доступа

Когда централизованная политика создана, ее нужно опубликовать, используя *объекты групповой политики* (group policy objects, GPO). Это нужно для того, чтобы довести ее до файловых серверов.

В диспетчере серверов (Server Manager) воспользуемся командой Средства ► Управление групповой политикой (Tools ► Group Policy Management). Затем следует щелкнуть правой кнопкой мыши на имени домена и выбрать команду Создать объект групповой политики в этом домене и связать его с данным контейнером (Create a GPO in this domain and Link it here).

Назовем GPO «Dynamic Access Control Policy», нажмем ОК. Выделим только что созданную политику в дереве объектов управления групповой политикой

и удалим добавленную в политику по умолчанию группу Прошедшие проверку (Authenticated users), так как нам не нужно, чтобы все пользователи, прошедшие проверку, могли получать доступ к данным подразделения Payroll.

Здесь же нужно выбрать соответствующие типы объектов (Object Types) для указания файлового сервера (или серверов), к которым будет применяться политика. Удостоверьтесь в том, что здесь в качестве типа объекта выбран тип Компьютеры (Computers).

Теперь щелчком правой кнопкой мыши нужно вызвать контекстное меню политики Dynamic Access Control Policy и выбрать в нем команду Изменить (Edit). Откроется окно Редактор управления групповыми политиками (Group Policy Management Editor). Затем следует пройти по пути Конфигурация компьютера ► Политики ► Конфигурация Windows ► Параметры безопасности ► Файловая система ► Централизованная политика доступа (Computer Configuration ► Policies ► Windows Settings ► Security Settings ► File System ► Central access policies) и из контекстного меню объекта Централизованные политики доступа (Central access policies) выбрать команду Управление централизованными политиками доступа (Manage Central Access Policies). Здесь следует выбрать политику, которую мы создали, нажать ОК и выйти из редактора управления групповыми политиками (Group Policy Management Editor).

Для того чтобы завершить процесс публикации политики, нам осталось выполнить еще два действия: включить расширенную защиту Kerberos и обновить групповую политику.

Расширенная защита Kerberos позволяет организовать защиту от угроз безопасности, которые сопутствуют аутентификации, с использованием протокола Kerberos. Среди этих угроз уязвимость к атакам методом грубой силы и спуфингу. С использованием расширенной защиты Kerberos между клиентским компьютером, подключенным к домену, и контроллером домена создается защищенный канал связи.

Расширенную защиту Kerberos включить легко. Выполнив в диспетчере серверов команду Средства ► Управление групповой политикой (Tools ► Group Policy Management), нужно перейти по пути Конфигурация компьютера ► Политики ► Административные шаблоны ► Система ► Kerberos (Computer Configuration ► Policies ► Administrative Templates ► System ► KDC). Далее следует включить параметр политики Поддержка клиентами Kerberos требований, комплексной проверки подлинности и защиты Kerberos (KDC support for claims, compound authentication and Kerberos armoring).

Для того чтобы выполнить обновление групповой политики, запустите Windows PowerShell и выполните команду `GPUPDATE/FORCE`.

Настройка файлового сервера

Все, о чем мы говорили до сих пор, касалось настройки DAC на контроллере домена. Следующие шаги выполним на файловом сервере, к которому нужно применить правила доступа, основанные на утверждениях.

Откроем диспетчер серверов (Server manager) файлового сервера, на панели мониторинга (Dashboard) щелкнем на ссылке **Добавить роли и компоненты** (Add roles and features) и доберемся, щелкая на кнопке **Далее** (Next), до окна, в котором можно выбирать роли сервера. Здесь нужно включить компонент **Диспетчер ресурсов файлового сервера** (File Server Resource Manager), который является частью уже установленного компонента **Файловые службы и службы хранилища** (File and Storage Services).

После завершения процедуры установки следует пройти к общей папке, доступ к которой нужно настроить. В нашем случае это общедоступная папка *Payroll*, для которой мы ранее создавали условия доступа, основанные на утверждениях. Нужно щелкнуть правой кнопкой мыши на этой папке и, вызвав окно ее свойств, найти вкладку **Классификация** (Classification). Здесь должно присутствовать свойство ресурса, которые мы создали ранее. Это хороший признак того, что в ходе настройки DAC все идет так как нужно.



Если вы не нашли на вкладке **Классификация** (Classification) свойство ресурса или набор свойств, это может означать, что в вашем домене требуется дополнительное время на репликацию изменений. Вы можете принудительно запустить обновление, выполнив в Windows PowerShell команду `Update-FSRMClassificationpropertyDefinition`.

Применение к папке централизованной политики

Прежде чем применять централизованную политику доступа к общей папке *Payroll*, следует выполнить принудительное обновление групповой политики,

для того чтобы централизованная политика, которую определяет GPO с именем Dynamic Access Control Policy, была применена к файловым серверам.

Далее следует открыть окно свойств папки, перейти на вкладку Безопасность (Security) и нажать кнопку Дополнительно (Advanced). В появившемся окне следует перейти на вкладку Централизованная политика (Central Police) и щелкнуть на ссылке Сменить (Change). Здесь из раскрывающегося меню нужно выбрать централизованную политику доступа (в данном случае это политика, которую мы назвали Domain File Server Policy), нажать Применить (Apply) и щелкнуть на кнопке ОК (рис. 5.6).

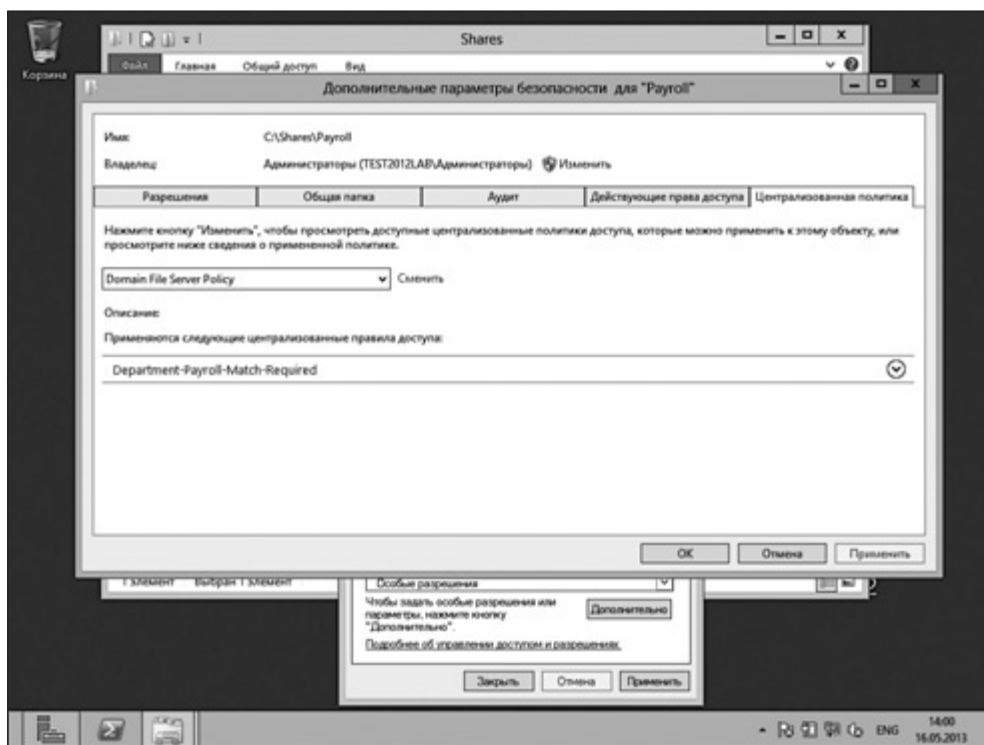


Рис. 5.6. Применение централизованной политики к общей папке

Проверка конфигурации

После того как заданы описанные ранее настройки, конфигурацию нужно протестировать, для того чтобы убедиться в ее работоспособности. DAC

обладает весьма удобной возможностью, которая заключается в просмотре действующих разрешений пользователей, определяемых настройкой системы. Посмотрим действующие разрешения, относящиеся к папке *Payroll*, у двух пользователей домена. Пользователь Betty Test является членом группы безопасности Executives, но не группы Payroll. Пользователь Henry Рум является членом группы Payroll.

Если DAC настроен верно, у пользователя Betty Test не должно быть доступа к общей папке *Payroll*. В окне свойств папки *Payroll* на вкладке **Безопасность** (Security) нажмите кнопку **Дополнительно** (Advanced). Как и ожидалось, у учетной записи пользователя Betty Test нет доступа к папке *Payroll* (рис. 5.7).

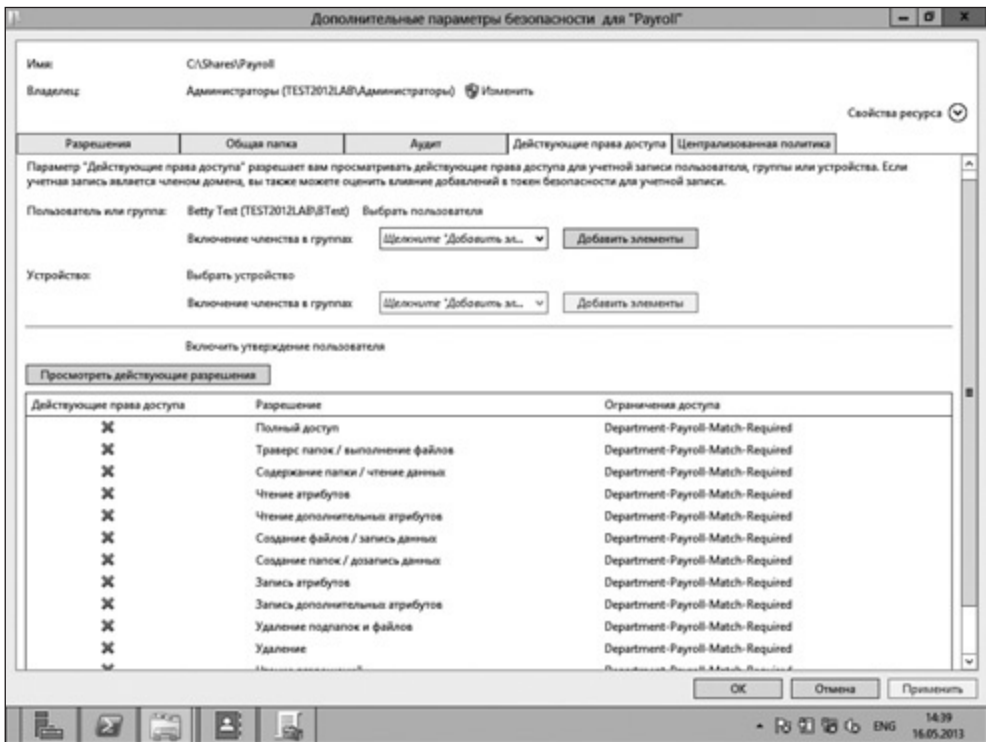


Рис. 5.7. DAC не дает этому пользователю доступ к общей сетевой папке

Просмотр действующих разрешений пользователя Henry Рум позволяет сделать вывод о том, что у него есть полный доступ к общей папке *Payroll*.

Это подтверждает, что DAC выполняет свои функции так, как нам нужно (рис. 5.8).

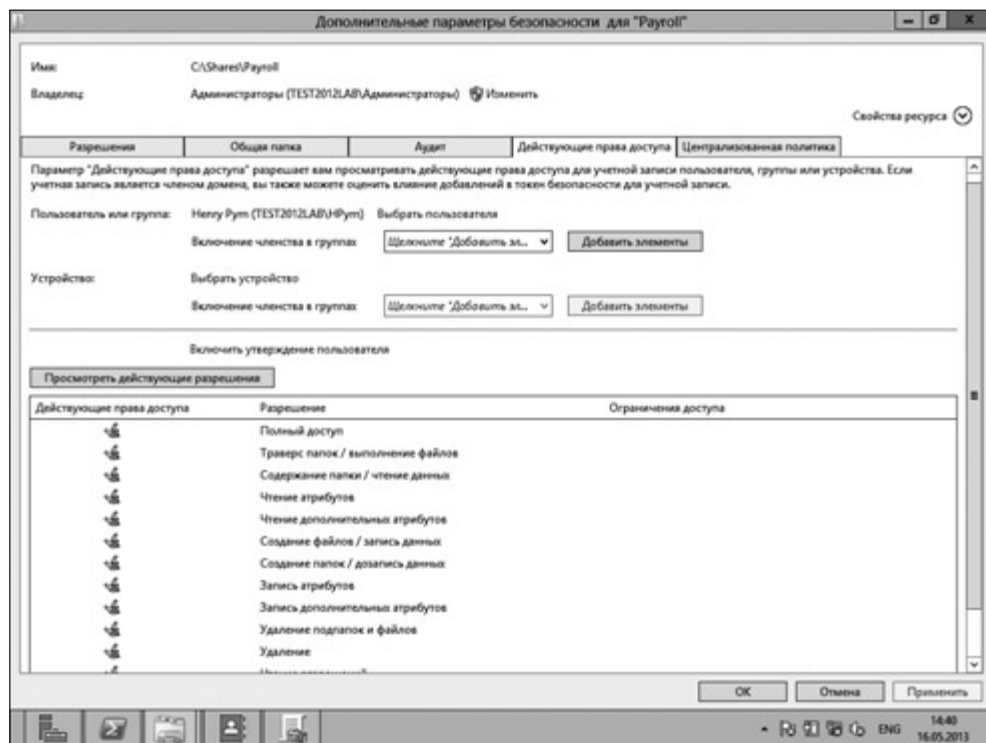


Рис. 5.8. У этого пользователя есть полный доступ к общей папке, настроенной с помощью DAC

Здесь приведен очень простой пример развертывания DAC, однако это отличный способ ознакомиться с основами данной технологии и сделать первые шаги в работе с ней.

Помощь при ошибке «Отказано в доступе»

Технология динамического контроля доступа (Dynamic Access Control) подразумевает возможность задавать сообщение, которое пользователь домена увидит в том случае, если он не может получить доступа к файлу или папке

из-за проблем с разрешениями. Этот механизм включает в себя настройку уведомлений, отправляемых по электронной почте владельцу данных или в IT-подразделение организации (или любому пользователю, который может проверить обоснованность попытки доступа к данным и предоставить такой доступ). Данная возможность реализуется в рамках функции помощи при ошибке «Отказано в доступе» (Access Denied Remediation).

В то время как Microsoft говорит о данной возможности как о еще одном улучшении DAC (и не поймите меня неправильно, это так и есть), я думаю, что основное преимущество от использования функции помощи при ошибке «Отказано в доступе» можно получить при использовании ее для быстрого решения проблем, которые могут возникать в процессе развертывания DAC. DAC не похож на те средства, которыми большинство из нас пользовались для управления разрешениями в сетевой инфраструктуре. Вполне вероятно, что при его развертывании будут возникать различные неувязки. С помощью функции помощи при ошибке «Отказано в доступе» проблемы, возникающие при управлении разрешениями, можно решать быстро и делать это централизованно.

Развертывание системы помощи при отказе в доступе

Сконфигурировать систему помощи при ошибке «Отказано в доступе» можно как для отдельных файловых серверов, так и для домена в целом. При развертывании в домене настройка данного компонента производится посредством групповой политики. На отдельных файловых серверах развертывание выполняется помощью диспетчера ресурсов файлового сервера (File Server Resource Manager).

Развертывание с помощью групповой политики

В окне Управление групповой политикой (Group Policy Management) щелкните правой кнопкой на политике для домена и выберите в появившемся меню команду Изменить (Edit). Пройдите по следующему пути: Конфигурация компьютера ► Политики ► Административные шаблоны ► Система ► Помощь при ошибке «Отказано в доступе» (Configuration ► Policies ► Administrative Templates ► System ► Access Denied Assistance). В открывшемся разделе вы увидите два параметра: Настроить сообщение об ошибке «Отказано в доступе» (Customize message) и Включить исправление ошибки «Отказано в доступе» для всех типов файлов клиента (Enable access denied assistance for Windows

clients). Первый элемент позволяет настроить инструкции, которые система помощи при отказе в доступе показывает пользователям. При настройке второго нужно учесть, что данная система поддерживается лишь Server 2012, Windows 8 и Windows RT.

Развертывание на файловом сервере

Для развертывания системы помощи при отказе в доступе на отдельных файловых серверах нужно воспользоваться диспетчером ресурсов файлового сервера (File Server Resource Manager). Здесь нужно щелкнуть правой кнопкой мыши на объекте Диспетчер ресурсов файлового сервера (локальный) (File Server Resource Manager (local)), выбрать в появившемся меню пункт Настроить параметры (Configuration Options), затем перейти на вкладку Помощь при отказе в доступе (Access Denied Remediation).

Здесь вы можете ввести собственный текст или использовать следующий встроенный макрос, создающий текст по шаблону:

- [Original File Path] (*путь к файлу*);
- [Original File Path Folder] (*путь к родительской папке файла, к которому пользователь пытается получить доступ*);
- [Admin e-mail] (*адрес электронной почты администратора*);
- [Data owner email] (*адрес электронной почты владельца данных*).

На рис. 5.9 показан пример сообщения системы помощи при отказе в доступе, настроенного администратором.

В настройке средства помощи при отказе в доступе есть некоторая гибкость. Например, вы можете задать различные сообщения об отказе в доступе для разных папок, используя диспетчер ресурсов файлового сервера (File Server Resource Manager). Это можно сделать, выполнив двойной щелчок на объекте Диспетчер ресурсов файлового сервера (локальный) (File Server Resource Manager (local)) и развернув группу Управление классификацией (Classification Management). Далее нужно щелкнуть правой кнопкой мыши на объекте Свойства классификации (Classification Properties) и выбрать команду Задать свойства управления папками (Set Folder Management Properties).

В поле Свойства (Properties) следует выбрать Сообщение для помощи при отказе в доступе (Access Denied Assistance Message) и нажать кнопку Добавить (Add). Теперь нужно перейти к папке, которой должно соответствовать данное сообщение, и либо создать собственное сообщение, либо воспользоваться макросом.



Рис. 5.9. Сообщение системы помощи при отказе в доступе, настроенное администратором

Настроить сообщение электронной почты можно, щелкнув правой кнопкой мыши на объекте Диспетчер ресурсов файлового сервера (локальный) (File Server Resource Manager (local)), выбрав в появившемся меню пункт Настроить параметры (Configuration Options), а затем перейдя на вкладку Уведомления (E-mail notification).

Аудит

Аудит — это еще один компонент системы динамического контроля доступа, претерпевший обновление. Windows Server 2008 и 2008 R2 создают события аудита всякий раз, когда происходит доступ к файлу. В Server 2012 система аудита централизована и более гибко подходит к процессу наблюдения за файлами.

С помощью системы аудита доступа к файлам в Server 2012 вы можете отслеживать изменения в централизованных правилах доступа и политиках, определениях утверждений и атрибутах файлов и, конечно, наблюдать за доступом к данным.

Если вы администрировали серверы, работающие на платформе Windows, или сейчас занимаетесь этим, то понимаете важность аудита. Он весьма важен при выполнении упомянутых ранее требований законодательных актов, когда нужно знать, кто получал доступ к конкретным данным. Кроме того, аудит важен в системе внутренней безопасности организации — для защиты интеллектуальной собственности и предотвращения утечек данных.

Усилив возможности аудита в Windows Server 2012, Microsoft пошла дальше, вместе с партнерами работая над решениями для интерпретации и анализа результатов аудита. Собственный продукт Microsoft, System Center Operations Manager (SCOM), предназначен для работы вместе с Server 2012. SCOM предоставляет инструменты для анализа результатов аудита.

Для настройки аудита на уровне домена достаточно выполнить пару шагов. Сначала надо настроить аудит доступа к глобальным объектам (Global Object Access Policy). Для этого следует открыть окно управления групповой политикой (Group Policy Management) для нужной политики и пройти по пути: Конфигурация компьютера ► Политики ► Конфигурация Windows ► Параметры безопасности ► Конфигурация расширенной политики аудита ► Политики аудита ► Доступ к объектам ► Аудит файловой системы (Computer Configuration ► Policies ► Windows Settings ► Security Settings ► Audit Policies ► Object Access ► Audit File System Properties). Здесь в окне свойств аудита файловой системы (рис. 5.10) следует установить флажок Настроить следующие события аудита (Configure the following audit events), а также флажки Успех (Success) и Отказ (Failure).

На панели навигации в разделе «Политики аудита» («Audit Policies») нужно щелкнуть на пункте Аудит доступа к глобальным объектам (Global Object Access Auditing), после чего сделать двойной щелчок на параметре Файловая система (File System). В появившемся окне нужно установить флажок Определить этот параметр политики (Define this policy setting) и нажать кнопку Настроить (Configure).

Будет открыто окно Дополнительные параметры безопасности для «Глобальный системный список управления доступом к файлам» (Advanced Security Settings for Global File SACL (security access control lists)). Здесь нужно щелкнуть на кнопке Добавить (Add), затем на ссылке Выберите субъект (Select a principal).

В случае с глобальной политикой обычно выбирают Все (Everyone), Полный доступ (Full Control) и затем Разрешения (Permissions).

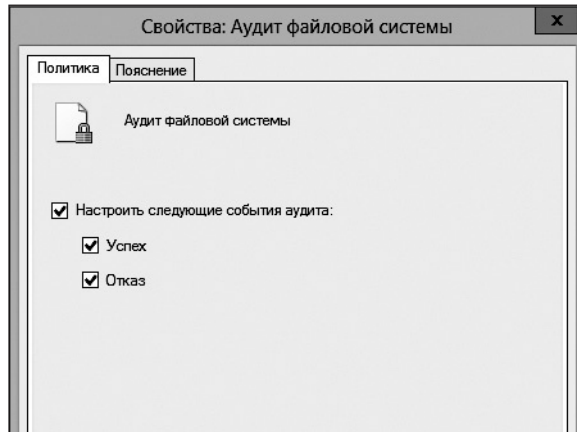


Рис. 5.10. Настройка события аудита при конфигурировании групповой политики

Именно здесь задают условия, которые хотят отслеживать. Например, если вам нужно знать, что происходит с общей папкой *Payroll* и файлами, которые в ней находятся, можно установить следующее:

```
[Ресурс][Department][Любой из][Значение][Payroll] ([Resource][Department]  
[Any of ][Value][Payroll])
```

После завершения работы с данным окном нужно три раза нажать кнопку ОК, для того чтобы вернуться на панель навигации. Здесь, для того чтобы завершить настройку, следует щелкнуть на пункте Доступ к объектам (Object Access) и сделать двойной щелчок на пункте Аудит работы с дескрипторами (Audit Handle Manipulation). В появившемся окне следует установить флажки Настроить следующие события аудита (Configure the following audit events), Успех (Success) и Отказ (Failure).

Когда политика аудита для домена будет настроена, нелишне запустить обновление групповой политики. Для того чтобы проверить правильность настроек аудита, например, для общей папки, вы можете изменить файл в папке и воспользоваться средством просмотра событий (Event Viewer), для того чтобы проверить, происходят ли события 4656 и 4663.

Автоматическая классификация файлов

Как и аудит, классификация файлов — это привычная возможность в ОС семейства Windows Server, однако в Server 2012 она была расширена. Классификация файлов добавляет в арсенал администратора мощные средства в виде правил классификации данных.

С помощью правил классификации вы можете, например, автоматически выполнить поиск строки «Конфиденциально» в заданном наборе файлов. Если эта строка присутствует в файле, ему можно присвоить высокий (High) уровень важности.

Правила классификации можно использовать для того, чтобы определять файлы с секретной информацией. Например, документы, содержащие номера социального страхования (Social Security) или сведения о здоровье пациентов.

Для развертывания системы автоматической классификации файлов следует начать с определения свойств ресурсов. На контроллере домена нужно запустить центр администрирования Active Directory (ADAC). Затем щелкнуть на пункте Динамический контроль доступа (Dynamic Access Control), после чего выбрать объект Resource Properties (Свойства ресурсов). Здесь нужно щелкнуть правой кнопкой мыши на свойстве (например, свойстве Impact), выбрать для него команду Включить (Enable), а затем включить свойство ресурса Personally Identifiable Information (Персональные данные).

Далее следует создать правило классификации содержимого (Content Classification Rule). Это делается на файловом сервере, который содержит данные, подлежащие классификации. На этом сервере нужно, используя учетную запись администратора, выполнить следующую команду:

```
Update-FSRMClassificationpropertyDefinition
```

Эта команда синхронизирует определения свойств, включенные на контроллере домена, с файловыми серверами. Далее выполните следующие шаги:

1. Запустите диспетчер ресурсов файлового сервера (File Server Resource Manager), разверните группу Управление классификацией (Classification Management), щелкните правой кнопкой мыши на объекте Правила классификации (Classification Rules) и в появившемся меню выберите команду Настроить расписание классификации

(Configure Classification Schedule). Установите флажки Включить фиксированное расписание (Enable fixed schedule) и Разрешить постоянную классификацию для новых файлов (Allow continuous classification for new files). Укажите день, когда вы хотите выполнять данную процедуру, и нажмите ОК.

2. Щелкните правой кнопкой мыши на объекте Правила классификации (Classification Rules) и выберите в появившемся меню команду Создать правило классификации (Create Classification Rule). Назовите ваше правило «Company Confidential» (Конфиденциально).
3. На вкладке Область (Scope) щелкните на кнопке Добавить (Add) и выберите папки, которые следует включить в правило. На вкладке Классификация (Classification) настройте следующее:
 - параметр Выберите метод назначения свойства файлам (Choose a method to assign a property to files) установите в значение Классификатор содержимого (Content Classifier);
 - параметр Выберите назначаемое свойство (Choose a property to assign to files) установите в значение Impact;
 - параметр Укажите значение (Specify Value) установите в значение High (Высокий уровень).
4. Теперь щелкните на кнопке Настроить (Configure), которая находится в группе Параметры (Parameters). Здесь в поле Тип выражения (Expression Type) нужно выбрать Строка (String), в поле Выражение (Expression) следует ввести «Company Confidential». В поле Тип выражения (Expression Type), кроме того, можно выбрать строковый тип выражения, чувствительный к регистру. Нажмите ОК.
5. На закладке Тип вычисления (Evaluation Type) установите флажок Заново определить существующие значения свойств (Re-evaluate existing property values) и выберите пункт Перезаписать существующее значение (Overwrite the existing values). Эта установка позволяет задать поведение системы при обнаружении конфликта между новыми и существующими значениями. Нажмите ОК.

Теперь у нас есть новое правило классификации, назначенное для выбранной папки. Благодаря ему осуществляется просмотр содержимого документов, расположенных в этой папке, на наличие текста «Company Confidential» (рис. 5.11).



Рис. 5.11. Правило классификации «Company Confidential»

Для того чтобы проверить правильность классификации файлов, нужно воспользоваться командой **Запустить классификацию со всеми правилами** (Run Classification with All Rules Now) для правила, находящегося в группе **Правила классификации** (Classification Rules) в диспетчере ресурсов файлового сервера (File Server Resource Manager). Благодаря этой команде для проверки используемых правил классификации будет запущено средство формирования отчета об автоматической классификации (Automatic Classification Report).

Шифрование классифицированных файлов

Когда данные классифицированы, вы можете зашифровать их с использованием средства шифрования сервера управления правами (Rights Management Server, RMS). Используя RMS, можете автоматически защищать документы, основываясь на их классификации.

Создадим правило для классификации любых документов, расположенных в папке *HR*, как документов высокой важности (High) в том случае, если в них обнаружена строка «Company Confidential». В диспетчере ресурсов файлового сервера (File Server Resource Manager) на файловом сервере, где расположена папка *HR*, нужно выбрать объект **Задачи управления файлами** (File Management Tasks) и щелкнуть правой кнопкой мыши, для того чтобы открыть меню, содержащее команду **Создать задачу управления файлами** (Create File Management Task).

Дадим создаваемой задаче имя «High Business Impact» («Высокий уровень важности») и описание «Автоматическая RMS-защита конфиденциальных документов» («Auto RMS protection for confidential docs»). На вкладке

Область (Scope) нужно включить параметр Файлы группы (Group Files). На вкладке Расписание (Schedule) задать расписание запуска (рекомендуется выполнять подобные задачи хотя бы раз в неделю). В группе параметров Непрерывное выполнение (Continuous operation) следует выбрать значение Выполнять непрерывно для новых файлов (Run task continuously on new files). На закладке Действие (Action) параметр Тип (Type) нужно установить в значение Шифрование RMS (RMS Encryption). Теперь добавим папку, для которой планируется выполнять эту задачу, и запустим задачу, чтобы проверить правильность настроек.

Выводы

Если раньше вы не работали с системой динамического контроля доступа, будьте готовы к тому, что вам понадобится некоторое время, чтобы привыкнуть к ней. Процесс ее развертывания состоит из множества небольших шагов, необходимых для того, чтобы обойти все настраиваемые параметры. Возможности новой системы контроля доступа простираются далеко за пределы механической настройки NTFS-разрешений.

Время от времени вы можете сталкиваться с некоторыми подводными камнями. Поэтому не занимайтесь освоением DAC, разворачивая эту систему в рабочей среде. Сначала протестируйте ее и посмотрите, как развертывание DAC повлияет на существующие разрешения.

DAC представляет собой весьма значительное улучшение Windows Server 2012. Ее мощь особенно очевидна в доменах уровня функциональности Windows Server 2012, в которых работают контроллеры домена под управлением Server 2012 и клиентские системы с установленной Windows 8. Однако вы можете начать использовать DAC, развернув минимальную инфраструктуру с контроллером домена и файловым сервером, работающим под управлением Windows Server 2012.

6 Управление хранилищами и кластеризация

Объемы данных, с которыми мы работаем, растут день ото дня, как и наша зависимость от компьютерных систем. Именно поэтому организация хранилищ данных и поддержка высокого уровня доступности систем хранения актуальны сегодня как никогда. Возможность гибкого развертывания эффективных систем хранения данных и управления ими играют важнейшую роль в организации здоровой ИТ-инфраструктуры.

Server 2012 предлагает новые компоненты и улучшения, предназначенные для организации хранилищ данных. Они позволяют поддерживать работоспособность инфраструктуры при системных сбоях или повреждениях информации. Технологии Storage Spaces (пространства данных) и ReFS (Resilient File System, отказоустойчивая файловая система) — это два важнейших нововведения Server 2012, которые нацелены на поддержание работоспособности хранилищ данных.

Пространства данных — это новый компонент, который устанавливается вместе с ролью Файловые службы и службы хранения (File and Storage Services). Пространства данных — это недорогая альтернатива RAID (но не заменитель, так как они основаны на программных механизмах, а многие RAID-решения для бизнеса зависят от аппаратных RAID-контроллеров).

С помощью пространств данных вы можете работать с дисками, обладающими интерфейсами SATA, SAS и даже USB. Эта технология позволяет создавать пулы устройств хранения данных и добавлять в систему дополнительное пространство для хранения данных.

Хранение данных позволяет экономно использовать ресурсы благодаря применению виртуальных жестких дисков. Можно создавать пулы устройств хранения данных (storage pools) для внутренних и внешних жестких дисков, то есть виртуальные диски, созданные из физических дисков. В свою очередь, эти пулы также можно настраивать с помощью пространств данных.

Кроме того, с помощью этой технологии можно динамически регулировать доступный объем дискового пространства. Это позволяет не только масштабировать хранилище данных, но и обеспечить отказоустойчивость системы, так как вы можете создавать пространства данных, которые поддерживают зеркалирование и контроль целостности данных за счет избыточности.

Благодаря гибкости, которую предлагают пространства данных, организации могут развертывать решения для хранения данных, такие как SAN (Storage Area Networks, сети хранения данных), с использованием протокола iSCSI без вложений в аппаратное обеспечение, которые обычно ассоциируются с развертыванием таких решений.

ReFS (Resilient File System, отказоустойчивая файловая система) — это новая файловая система, которая появилась в Server 2012. Ключ к пониманию основного предназначения ReFS заключается в понятии «отказоустойчивость». В ReFS все нацелено на обеспечение целостности данных, то есть на то, чтобы данные были меньше подвержены искажениям. Это уменьшает вероятность потери информации.

ReFS создана для работы совместно с пространствами данных. В частности, для пространств данных с зеркалированием. При использовании технологии зеркалирования данные, целостность которых нарушена, автоматически восстанавливаются на зеркалированных томах. Поскольку ReFS использует встроенные метаданные, хранящие контрольные суммы, она не только подходит для создания пространств данных на базе виртуальных дисков, которые обеспечивают отказоустойчивость, но и позволяет масштабировать системы хранения данных. Кроме того, ReFS поддерживает автоматическое восстановление поврежденных данных.

Я могу представить себе лишь одну причину для дискуссий вокруг пространств данных. Это функциональное RAID-решение, но реализовано оно программно. Программный RAID-массив отлично подойдет многим организациям в качестве отказоустойчивого решения для хранения данных. Однако

те организации, для которых отказоустойчивость имеет первостепенную важность, могут предпочесть использовать аппаратные RAID-решения сторонних разработчиков. Аппаратные RAID-массивы имеют некоторые преимущества в сравнении с программными. Они могут быть созданы на базе выделенного аппаратного обеспечения, независимого от какого-либо сервера и не нагружающего сервер дополнительными задачами. Потенциальная проблема аппаратных RAID-массивов заключается в том, что при отказе RAID-контроллера может быть разрушена вся система хранения данных. Конечно, от проблем не избавлены и программные решения наподобие пространств данных. Например, если зеркалированные тома окажутся поврежденными, все данные подвергнутся риску.

Вы можете развернуть систему пространств данных для использования в качестве файлового сервера, который поддерживает функцию защиты данных. Это потребует развертывания файлового сервера, подключенного к дисковой конфигурации JBOD (Just a Bunch of Disks, простой массив дисков), с использованием дисков с интерфейсами SATA или SAS. Также вы можете использовать пространства данных в серверном кластере, состоящем из двух узлов, для обеспечения отказоустойчивости.

Пространства данных могут оказаться настоящей находкой для организаций, которые желают внедрить недорогое решение для хранения данных. Эта технология может быть использована для развертывания систем NAS (Network-Attached Storage, хранилище, подключенное к сети) и SAN (Storage Area Network, сеть хранения данных), что при обычном подходе требует покупки дополнительного аппаратного обеспечения. Преимущества использования пространств данных в сравнении с аппаратными решениями сторонних разработчиков в итоге зависят от требований, которые предъявляет ваша инфраструктура к системам хранения данных и их отказоустойчивости.

Сравнение ReFS и NTFS

ReFS не предназначена для использования вместо NTFS, скорее как дополнение к ней. С ReFS-тома нельзя произвести загрузку операционной системы, нельзя производить непосредственное преобразование NTFS-томов в ReFS-тома. ReFS создана для организации хранилищ с возможностью коррекции данных.

Так как ReFS представляет собой развитие NTFS, эти две файловые системы имеют некоторые общие черты (табл. 6.1).

Таблица 6.1. Сравнение NTFS и ReFS

Атрибут	NTFS	ReFS
Максимальный размер файла	2^{64} — 1 Кбайт	2^{64} — 1 Кбайт
Максимальный размер тома	2^{64} кластеров	2^{78} байт при размере кластера 16 Кбайт ($2^{64} \cdot 16 \cdot 2^{10}$). Система адресации Windows поддерживает 2^{64} байт
Максимальное количество файлов в папке	4 294 967 295	2^{64}

Кроме того, ReFS поддерживает пулы хранения данных объемом до 4 Пбайт. Количество пулов хранения данных и пространств данных, которые можно создать, не ограничено.

Существует несколько сценариев развертывания пространств данных. В следующем разделе описаны некоторые основные параметры установки, знание которых позволит вам начать пользоваться этой системой.

Создание пространства данных

Пространство данных можно создать из диспетчера серверов, используя неформатированные диски. Пространства данных устанавливаются вместе с компонентом службы хранения данных (Storage Services) при установке роли **Файловые службы и службы хранения** (File and Storage Services). Все они устанавливаются по умолчанию как часть сервера с графическим интерфейсом.

Выполняя описанные далее шаги, вы можете использовать внешний USB-диск для создания пространства данных. Конечно, можно воспользоваться различными неформатированными дисками, подключаемыми по USB, SATA или SAS.

В диспетчере серверов перейдите в раздел **Файловые службы и службы хранения** (File and Storage Services), затем в раздел **Диски** (Disks) и создайте новый том. Для этого щелкните правой кнопкой мыши на диске и выберите команду **Создать том** (New Volume). Два раза щелкните на кнопке **Далее** (Next).

Мастер создания томов (New Volume Wizard) распознает неформатированный диск и инициализирует его как GPT-диск (диск с таблицей разделов GUID). На следующем экране задайте размер тома, затем можете назначить букву диска и при необходимости назначить его папке. Обычно, назначая диску букву, для этих параметров оставляют значения по умолчанию. Щелкните на кнопке **Далее** (Next). Вы можете указать для форматирования диска файловую систему ReFS, выбрав соответствующий пункт из списка **Файловая система** (File System). Щелкните еще раз на кнопке **Далее** (Next), а затем на кнопке **Создать** (Create).

Теперь создадим новый пул хранения данных для нашего пространства данных. В разделе **Файловые службы и службы хранилища** (File and Storage Services) на панели мониторинга диспетчера серверов нужно перейти в раздел **Пулы носителей** (Storage Pools).

В списке **Пространства данных** (Storage Spaces) вы увидите диск с именем **Primordial** (Исходный). Термин *Primordial* обычно используется для указания

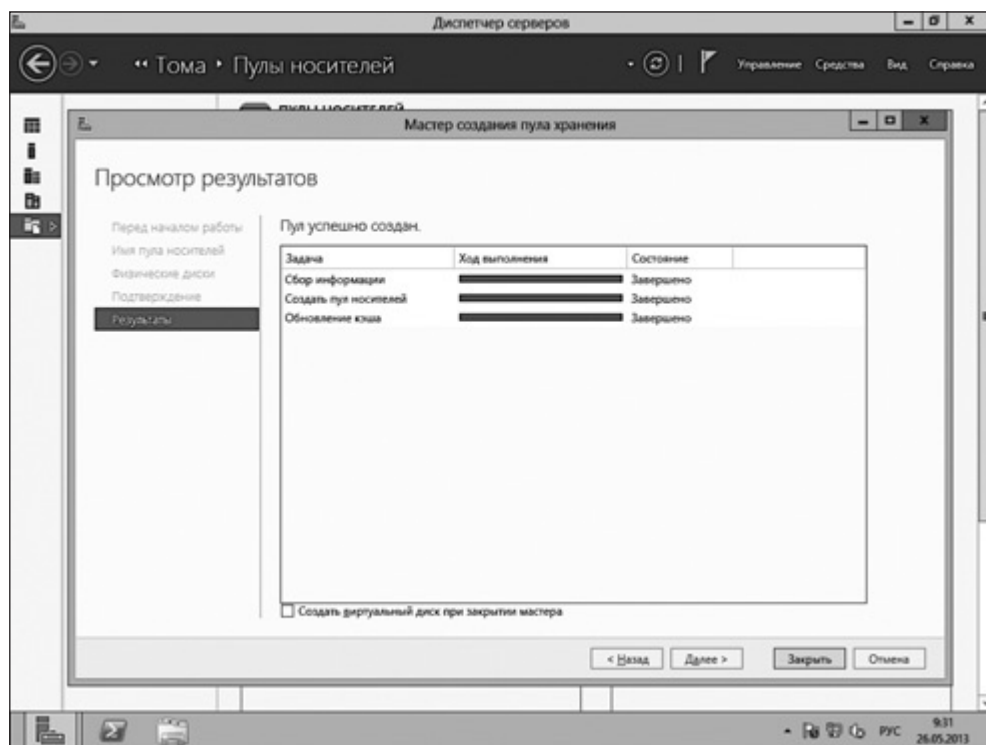


Рис. 6.1. Новый пул хранения данных

на то, что пространство диска не отформатировано, не подготовлено к работе, диску не назначена емкость. Щелкните на диске и из меню **Задачи** (Tasks) выберите **Создать пул носителей** (New Storage Pool). Это приведет к запуску мастера создания пула хранения (New Storage Pool Wizard). Теперь нажмите кнопку **Далее** (Next), дайте имя новому пулу и еще раз нажмите **Далее** (Next). Укажите диски для добавления в пул, еще раз нажмите **Далее** (Next), а затем кнопку **Создать** (Create). На рис. 6.1 вы видите экран подтверждения операции создания пула хранения данных.

Теперь в области **Пространства данных** (Storage Spaces) имеется новый пул хранения (рис. 6.2).

Далее в пространстве данных вы можете создать виртуальный диск с возможностью зеркалирования и контроля четности. В окне **Виртуальные диски** (Virtual Disks) воспользуйтесь командой **Создать виртуальный диск** (New Virtual Disk) из меню **Задачи** (Tasks). Выберите пул хранения данных и дайте

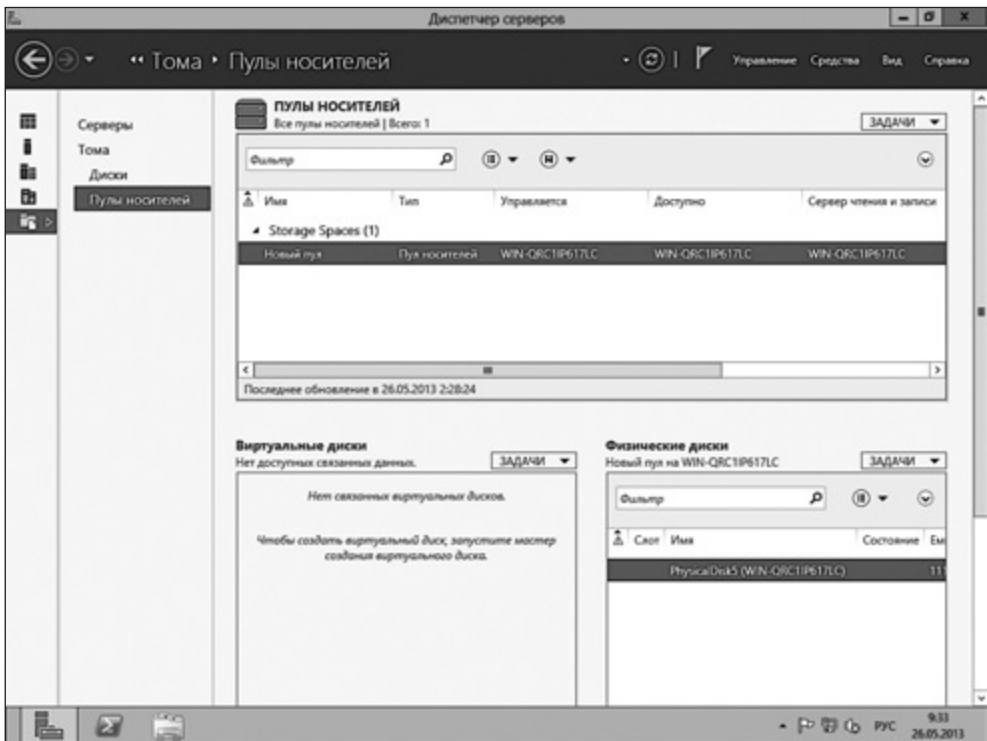


Рис. 6.2. Новое пространство данных

имя виртуальному диску. Если вы хотите настроить зеркальный том для хранения файловых ресурсов подразделений организации, нужно назвать виртуальный диск соответствующим образом, например «Файловые ресурсы подразделений» («Department Shares»), и нажать **Далее (Next)**.

В Windows Server 2012 есть три варианта настройки хранилища:

- *Простое (Simple)*. В этом режиме данные будут распределены между физическими дисками, на которых основан виртуальный диск. Этот вариант эквивалентен конфигурации RAID 0. Он используется для увеличения производительности, но не для обеспечения отказоустойчивости или резервирования данных.
- *Зеркальное (Mirror)*. Обычно этот вариант настройки используется вместе с пространствами данных. Благодаря зеркалированию копии данных хранятся на двух или трех дисках. Эта установка эквивалентна конфигурации RAID 1, она обеспечивает отказоустойчивость.
- *Контроль четности (Parity)*. Это вариант конфигурации RAID 5, реализованной с помощью пространств данных. Контроль четности — это самая надежная технология обеспечения отказоустойчивости, но она использует больше дискового пространства, чем зеркалирование, и требует, чтобы в пуле присутствовало как минимум три физических диска.

После выбора конфигурации хранилища вы можете задать параметр экономного (thin, его иногда называют и просто тонким) или фиксированного (fixed) выделения ресурсов для виртуальных дисков. Экономное выделение ресурсов позволяет динамически выделять необходимое пространство, основываясь на размере тома. Применение фиксированного выделения означает использование виртуальным диском физического пространства, равного размеру тома. Если в вашем рабочем окружении данные накапливаются быстро, использование экономного выделения ресурсов предпочтительнее. В частности, это дает больше возможностей масштабирования инфраструктуры.

Теперь нужно задать размер виртуального диска, щелкнуть на кнопке **Далее (Next)**, затем на кнопке **Создать (Create)**. После этого настройка пространств данных завершится. При этом, если нужно, хранилище будет поддерживать отказоустойчивость, зеркалирование и контроль четности. Пространства данных сравнительно быстро и легко развернуть, они выполняют роль эффективного хранилища данных, использование которого не требует покупки дополнительного аппаратного или программного обеспечения.

Кластеризация

В дополнение к гибким решениям для организации хранилищ данных, внедрение которых не грозит перерасходом ИТ-бюджета, новые возможности Server 2012 в области кластеризации позволяют сохранить работоспособность бизнес-среды даже в случае возникновения форс-мажорных обстоятельств.

Кластеризация — это один из лучших способов обеспечения отказоустойчивости и выполнения резервирования инфраструктуры. Благодаря кластеризации несколько серверов (узлов) работают совместно, что приводит к улучшению производительности благодаря балансировке нагрузки. Также подобная схема работы обеспечивает отказоустойчивость системы и высокий уровень ее доступности (HA, high availability). Организации часто объединяют в кластеры серверы, выполняющие задачи особой важности. Например, такие, которые поддерживают работу баз данных или обеспечивают функционирование бизнес-приложений. В двух словах, кластеризация — это отличное решение для любых серверных приложений, простой или низкая производительность которых могут плохо сказаться на выполнении организацией ее основных задач.

Кластеризация в Server 2012 — это решение, которое позволяет организациям не нести дополнительных затрат при развертывании отказоустойчивых кластеров для поддержки важных систем. Дело в том, что эта функция присутствует в стандартной поставке Windows Server 2012 и для ее использования нужно лишь потратить некоторое время на установку и настройку служб. Кроме того, кластеры могут быть частью инфраструктуры при развертывании SAN, поддерживать системы хранения iSCSI, Fibre Channel и SAS. Конечно, кластеризация касается не только физических серверов, виртуальные машины (VM, virtual machines) также могут быть кластеризованы.

Члены кластера соединены LAN или WAN (локальной или глобальной сетью) и сгруппированы с помощью серверного программного обеспечения Windows. Самостоятельные сетевые узлы при объединении в кластер работают как единая система. Если один из них, выполняющий какую-либо задачу, окажется неработоспособным, другой сервер кластера немедленно, без задержки продолжит выполнять ту же задачу. Поддержка отказоустойчивости реализована бесшовно. Поэтому вам не нужно выполнять какие-либо промежуточные настройки ни на узле, который принимает на себя нагрузку, ни на пользовательских рабочих местах. Например, нет нужды в настройке перенаправления клиентских подключений на резервный сервер

Хотя кластеризация существует уже довольно давно — впервые она появилась еще в Windows NT 4.0 Enterprise Server, — теперь в ней присутствует немало новых возможностей и улучшений, которые упрощают управление кластером.

Обеспечение высокой доступности — это не единственная цель технологий кластеризации в Server 2012. Не меньшую значимость имеет и высокая масштабируемость решений. Server 2008 R2 x64 Enterprise поддерживает до 16 узлов в кластере. Hyper-V R2 с Server 2008 R2 SP1 поддерживает до 1000 виртуальных машин в кластере (при развертывании в режиме использования пяти узлов, четыре из которых активны, а один нужен для обеспечения отказоустойчивости). Server 2012 поддерживает до 64 узлов в кластере, а Hyper-V R3 — весьма впечатляющие 4000 виртуальных машин на кластер!

Обновление отказоустойчивых кластеров с поддержкой доступности (Cluster-Aware Updating, CAU) — это новый компонент, весьма ожидаемый системными администраторами Windows. CAU позволяет узлам кластера выполнять обновления Windows, не прерывая работу.

Технология общих томов кластера (Cluster Shared Volumes, CSV) обновлена до версии 2.0. В Server 2008 R2 данный компонент можно было включить при организации отказоустойчивой кластеризации и использовать с виртуальными машинами Hyper-V. Благодаря CSV узлы кластера имеют доступ к кластеру, в котором эта функция включена. Программное обеспечение узлов, которые являются частью отказоустойчивого кластера, может исполняться на разных виртуальных машинах, которые работают с файлами, хранящимися на одном и том же томе. С помощью общих томов виртуальных машин легче создавать инфраструктуры SAN. При этом нужно меньше номеров логических устройств (LUN, Logical Unit Number, их используют для идентификации логических устройств на устройствах хранения данных в SAN-инфраструктурах), поскольку несколько виртуальных машин могут пользоваться одним и тем же томом. Это обеспечивает еще более высокий уровень доступности системы, так как каждая система может обрабатывать ситуацию отказа. Можно организовывать миграцию или перемещение виртуальной машины независимо от других виртуальных машин, использующих тот же самый том. Кроме того, при использовании технологии VHD (virtual hard disk, виртуальный жесткий диск) более эффективно используется дисковое пространство, так как VHD-файл не нужно размещать на другом диске.

CSV 2.0 демонстрирует нам очередной этап развития этой технологии: теперь CSV — это часть компонента отказоустойчивой кластеризации. Вы можете включить данную функцию буквально одним щелчком мыши. CSV-диски

будут отображаться в интерфейсе управления хранилищами данных диспетчера отказоустойчивости кластеров (Failover Cluster Manager Storage), что позволяет централизовать управление ими, а значит, сделать его более эффективным.

Настройка отказоустойчивого кластера

Перед установкой отказоустойчивого кластера важно спланировать количество узлов кластера, а для больших организаций — и количество создаваемых кластеров. Для отказоустойчивых кластеров в целях повышения доступности часто требуется отдельный диск или том, который называется *диск кворума* (*quorum disk*). С помощью Server 2012 маленькая организация может развернуть кластер, состоящий из двух узлов, но при установке будет выведено предупреждение о том, что для диска кворума не было найдено подходящего диска.

Хотя эта книга не нацелена на изучение тонкостей технологии кластеризации, важно, чтобы вы понимали их основы. «Кворум» — это один из терминов, который нуждается в дополнительных пояснениях.

Кластер может считаться кластером высокой доступности в том случае, если работают более половины его узлов. Эти узлы и называются *кворумом*. В двух словах, кворумы позволяют узлам отказоустойчивого кластера обмениваться друг с другом информацией.

При развертывании кластера, состоящего из двух узлов, можно воспользоваться конфигурацией кворума узла (Node) и диска (Disk). Эти конфигурации применимы при настройке диска кворума. Если же имеется как минимум три узла или нечетное количество узлов, будет установлена соответствующая конфигурация кворума, которую Windows настроит с помощью роли отказоустойчивого кластера.

Для начала установки отказоустойчивого кластера в диспетчере серверов щелкните на ссылке **Добавить роли и компоненты** (Add Roles and Features), нажмите кнопку **Далее** (Next) и выберите сервер, который будет использоваться в кластере. Снова нажмите **Далее** (Next), в левом меню выберите **Компоненты** (Features), в окне **Выбор компонентов** (Select features) установите флажок **Отказоустойчивая кластеризация** (Failover clustering) и добавьте необходимые дополнительные компоненты (в частности, **Средства управления отказоустойчивыми кластерами** (Failover Clustering Tools)) (рис. 6.3).

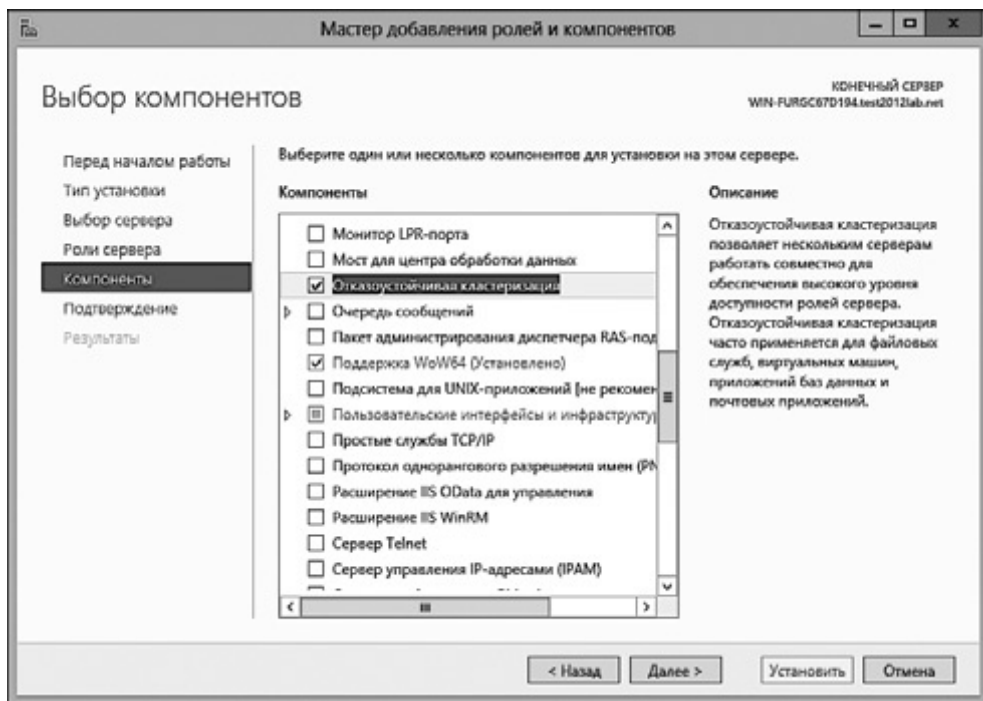


Рис. 6.3. Выбор компонента Отказоустойчивая кластеризация

Снова щелкните на кнопке **Далее** (Next), включите автоматический перезапуск сервера и нажмите кнопку **Установить** (Install).

Для того чтобы после установки запустить диспетчер отказоустойчивости кластеров (Failover Cluster Manager), воспользуйтесь меню **Средства** (Tools) диспетчера серверов.

Создание кластера

Чтобы создать отказоустойчивый кластер, воспользуйтесь командой **Создать кластер** (Create Cluster) из меню **Действия** (Actions) диспетчера отказоустойчивости кластеров (Failover Cluster Manager) (рис. 6.4).

Для того чтобы приступить к созданию кластера, введите имена серверов для кластера в ответ на соответствующий запрос мастера создания кластеров (Create Cluster wizard) (рис. 6.5).

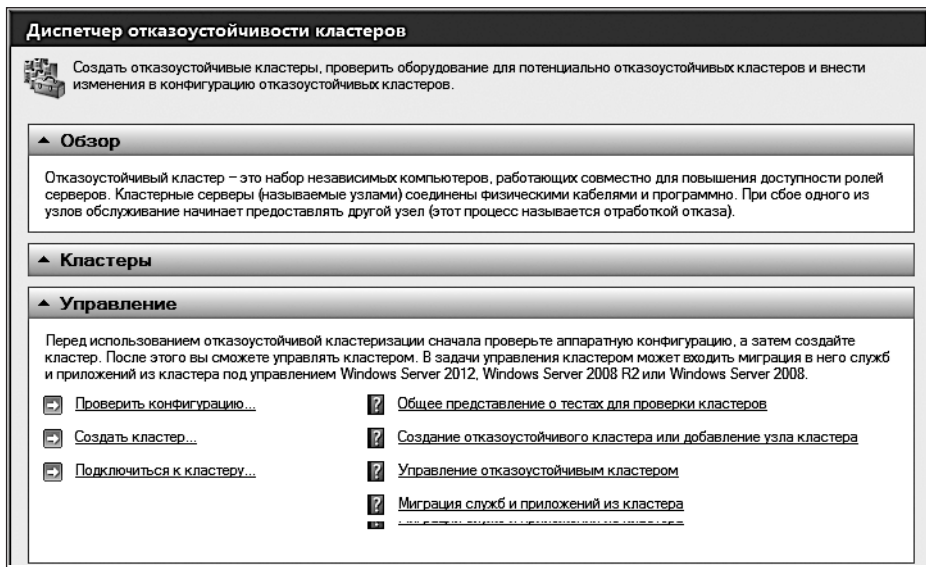


Рис. 6.4. Ссылка Создать кластер в Диспетчере отказоустойчивости кластеров

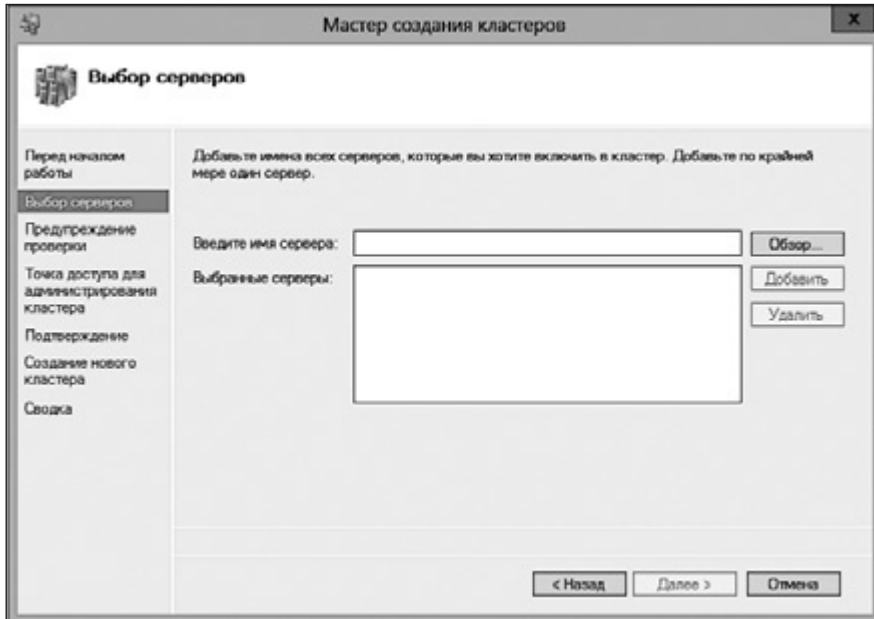


Рис. 6.5. Окно для выбора серверов, добавляемых в кластер

Затем нужно указать, следует ли выполнить проверочные тесты для создаваемого кластера (рис. 6.6).

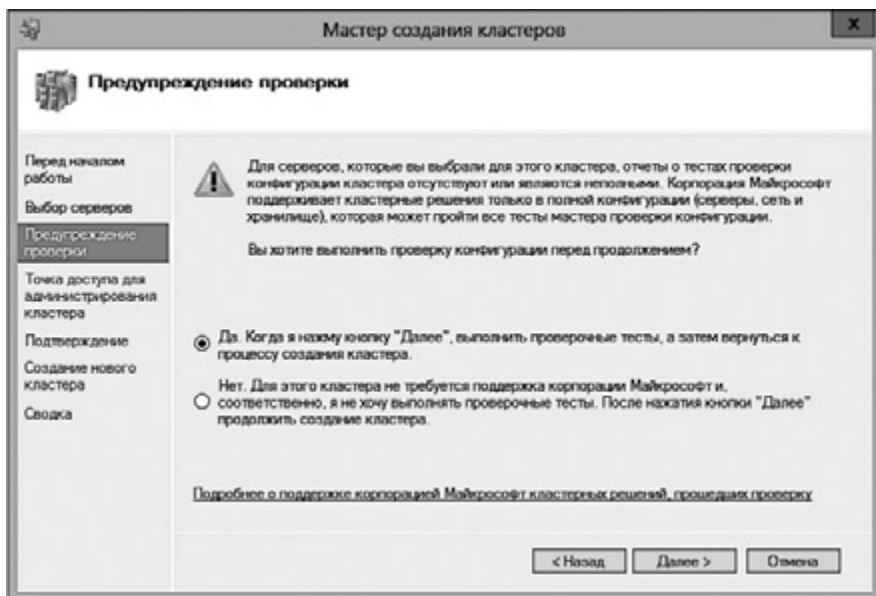


Рис. 6.6. Установка, позволяющая выполнить проверочные тесты



Если вы создаете кластер в рабочей бизнес-среде, вам придется выполнить проверочные тесты, так как Microsoft поддерживает только кластеры, прошедшие проверку.

Дважды щелкните на кнопке **Далее** (Next). Вы сможете либо запустить все проверочные тесты (именно так и рекомендуется поступить), либо выбрать отдельные тесты для запуска.

Когда тесты будут выполнены, система подготовит отчет о проверке отказоустойчивого кластера (Failover Cluster Validation Report), в котором будут представлены подробные сведения о пройденных и не пройденных тестах, а также — предупреждения (рис. 6.7).

И наконец, кластеру нужно дать имя и нажать кнопку **Готово** (Finish). После того как создание кластера завершится, выводится еще один отчет, содержащий сведения о создании кластера и его параметрах.

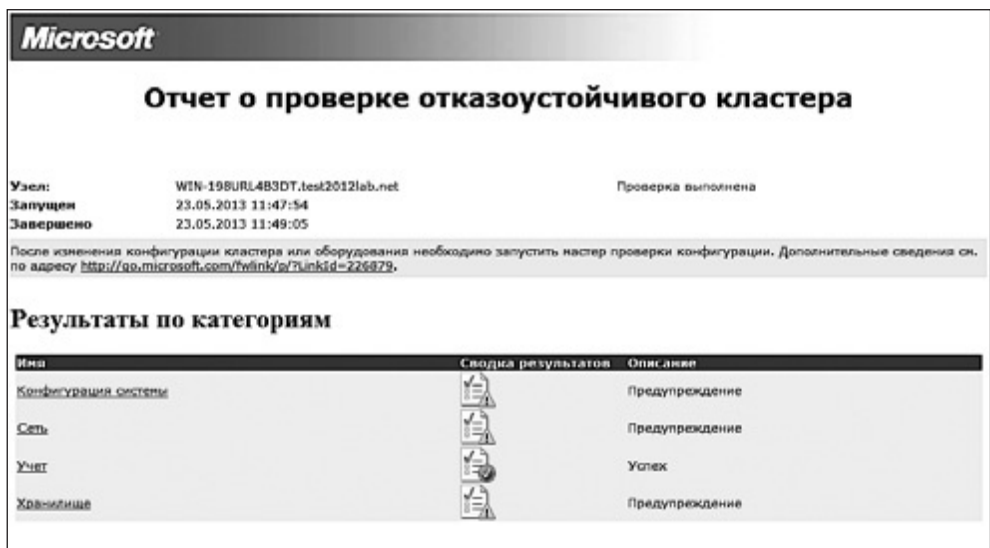


Рис. 6.7. Отчет о проверке отказоустойчивого кластера

На любой компьютер, который предполагается сделать частью кластера, нужно установить диспетчер отказоустойчивости кластеров (Failover Cluster Manager).

На следующем шаге нужно добавить в кластер узлы. Для этого следует воспользоваться ссылкой **Добавить узел** (Add Node) в окне диспетчера отказоустойчивости кластеров (Failover Cluster Manager) (рис. 6.8).

Если вы создаете отказоустойчивый кластер из двух узлов, после того как будет добавлен второй узел, мастер добавления узлов (Add Node Wizard) отобразит предупреждение (рис. 6.9).

Чтобы правильно настроить конфигурацию кворума кластера, нужно отредактировать свойства кластера. Для этого щелкните правой кнопкой мыши на имени кластера в левом меню диспетчера отказоустойчивости кластеров (Failover Cluster Manager) и выберите пункт контекстного меню **Дополнительные действия** (More Actions). Выберите команду **Настроить параметры кворума кластера** (Configure Cluster Quorum Settings) (рис. 6.10).

Будет открыт мастер настройки кворума кластера (Configure Cluster Quorum Wizard). Он предлагает три варианта конфигурации кворума кластера (рис. 6.11).

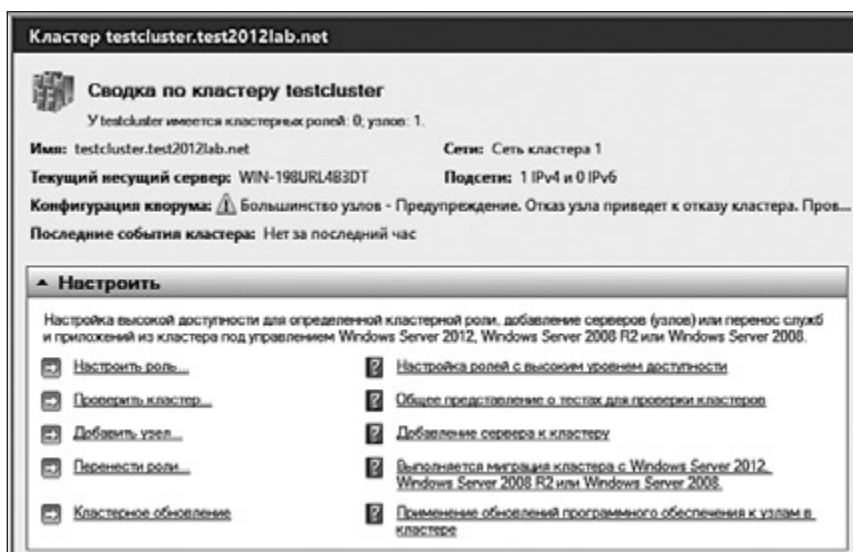


Рис. 6.8. Добавление узлов в кластер

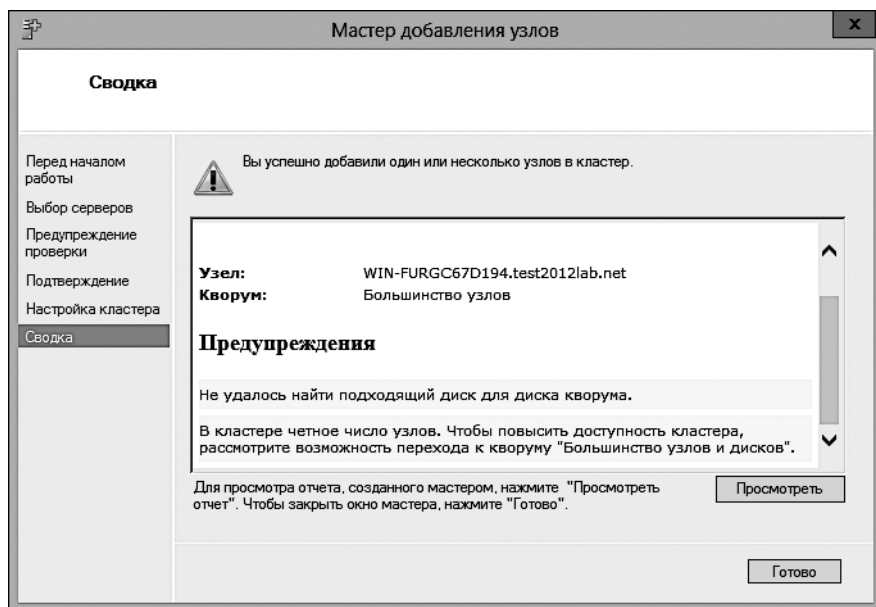


Рис. 6.9. Предупреждение об отсутствии диска кворума

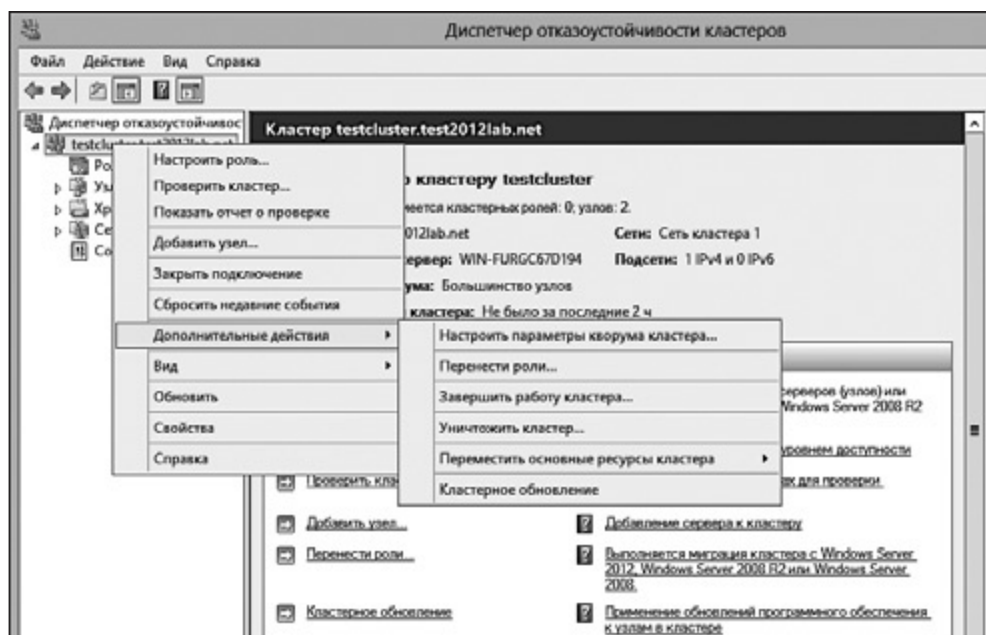


Рис. 6.10. Настройка параметров кворума кластера

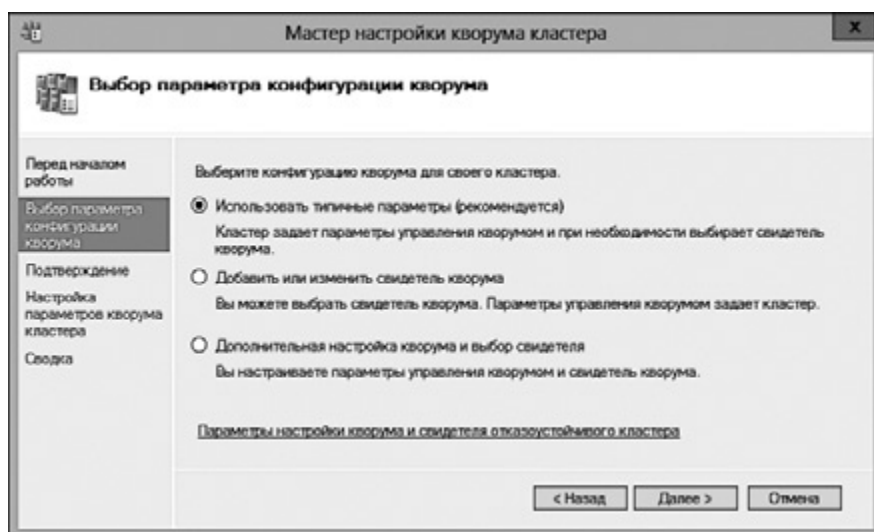


Рис. 6.11. Параметры конфигурации кворума

Если нет веских причин для использования особенной конфигурации кворума, лучше всего позволить программному обеспечению самостоятельно настроить кворум, выбрав первый вариант, **Использовать типичные параметры** (Use typical settings).

В соответствии с материалом Microsoft TechNet, который посвящен настройке отказоустойчивых кластеров (<http://technet.microsoft.com/en-us/library/cc770620%28v=ws.10%29.aspx>), настраивать кворумы кластеров в Server 2012 можно одним из четырех способов. Узлы в кластере могут голосовать за достижение кластером кворума:

- **Большинство узлов (Node Majority).** Каждый доступный узел может голосовать. Кластер работает лишь в том случае, когда имеется большинство голосов, то есть если их больше половины.
- **Большинство узлов и дисков (Node and Disk Majority).** Голосовать могут каждый доступный и работающий узел, а также диск, назначенный в кластерном хранилище данных (так называемый диск-свидетель (disk witness)). Кластер работает лишь в том случае, когда имеется большинство голосов, то есть их больше половины.
- **Большинство узлов и файловых ресурсов (Node and File Share Majority).** Голосовать могут каждый доступный и работающий узел, а также назначенный файловый ресурс, созданный администратором (так называемый файловый ресурс-свидетель (file share witness)). Кластер работает лишь в том случае, когда имеется большинство голосов, то есть их больше половины.
- **Без учета большинства голосов: только диск (No Majority: Disk Only).** В кластере имеется кворум в том случае, если доступен и работает хотя бы один узел с диском в кластерном хранилище данных.

Выбор варианта **Использовать типичные параметры** (Use typical settings) позволяет Server 2012 самостоятельно настроить кворум кластера.

Кластерное обновление

Обновление отказоустойчивых кластеров с поддержкой доступности (Cluster-Aware Updating, CAU) можно настроить с помощью диспетчера отказоустойчивости кластеров (Failover Cluster Manager), воспользовавшись ссылкой **Кластерное обновление** (Cluster-Aware Updating) (рис. 6.12).

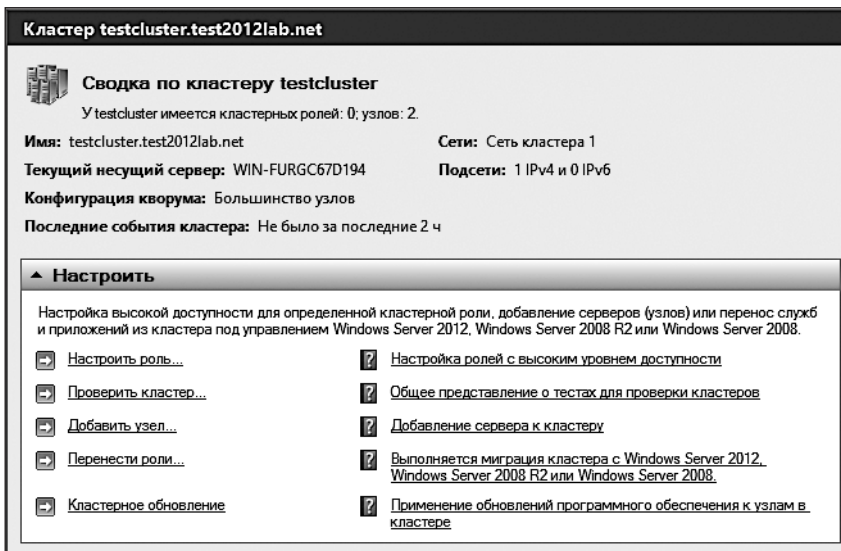


Рис. 6.12. Ссылка для запуска процесса настройки конфигурации кластерного обновления

Интерфейс окна Кластерное обновление (Cluster-Aware Updating) упрощает процесс обновления кластера. Подключитесь к кластеру и выберите параметры применения обновлений (рис. 6.13). Начните настройку параметров, воспользовавшись командой Настроить параметры самообновления кластера (Configure cluster self-updating options).

Будет запущен мастер настройки параметров самообновления (Configure Self-Updating Options wizard). Сначала он предложит вам добавить роль Кластерное обновление (Cluster-Aware Updating), которая необходима для работы механизма CAU.

В окне Добавить кластерную роль CAU с включенным самообновлением (Add CAU Clustered Role with Self-Updating Enabled) установите флажок Добавить в этот кластер кластерную роль CAU с включенным режимом самообновления (Add the CAU clustered role, with self-updating mode enabled, to this cluster) (рис. 6.14).

Щелкните на кнопке Далее (Next) и настройте расписание обновления. По умолчанию планировщик настроен на печально известный «патчевый вторник».

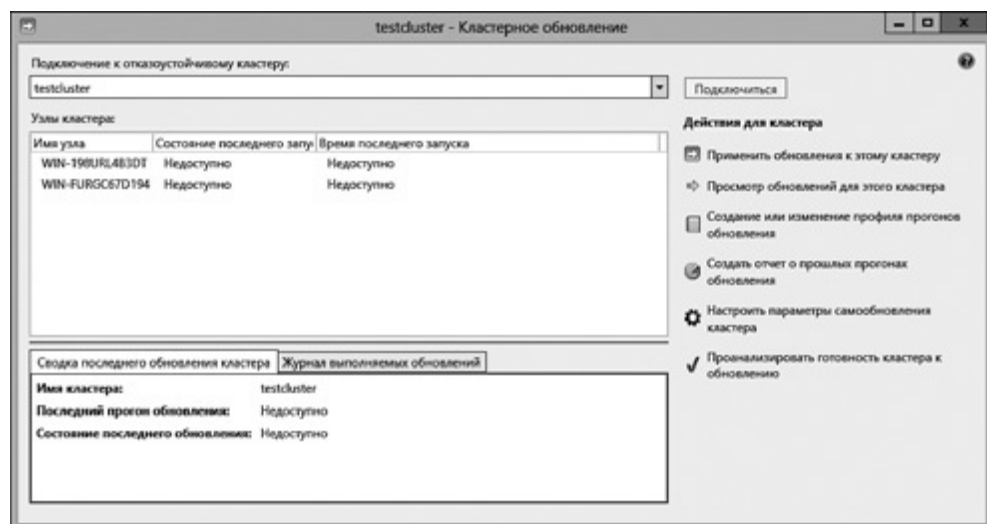


Рис. 6.13. Настройка параметров обновления кластера

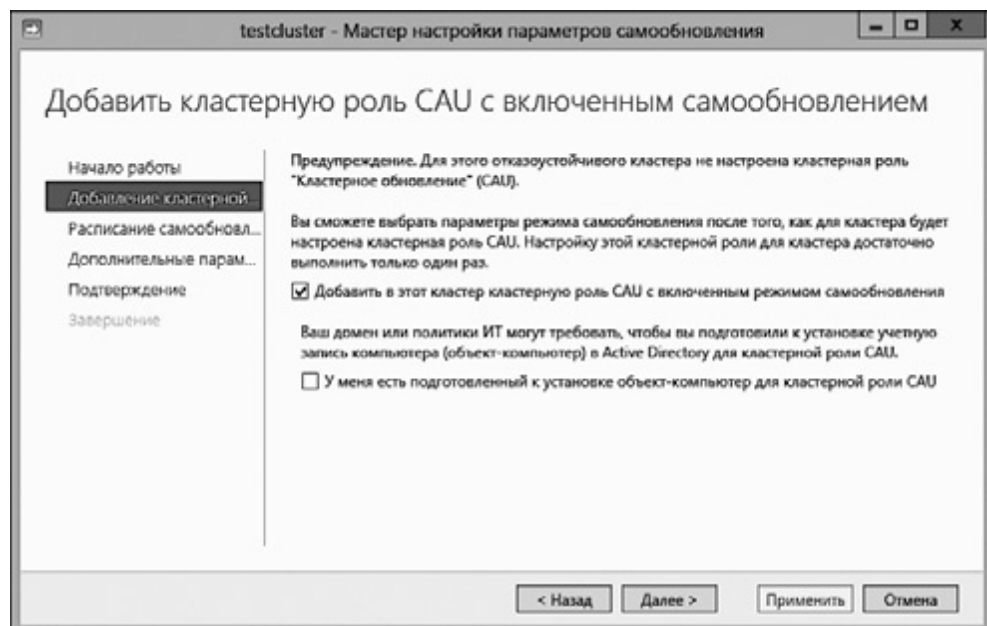


Рис. 6.14. Добавление роли Кластерное обновление

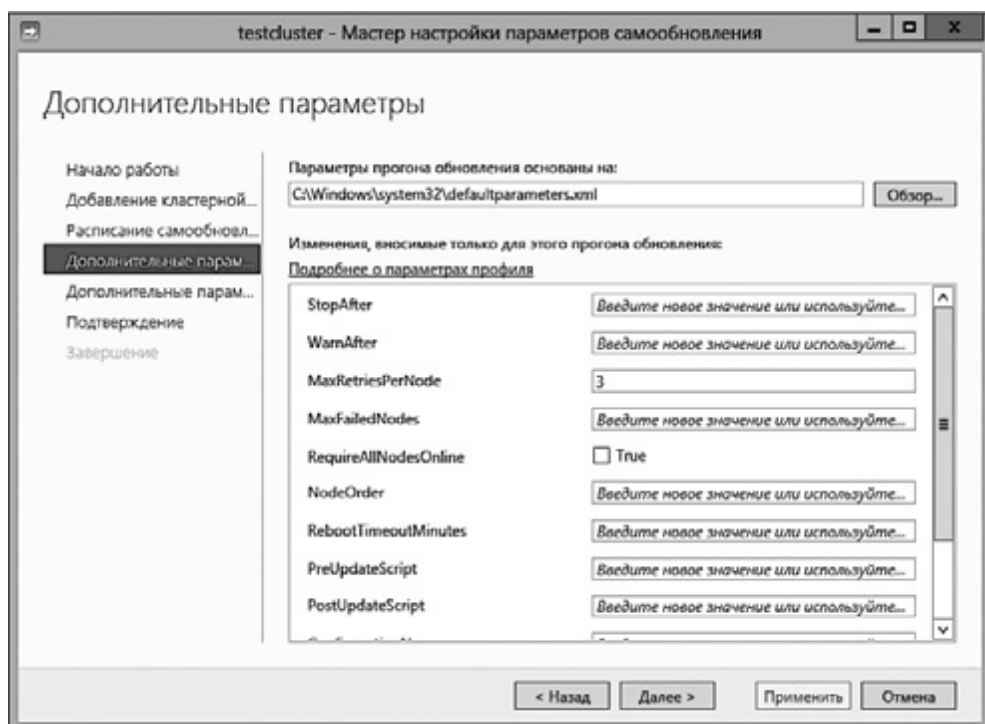


Рис. 6.15. Дополнительные параметры кластерного обновления

Нажмите **Далее** (Next), и вы сможете настроить дополнительные параметры CAU, такие как запуск сценариев до или после обновления (рис. 6.15).

Снова нажмите кнопку **Далее** (Next). В данный момент процесса настройки параметров вы можете настроить CAU на получение рекомендованных обновлений Windows таким же образом, как настраивали критические обновления. Нажмите кнопку **Далее** (Next) еще раз, а затем кнопку **Применить** (Apply).

Выводы

Пространства данных (Storage Spaces) и ReFS (Resilient File System, отказоустойчивая файловая система) — это два нововведения Server 2012, предназначенных для хранения данных, которые помогают обеспечивать целостность данных и отказоустойчивость системы. Хотя ReFS более надежна, чем

NTFS, пространства данных, по существу, представляют собой программную реализацию RAID. Если сравнить их с аппаратными реализациями RAID, то можно говорить о том, что они подвержены тем же уязвимостям, что и программные RAID-решения сторонних производителей. Вопрос о применении пространств данных следует решать с учетом уровня отказоустойчивости, который требуется каждой конкретной организации.

Кроме того, помните, что технологии обеспечения отказоустойчивости — вне зависимости от того, используете вы зеркалирование или контроль четности, — не способны заменить резервное копирование. Даже если вы развернули пространства данных, нужна продуманная стратегия резервного копирования для обеспечения максимального уровня защиты данных.

Кластеризация — это наилучший способ достижения высокого уровня доступности систем при повреждениях дисков или каких-то других сбоях. Server 2012 предлагает простую процедуру настройки отказоустойчивых кластеров, избавляя администратора от сложных манипуляций, которые обычно связывают с такими конфигурациями. Общие тома кластера (Cluster Shared Volumes, CSV) позволяют осуществлять интеграцию с SAN и Hyper-V. Благодаря этому можно добиться еще более высокого уровня отказоустойчивости и рациональнее использовать дисковое пространство. И наконец, обновление отказоустойчивых кластеров с поддержкой доступности (Cluster-Aware Updating, CAU) позволяет поддерживать программное обеспечение кластеров в актуальном состоянии. Благодаря данной технологии установка критических и рекомендуемых обновлений производится без прерывания работы кластеров.

7

Hyper-V

Если бы мне пришлось выбирать какую-то одну интересную возможность Server 2012, которая не только являлась бы стимулом обновления до Server 2012 для организаций, уже использующих платформу Windows, но и привлекла бы новых клиентов, это была бы технология Hyper-V.

Одновременно с Server 2012 представлена последняя версия этой технологии — Hyper-V R3. Hyper-V R3 встроена в Server 2012, а кроме того, доступна в виде самостоятельного бесплатного продукта.

Hyper-V — это решение для виртуализации от Microsoft. Со времен выхода Server 2008 R2 эта технология обрела множество новых возможностей и улучшений. Теперь Hyper-V настолько хороша, что она подходит для построения сложных виртуальных инфраструктур и становится смертельно опасным конкурентом для решений от VMware, занимающих сейчас основную долю рынка.

Для начала хочу сказать пару слов о текущем состоянии дел в сфере виртуализации. На рынке решений для виртуализации выступают три основных игрока: Citrix, VMware и Microsoft. У всех них есть предложения, ориентированные как на SMB-сектор (Small to medium-size business, малый и средний бизнес), так и на крупные корпорации. Рыночное преимущество в настоящий момент принадлежит VMware. Однако Microsoft упорно продвигается

вперед. Аналитики сообщают о том, что Hyper-V — это вторая в мире по распространенности платформа виртуализации.

Эти успехи Microsoft достигнуты отчасти благодаря жестокой, почти маниакальной конкурентной борьбе с VMware. VMware реагировала на это соответствующим образом. Маркетинговые подразделения обеих компаний были заняты подготовкой таблиц и диаграмм, в которых старательно сравнивали характеристики решений от VMware и Microsoft, сопоставляли их масштабируемость, совокупную стоимость эксплуатации и многое другое. Ни VMware, ни Microsoft не упускали случая обнаружить изъян в портфеле виртуализации конкурента.

На фоне ожесточенной борьбы двух корпораций общее мнение сходилась к тому, что Hyper-V не обладает некоторыми расширенными возможностями ПО VMware, в частности теми, которые характерны для корпоративных версий продуктов (таких как vSphere). Сразу после выпуска Hyper-V стал реальным конкурентом VMware, претендентом на значительную долю рынка в области виртуализации, особенно в сегменте SMB.

Почему? В Hyper-V Microsoft представила несколько новых возможностей, которые ставят его на один уровень с VMware. Важнейшей из них является возможность по-настоящему динамической миграции. В Server 2008 R2 миграция виртуальных машин (VM, virtual machine) с одного несущего компьютера на другой была возможна только для кластеризованных виртуальных машин или посредством общего хранилища данных. Hyper-V R3 поддерживает динамическую миграцию виртуальных машин и в кластерах, и между отдельными несущими компьютерами. Кроме того, R3 поддерживает одновременную динамическую миграцию нескольких виртуальных машин. Миграции могут быть выполнены без простоев. Такая гибкость означает более быструю миграцию, которая не приводит к перерывам в работе. Это позволяет преодолеть некоторые существующие в настоящий момент в VMware ограничения на миграцию.

Теперь Hyper-V позволяет создавать и развертывать частные и общедоступные облачные службы, способные обеспечивать изоляцию и мультиарендность. Крупные организации, которым нужно создавать изолированные виртуальные облака для различных сегментов бизнеса, в составе Hyper-V получают необходимые для этого инструменты. Кроме того, если ваша организация предлагает управляемые службы, новые сетевые возможности Hyper-V обеспечивают удобную изоляцию облачных служб клиентов. Это улучшает управляемость и позволяет соблюдать соглашения об уровне обслуживания (SLA, service-level agreements).

Если говорить о масштабируемости, то здесь Hyper-V не только догнал, но и опередил vSphere — сравнимый корпоративный продукт от VMware. Hyper-V поддерживает до 64 узлов и до 4000 виртуальных машин в кластере, а vSphere — 32 узла и 3000 виртуальных машин.

Вы можете настроить систему на использование до 320 логических процессоров на аппаратном обеспечении, на котором в составе Server 2012 работает Hyper-V. Также можно использовать до 4 Тбайт физической оперативной памяти. Одна виртуальная машина поддерживает до 64 виртуальных процессоров и до 1 Тбайт памяти.

Энтузиастам виртуализации понравится и целый ряд прочих новых функций. Среди них зашифрованные кластеры, динамическое слияние моментальных снимков, мониторинг ресурсов.

Есть и еще одна причина, по которой Hyper-V вполне может одержать верх над VMware в корпоративной среде. Она заключается в том, что многим знакомы технологии от Microsoft. Хотя сейчас VMware принадлежит большая часть рынка виртуализации, экосистемы Microsoft развернуты во многих организациях. Системные администраторы, которые уже работали с системами от Microsoft, могут быстрее освоить Hyper-V, нежели VMware. Это означает меньшую стоимость обучения, относящегося к развертыванию Hyper-V, кроме того, эта технология уже встроена в Server 2012.

Конечно, найдутся пользователи, которым больше по душе VMware. Возможно даже, что вы, когда это читаете, качаете головой и говорите: «Без вариантов. VMware — это признанный стандарт виртуализации». Не спорю, VMware создает отличные продукты для виртуализации, и одно из основных преимуществ работы с ПО от VMware заключается в том, что компания живет и дышит исключительно технологиями виртуализации.

В итоге я признаю, что там, где инфраструктуры VMware уже развернуты, переход на Hyper-V непрост и, скорее всего, не особенно привлекателен с точки зрения стоимости и трудозатрат. Однако для многих организаций, которые лишь рассматривают возможность перехода к работе с виртуализированными и облачными платформами и в инфраструктурах которых уже используются продукты от Microsoft, Hyper-V выглядит весьма привлекательно как возможность перехода к использованию таких платформ. Рыночные тенденции отчетливо указывают на рост использования частных и общедоступных облачных сред и на переход от физическим к виртуальным инфраструктурам. Для многих организаций Hyper-V вполне может быть частью этого перехода.

Хотя в Hyper-V появилось множество новшеств и улучшений, следующие разделы ознакомят вас и с базовыми принципами этой технологии,

и с основными новыми возможностями, которые, весьма вероятно, будут интересны большинству организаций вне зависимости от их размера и сферы деятельности. Для начала взглянем на системные требования, необходимые для развертывания Hyper-V.

Системные требования

Hyper-V включен в две из четырех редакций Server 2012: Datacenter и Standard. И как уже сказано, для загрузки доступна бесплатная автономная версия Hyper-V.

Хост-компьютер, на котором запущен Hyper-V (то есть тот, на который установлена роль Hyper-V или автономная версия Hyper-V), должен обладать x64-процессором, поддерживающим аппаратную виртуализацию (технологии Intel VT или AMD-V). Кроме того, процессор должен поддерживать функцию предотвращения выполнения данных (DEP, data execution prevention). Возможно, вам придется включить эту функцию в BIOS сервера.

Microsoft заявляет, что хост-компьютеру требуется не менее 2 Гбайт оперативной памяти. Но виртуальные машины тоже используют физическую оперативную память. Поэтому, чем больше виртуальных машин вы планируете развернуть, тем больше оперативной памяти понадобится для достижения оптимальной производительности системы. Поэтому забудем о минимальных требованиях и сосредоточимся на требованиях реального мира.

Недостаток памяти может значительно снизить производительность Hyper-V. Память играет здесь важнейшую роль, поэтому, прежде чем развертывать Hyper-V, вы должны четко понять, какое количество оперативной памяти требуется хост-компьютеру и как вы будете выделять память для виртуальных машин.



Есть практическое правило для вычисления количества памяти, которое выделяется при использовании Hyper-V. Общая память физического сервера должна быть как минимум равна сумме объемов памяти, выделяемых каждой виртуальной машине. Кроме того, Hyper-V для оптимальной производительности требуется 300 Мбайт на нужды гипервизора, по 32 Мбайт для первого гигабайта оперативной памяти, выделяемого каждой виртуальной машине, и по 8 Мбайт для каждого последующего гигабайта. Кроме того, требуется 512 Мбайт для собственной операционной системы сервера.

Теперь в Windows Server 2012 виртуальные машины поддерживают архитектуру NUMA (non-uniform memory architecture, архитектура памяти с неоднородным доступом). Изначально эта технология была предназначена для многопроцессорных систем, таких как компьютеры, которые используются в научных вычислительных средах. Она позволяла повысить производительность. С помощью NUMA процессор может обращаться к памяти, с которой у него есть прямая связь, быстрее, нежели к памяти, подключенной к другому процессору системы. Hyper-V R3 использует существующую в системе NUMA-топологию (как правило, в серверах уровня организации) для увеличения производительности и масштабируемости системы без вмешательства пользователя.

Есть и некоторые другие рекомендации, которые стоит учесть перед внедрением Hyper-V. Для максимизации производительности используйте на хосте Hyper-V несколько сетевых адаптеров. Когда их в системе несколько, один физический адаптер выделяется для целей управления Hyper-V, другой могут использовать виртуальные машины. Кроме того, системные администраторы часто используют выделенные сетевые адаптеры для iSCSI-хранилищ и объединения систем в кластеры.

Не рекомендуется размещать виртуальные машины в системном разделе диска. Следует либо создать другой раздел для хранения их данных, либо поместить их на отдельный жесткий диск.

Установка роли Hyper-V

Развертывание Hyper-V в Server 2012 требует добавления роли Hyper-V. Как и в случае с другими ролями и компонентами, сделать это можно с помощью диспетчера серверов. Как и в большинстве инструкций, приведенных в этой книге, здесь мы рассмотрим выполнение этой задачи с использованием средств, обладающих графическим пользовательским интерфейсом. Помните, однако, что то же самое можно сделать и с помощью PowerShell.

Итак, в панели мониторинга диспетчера серверов сделайте следующее.

1. Нажмите ссылку **Добавить роли и компоненты** (Add roles and features), затем щелкните на кнопке **Далее** (Next) и выберите вариант **Установка ролей и компонентов** (Role-based or feature-based installation). Щелкайте на кнопке **Далее** (Next) до тех пор, пока не доберетесь до окна **Выбор ролей сервера** (Select server roles).

2. Найдите в списке роль Hyper-V. Кроме того, по умолчанию устанавливаются модуль Hyper-V для Windows PowerShell (Hyper-V Module for Windows PowerShell) и средства управления Hyper-V с графическим интерфейсом (Hyper-V GUI Management tools). В окне, где перечислены компоненты, необходимые для Hyper-V, оставьте их выбранными и нажмите кнопку **Добавить компоненты** (Add Features).
3. Нажмите **ОК** для того, чтобы выбрать конечный компьютер, после чего станет доступной кнопка **Далее** (Next). Нажимайте ее до тех пор, пока не доберетесь до окна **Создание виртуальных коммутаторов** (Create Virtual Switches). Именно здесь нужно выбрать сетевой адаптер, установленный на физическом компьютере-хосте, который будет использован для создания виртуального коммутатора. Виртуальный коммутатор позволяет виртуальным машинам подключаться к сети. По умолчанию будут перечислены все сетевые адаптеры, установленные в Server 2012. Выберите сетевой адаптер, который хотите использовать (рис. 7.1). Завершите этот шаг щелчком на кнопке **Далее** (Next).

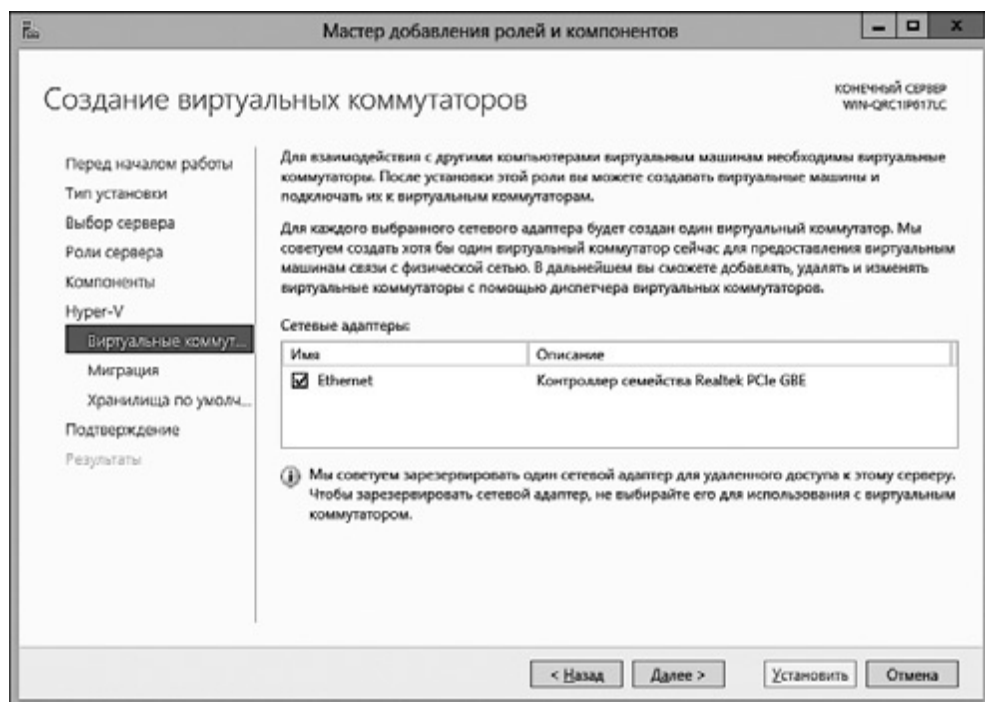


Рис. 7.1. Выбор сетевого адаптера

- Теперь вы видите окно Миграция виртуальной машины (Virtual Machine Migration) (рис. 7.2). Здесь можете включить на сервере функцию динамической миграции. Если вы планируете осуществлять эту операцию на сервере в сети, для которой устанавливаете Hyper-V, установите флажок Разрешить этому серверу отправку и получение миграций виртуальных машин (Allow this server to send and receive live migrations of virtual machines). Не устанавливайте этот флажок, если, например, вы планируете настроить кластеризацию или частную сеть между узлами кластера, развернутую внутри кластера. Вместо этого можете выбрать нужную сеть после установки Hyper-V в сетевых параметрах.

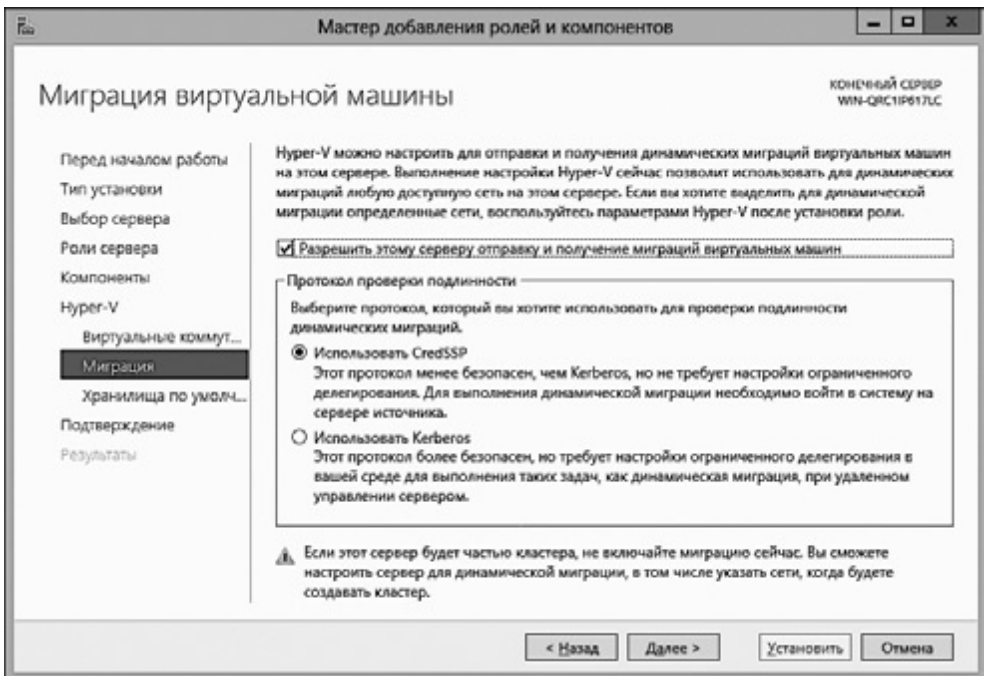


Рис. 7.2. Настройка протокола проверки подлинности динамических миграций

- Если вы выполняете сравнительно простое развертывание Hyper-V без кластеризации, можете включить параметр, который позволяет серверу осуществлять динамическую миграцию. Кроме того, вы должны выбрать протокол, который используется для проверки подлинности динамических миграций, — CredSSP (credential security support provider) или Kerberos (см. рис. 7.2).



CredSSP и Kerberos — это SSPI-протоколы (security support provider interfaces), используемые для проверки подлинности в Windows-окружении. Большинство Windows-инфраструктур, основанных на Active Directory, используют Kerberos. CredSSP используется в окружениях, в которых невозможно использовать Kerberos. Например, CredSSP применяется, когда системные администраторы удаленно исполняют команды PowerShell, имеющие отношение к кластеризации. При таком сценарии в среде, где развернут Kerberos, могут возникать различные проблемы.

6. Теперь мастер добавления роли Hyper-V (Hyper-V Role Wizard) позволит вам выбрать расположение по умолчанию для виртуального жесткого диска и конфигурационных файлов виртуальной машины. Вы можете изменить пути к ним и после установки. Нажмите **Далее (Next)**. В следующем окне вы сможете задать автоматический перезапуск сервера, если это понадобится (в случае с ролью Hyper-V это действительно понадобится). Нажмите кнопку **Установить (Install)**.

Когда сервер перезагрузится, автоматически будут выполнены еще некоторые задачи, связанные с установкой.

Создание и настройка виртуальных машин

Хотя у любого, кто уже создавал виртуальные диски в Hyper-V из Server 2008 R2, не должно возникнуть сложностей при создании виртуальных машин и виртуальных дисков в Hyper-V R3, теперь в ходе этих процедур доступны некоторые новые возможности. Одна из наиболее значительных — новый формат файлов виртуальных дисков.

Настройка виртуальных дисков

Hyper-V R3 использует новый формат файлов для виртуальных жестких дисков **.VHDX**. В Server 2008 R2 это был формат **.VHD**. VHDX поддерживает виртуальные дисковые хранилища объемом до 64 Тбайт (VHD — до 2 Тбайт). Виртуальные диски — это хранилища данных для виртуальных машин, и замечательно то, что они динамически расширяемы. Динамическое расширение происходит при добавлении данных в виртуальную машину.



Традиционно жесткие диски использовали сектора размером 512 Кбайт. От современных носителей информации требуется огромная емкость, и для того чтобы они соответствовали последним тенденциям технологий хранения данных, производители разработали диски, которые используют сектора размером 4 Кбайт. Теперь это стандарт в данной области.

Конечно, для виртуальных машин вы можете использовать и физические диски, те, которые установлены в хост-компьютере. Здесь можно использовать и логические устройства, которым назначен номер (LUN, Logical Unit Number) в SAN-решениях (Storage Attached Network, сеть хранения данных). В данном примере мы создаем виртуальный диск, который поддерживает динамическое расширение. В диспетчере серверов выполните команду Средства ► Диспетчер Hyper-V (Tools ► Hyper-V Manager). В правой части появившегося окна в меню Действия (Actions) выполните команду Создать ► Жесткий диск (New ► Hard Disk). Будет запущен мастер создания виртуального жесткого диска (New Virtual Hard Disk wizard). Сначала нужно выбрать формат диска (рис. 7.3).

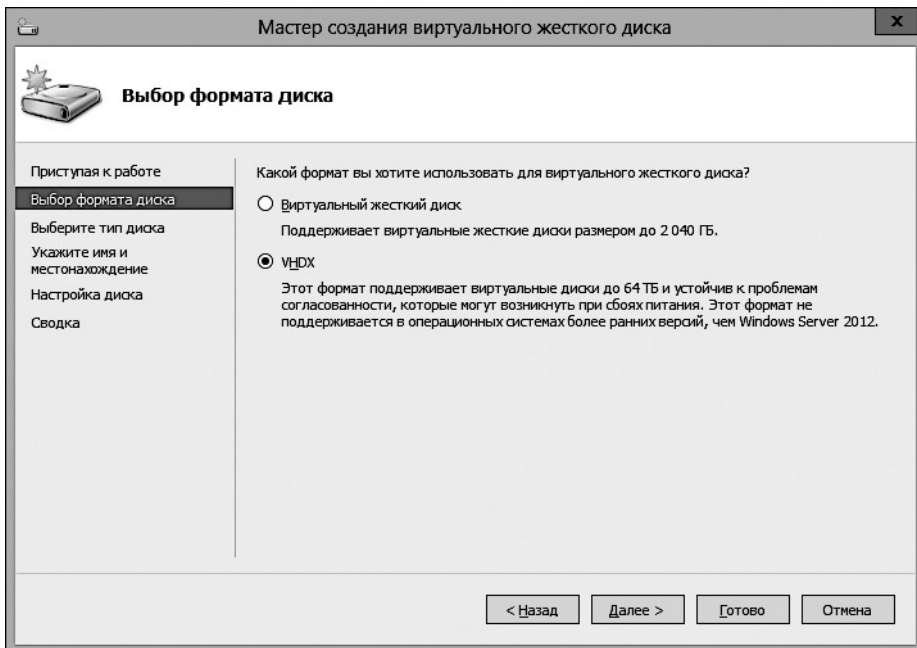


Рис. 7.3. Выбор формата виртуального диска

Это может быть либо VHD, либо VHDX. Хотя VHDX позволяет работать с дисками большей емкости и обеспечивает лучшую защиту данных, этот формат поддерживается лишь Windows Server 2012. Если ваша виртуальная среда подразумевает использование предыдущих версий Windows Server, придется использовать VHD.

На следующем шаге нужно выбрать тип диска. Можно создавать диски трех типов:

- *диск фиксированного размера (Fixed)*. Обладает наилучшей производительностью. Если вы планируете использовать жесткий диск с приложениями, которые интенсивно используют дисковые операции, например базы данных с большим количеством транзакций, — это лучший выбор. Планирование размера такого диска весьма важно, так как он всегда имеет тот размер, который указан при его создании, независимо от объема хранящихся на нем данных;
- *динамически расширяемый диск (Dynamically expanding)*. Такой виртуальный жесткий диск автоматически расширяется, если на нем нужно сохранить дополнительные данные. Если диск используется для приложений, которым не нужна интенсивная работа с дисковой подсистемой и которые не занимают большого дискового пространства, то для большинства инфраструктур диск такого типа окажется наиболее очевидным выбором;
- *разностный диск (Differencing)*. Связан с другим диском, который играет роль родительского диска. Изменения, внесенные в данные дочернего (разностного) диска, не влияют на родительский диск. Разностные диски обычно используются при тестировании или разработке программного обеспечения, когда изменения могут быть записаны на диск в тестовом режиме, а затем тестер может развернуть точно такой же образ диска без изменений для повторного тестирования. Разностные диски, вероятно всего, наименее распространены в производственной среде.

На данном шаге выберите вариант Динамически расширяемый (Dynamically expanding) и щелкните на кнопке Далее (Next). В окне Укажите имя и местонахождение (Specify Name and Location) дайте виртуальному диску имя и укажите местонахождение его файла.

В окне Настройка диска (Configure Disk) вы можете создать чистый виртуальный диск и задать его размер. Также можно скопировать содержимое

физического диска, подключенного к хост-компьютеру, либо другого виртуального диска. Это позволяет сэкономить немало времени, если у вас есть образы дисков, которые вы хотите развернуть на новом виртуальном диске. Нажмите **Далее (Next)**, и настройка диска завершится.

Создание виртуальных машин

Далее подробно описан процесс создания новой виртуальной машины.

1. Выполните команду **Создать ► Виртуальная машина (Create ► Virtual Machine)**. Сначала нужно дать ей имя, и если вы хотите хранить виртуальную машину в месте, которое отличается от предложенного по умолчанию при установке Hyper-V, вам нужно указать ее расположение (рис. 7.4).

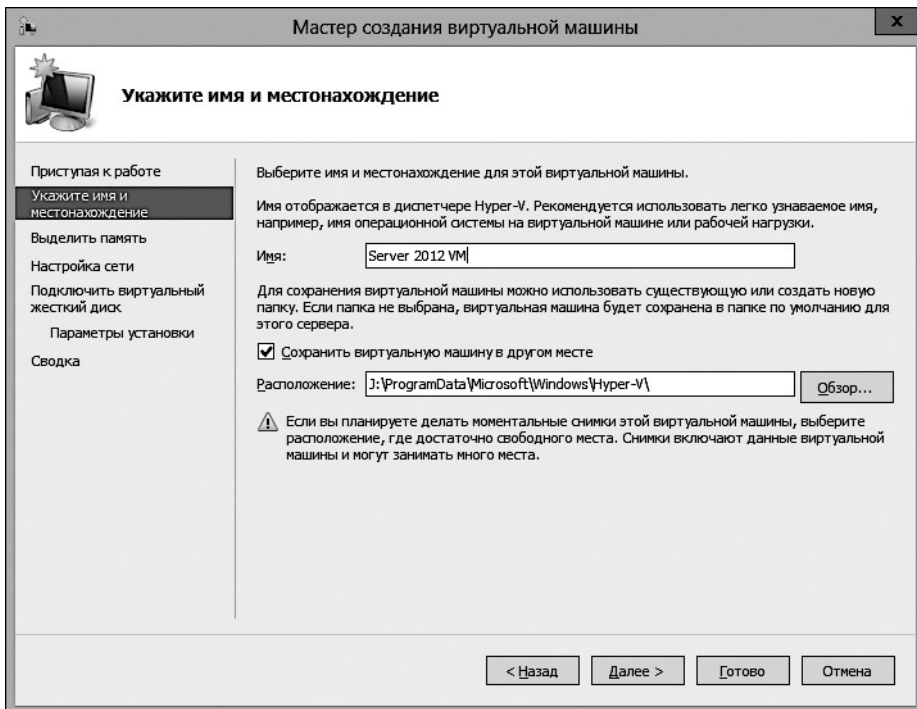


Рис. 7.4. Указание имени и расположения виртуальной машины

Следующий шаг заключается в указании объема памяти, доступного виртуальной машине. Доступен вариант использования динамической памяти.



Конфигурация оперативной памяти сильно влияет на производительность Hyper-V. В случае использования динамической памяти виртуальным машинам, которым требуется больше памяти, выделяются ресурсы памяти виртуальных машин, требования которых к объему оперативной памяти ниже. Например, тех, которые находятся в состоянии простоя. Интеллектуальная работа со страницами памяти — это функция динамической памяти, которая очень напоминает работу с файлом подкачки на жестком диске. Когда системе не хватает памяти, ресурсы отдаются активному приложению. Вы можете включить использование динамической памяти для виртуальной машины. Однако вполне можете не получить прироста производительности, если только не используете одновременно несколько виртуальных машин.

2. Затем мастер создания виртуальной машины (New Virtual Machine wizard) покажет экран **Настройка сети (Configure Networking)**. Здесь вы можете указать сетевой адаптер, который будет использовать виртуальная машина. После того как вы это сделаете, мастер предложит подключить виртуальный диск. На данном шаге можно либо создать новый виртуальный диск, либо подключить существующий, либо подключить виртуальный диск позже.
3. На экране **Параметры установки (Installation Options)** вы можете выбрать варианты установки операционной системы. Можно использовать загрузочный диск или образ, можно выполнить сетевую установку или указать параметр, который позволит установить ОС позднее. На рис. 7.5 я устанавливаю в качестве гостевой ОС для виртуальной машины Windows Server 2012 с *.iso*-образа.
4. Щелкните на кнопке **Далее (Next)**, а затем **Готово (Finish)** для завершения настройки виртуальной машины. Запись о новой виртуальной машине появится в диспетчере Hyper-V (Hyper-V Manager) в состоянии **Выключена (Off)**. Щелкните правой кнопкой мыши на виртуальной машине и выберите команду **Пуск (Start)**, а затем **Подключить (Connect)** для выполнения установки гостевой ОС.

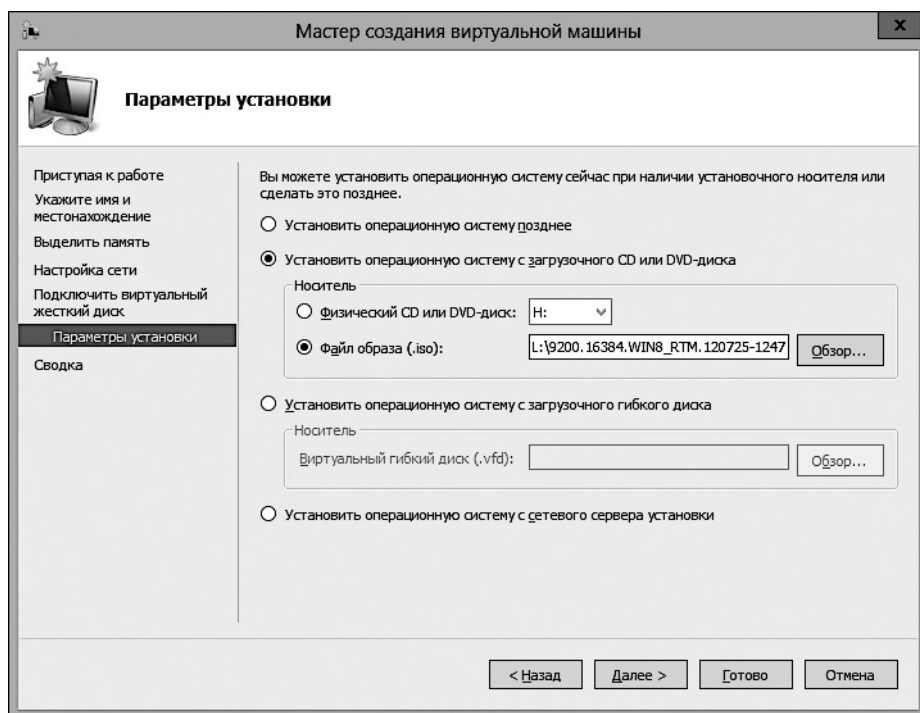


Рис. 7.5. Выбор варианта установки ОС на виртуальную машину

Управление виртуальными машинами и виртуальными дисками

В следующих разделах вы найдете пошаговые примеры, демонстрирующие некоторые из важнейших возможностей Hyper-V R3.

Динамическая миграция виртуальных машин

Возможность динамической миграции виртуальных машин — это большой шаг вперед, сделанный в Hyper-V R3. Динамическая миграция — это перемещение виртуальных машин с одного физического хост-компьютера на другой без простоя виртуальных машин. Улучшение заключается в возможности миграции виртуальных машин без общего хранилища данных и без

необходимости нахождения обоих хостов в кластере — все это требовалось для обеспечения динамической миграции в Server 2008 R2.

Упрощение динамической миграции необходимо для виртуализированных окружений. Возможность быстро перемещать виртуальные машины с одного физического компьютера на другой весьма важна для быстрого восстановления работоспособности системы даже при возникновении форс-мажорных обстоятельств. Если один хост-компьютер не способен выполнять свои функции, вы можете переместить виртуальную машину на другой.

Для того чтобы выполнить динамическую миграцию, вам понадобятся два или большее количество серверов с установленной Hyper-V. На серверах должны быть установленные процессоры одного производителя, поддерживающие виртуализацию (все либо от AMD, либо от Intel, если это не так, виртуальная машина перед миграцией должна быть остановлена). Серверы должны принадлежать одному и тому же домену или доменам, между которыми установлены доверительные отношения. Кроме того, виртуальные машины должны быть настроены на использование виртуального хранилища данных или виртуальных дисков Fibre Channel.

Для того чтобы выполнить динамическую миграцию виртуальных машин, вы должны войти в систему с учетной записью администратора домена или учетной записью, имеющей соответствующие разрешения. Динамическую миграцию можно выполнить локально, пользуясь удаленным Рабочим столом (Remote Desktop), посредством удаленной PowerShell-сессии или с использованием инструментов удаленного администрирования, установленных на Windows 8-клиенте.

Далее приведена последовательность действий при миграции виртуальной машины с установленной ОС Server 2012 с одного физического сервера на другой. И на том и на другом также установлена ОС Server 2012. Оба хост-компьютера расположены в одной и той же подсети физической сети, миграция выполняется локально.

1. Для начала миграции виртуальной машины щелкните на ней в диспетчере Hyper-V (Hyper-V Manager) правой кнопкой мыши, в появившемся меню выберите команду Переместить (Move), щелкните на кнопке Далее (Next). В окне Выбор типа перемещения (Choose Move Type) выберите вариант Переместить виртуальную машину (Move the virtual machine), нажмите кнопку Далее (Next).
2. Теперь вы должны указать имя конечного сервера. Можете найти его с помощью средств Active Directory (рис. 7.6).

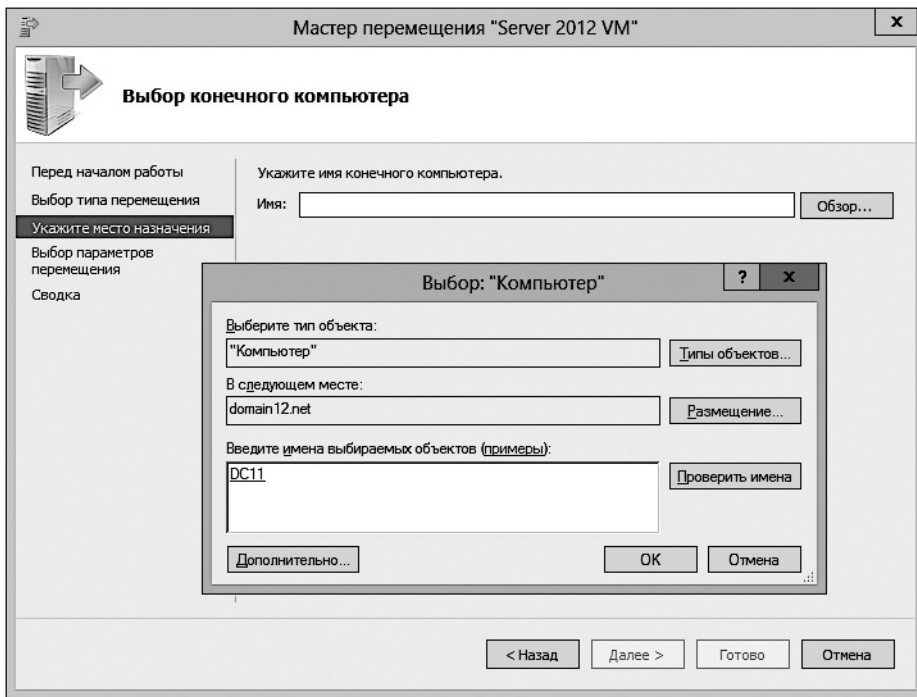


Рис. 7.6. Выбор конечного сервера для выполнения динамической миграции

3. Нажмите кнопку **Далее** (Next), и мастер перемещения (Move wizard) отобразит окно **Выбор параметров перемещения** (Choose Move Options). Здесь будут представлены настройки, которые позволяют переместить всю виртуальную машину вместе со связанными с ней данными (такими, как виртуальный жесткий диск, моментальные снимки, файл подкачки), переместить только виртуальную машину или переместить виртуальную машину и связанные с ней ресурсы в различные расположения. На рис. 7.7 я выбрала вариант **Переместить данные виртуальной машины в одно расположение** (Move the virtual machine's data to a single location) для перемещения всего, что связано с виртуальной машиной, по единому адресу.
4. Теперь нужно выбрать папку файловой системы на конечном сервере, где будет сохранена виртуальная машина (рис. 7.8). Нажмите **Далее** (Next) и затем **Готово** (Finish).

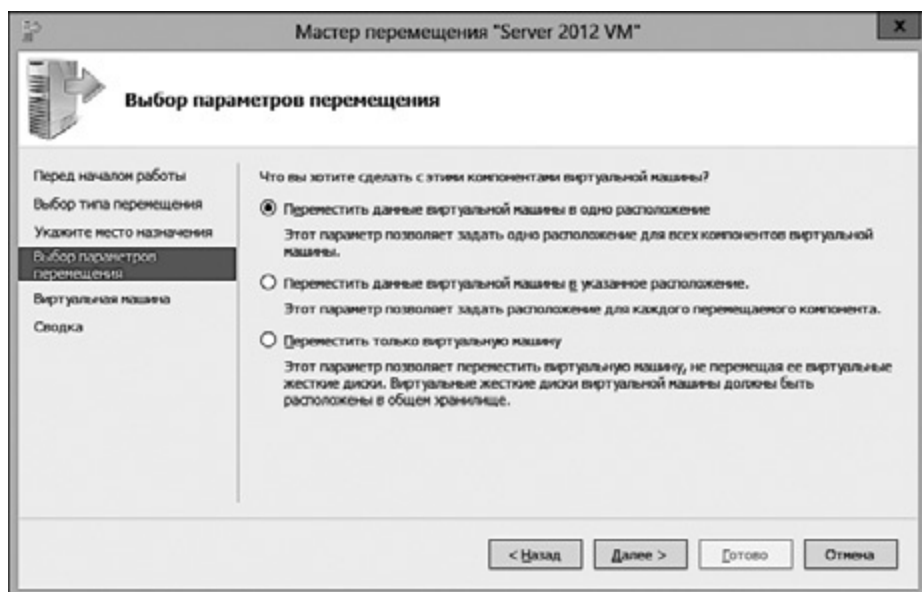


Рис. 7.7. Выбор параметров перемещения

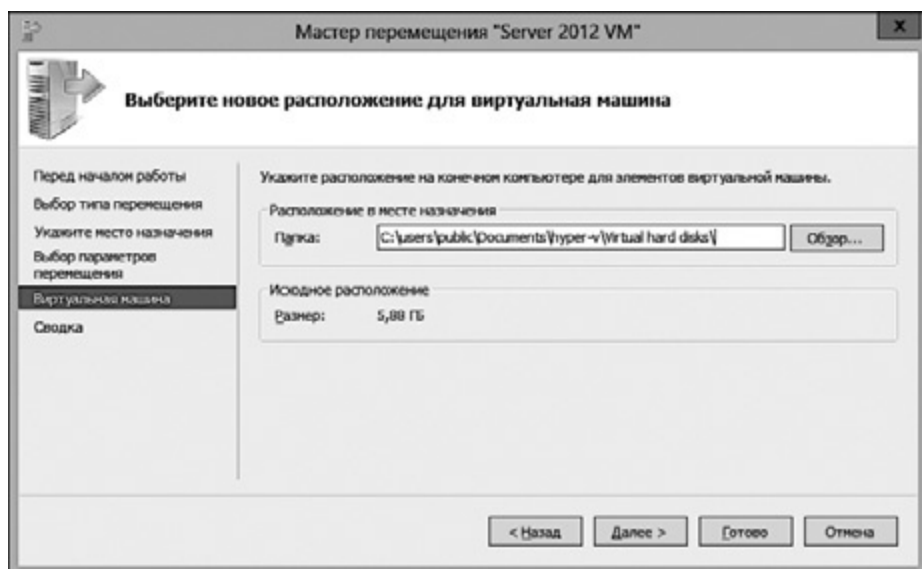


Рис. 7.8. Выбор расположения для перемещаемой виртуальной машины

Кроме того, вы можете перемещать виртуальные хранилища данных (VHD и VHDX-файлы) для одной или нескольких виртуальных машин с одного хост-компьютера на другой, не прерывая работы виртуальных машин. Эта возможность дает вам больший простор для маневра с виртуальным хранилищем данных. Системные администраторы могут использовать динамическую миграцию хранилищ для обновления хранилищ, решения проблем или изменения конфигурации хранилища.

Реплика Hyper-V

Реплика Hyper-V (Hyper-V Replica) — это новая функция Server 2012, которая позволяет выполнять *асинхронную репликацию (asynchronous replication)* виртуальных машин (удобный способ заявить о том, что вы реплицируете виртуальную машину с одного хоста на другой). Данная возможность весьма полезна для случаев, когда с одним из хостов что-то случилось.

Помните о том, что это не миграция, так как вы не перемещаете виртуальную машину с одного Hyper-V-сервера на другой. Вместо этого вы создаете точную копию виртуальной машины и размещаете ее на другом сервере. Как и в случае с динамической миграцией, Hyper-V-серверы не должны иметь общих хранилищ или принадлежать одному кластеру. Они лишь должны быть связаны компьютерной сетью.

1. Создавая реплику виртуальной машины, для начала вы должны включить данную функцию. В диспетчере Hyper-V (Hyper-V Manager) щелкните правой кнопкой мыши на виртуальной машине, которую нужно реплицировать, и выберите команду **Включить репликацию (Enable Replication)**. После этого будет запущен соответствующий мастер.
2. Далее нужно задать сервер реплики. На рис. 7.9 я выбрала сервер, который примет реплицируемую виртуальную машину. Однако здесь я столкнулась с ошибкой, которая указывает на то, что выбранный сервер не настроен для приема реплик.

Hyper-V позволяет выполнить удаленную настройку сервера-реплики с хост-компьютера, на котором находится виртуальная машина для репликации. Когда выводится сообщение об ошибке, появляется кнопка **Настроить сервер (Configure Server)**.

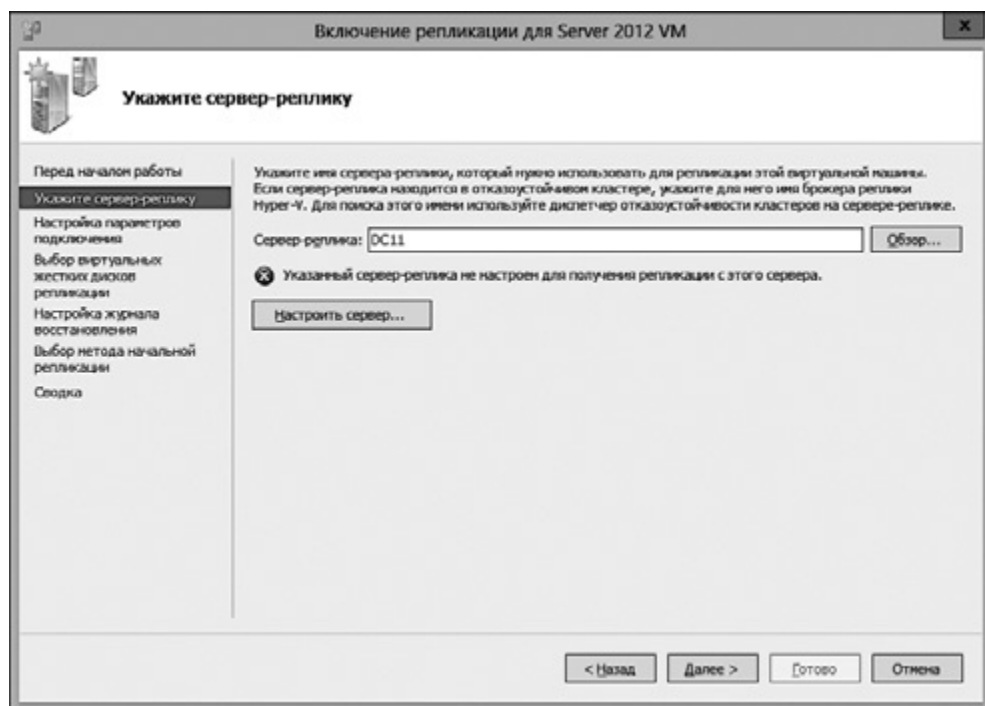


Рис. 7.9. Ошибка репликации

3. В окне настройки параметров Hyper-V для сервера-реплики установите флажок **Включить компьютер как сервер-реплику** (Enable this computer as a Replica server). Далее выберите метод проверки подлинности для трафика репликации. При использовании протокола Kerberos репликация будет производиться без шифрования данных, но вы можете выбрать протокол HTTPS, и данные, которыми обмениваются хосты, будут шифроваться. И наконец, выберите серверы, которым разрешено участвовать в операциях репликации в пределах домена.

Сэкономьте свое время и настройте серверы, которые будут использоваться для репликации, сразу после установки Hyper-V. Это можно сделать в диспетчере Hyper-V (Hyper-V Manager), воспользовавшись ссылкой для вызова окна настройки параметров Hyper-V.

4. Теперь, когда конечный сервер настроен для репликации, нажмите **Далее** (Next). Будет открыто окно **Настройка параметров подключения** (Specify Connection Parameters). Здесь вы можете проверить, какой

протокол используется для трафика репликации (HTTP или HTTPS), а также настроить сжатие данных, передаваемых по сети (оно включено по умолчанию). Нажмите **Далее (Next)**.

Следующий экран (рис. 7.10) позволяет вам указать, какие виртуальные жесткие диски следует реплицировать, а какие — нет.

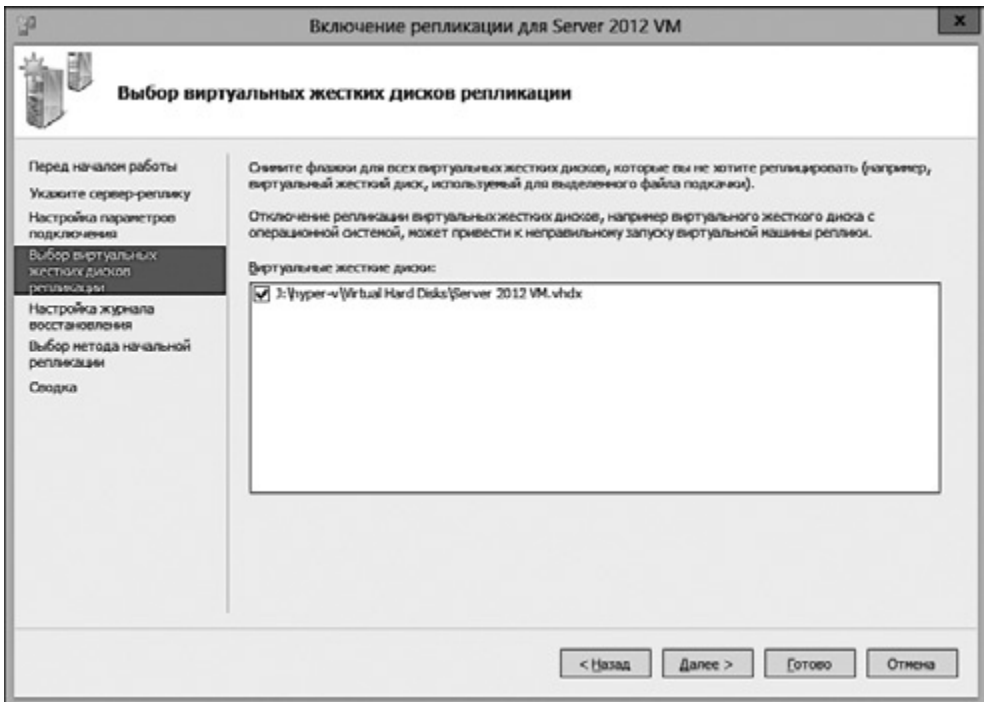


Рис. 7.10. Отмеченные флажками виртуальные диски будут включены в реплику

Затем мастер позволит вам настроить журнал восстановления. Настройка журнала восстановления означает выбор точек восстановления реплицируемой виртуальной машины, которые вы хотите сохранить. По умолчанию включено сохранение лишь последней точки восстановления (это экономит дисковое пространство), однако вы можете указать и большее число точек.

5. Последняя настройка перед выполнением репликации позволяет выбрать метод начальной репликации виртуальной машины. По умолчанию

реплицируемая виртуальная машина пересылается с хоста А на хост Б по сети. Однако в том случае, если пропускная способность сети ограничена, реплицируемая виртуальная машина может быть экспортирована на внешний носитель информации, позже данные можно будет передавать по сети. Третий параметр можно использовать, если вы уже восстановили ту же самую виртуальную машину на сервере-реплике. Эту восстановленную виртуальную машину можно использовать в качестве начальной копии репликации. Данный параметр позволяет уменьшить время, необходимое на репликацию, и объем сетевого трафика. Дело в том, что при таком подходе на сервер назначения по сети передаются лишь изменения, внесенные в реплицированную виртуальную машину после ее восстановления.

Здесь же вы можете указать, что репликацию следует запустить немедленно, либо запланировать проведение репликации и нажать **Готово** (Finish).



Убедитесь в том, что брандмауэр на сервере-реплике настроен на прием входящего трафика репликации. Если это не так, вы столкнетесь с ошибкой **Unable to replicate** (Невозможно провести репликацию). В брандмауэре Windows (Windows Firewall) включите правило **Прослушиватель HTTP-реплики Hyper-V** (входящий трафик TCP) (Hyper-V Replica HTTP Listener (TCP-In)). Сделать это нужно при использовании как системы проверки подлинности Kerberos, так и системы, основанной на сертификатах (HTTPS).

- После успешного завершения настройки и запуска репликации вы увидите в поле **Статус** (Status) сообщение «Отправка исходной реплики» (Sending Initial Replication) (рис. 7.11). После будет выведено сообщение о выполнении слияния (merge). Когда все завершится, виртуальная машина будет видна в диспетчере Hyper-V (Hyper-V Manager) на сервере-реплике.

Клонирование виртуального контроллера домена

Клонирование виртуального контроллера домена возможно и в предыдущих версиях ОС семейства Windows Server. Однако в Server 2012 этот процесс упрощен.



Рис. 7.11. Процесс репликации работающей исходной виртуальной машины

Из клонирования контроллера домена можно извлечь немало пользы. Во-первых, это идеальный способ масштабирования растущей инфраструктуры Windows, так как вы можете быстро развертывать контроллеры домена, не тратясь на дополнительное аппаратное обеспечение. Кроме того, это сохраняет время ИТ-специалистов, поскольку при таком подходе не нужно заниматься настройкой контроллера домена. Также возможность клонирования контроллера домена — это неплохая часть стратегического плана восстановления системы после какой-нибудь крупной неприятности.

Прежде чем клонировать виртуальный контроллер домена, нужно провести некоторую подготовку и проверку. Например, авторизовать контроллер домена для клонирования. Это можно сделать, добавив его в группу Клонлируемые контроллеры домена (Cloneable Domain Controllers) в Active Directory. Группа находится в контейнере Users (Пользователи).

Также нужно убедиться в том, что контроллер домена, обслуживающий роль эмулятора PDC (Primary Domain Controller, основной контроллер домена) FSMO (Flexible Single Master Operations, операции с одним исполнителем), работает под управлением Windows Server 2012. Кроме того, следует проверить, все ли приложения, исполняющиеся на контроллере домена, поддерживают клонирование.

Проверить, поддерживает ли приложение клонирование, довольно легко. Достаточно запустить следующую команду PowerShell:

`Get-ADDCloningExcludedApplicationList`

Этот командлет запускают на контроллере домена, который готовят к клонированию. Команда проверяет список приложений, которые могут быть клонированы в виртуальной среде. Выходные данные команды указывают на приложения, которые не были распознаны как безопасные для целей клонирования. Это может произойти либо из-за условий их лицензирования, либо из-за их функциональных особенностей. Если вы запустили вышеупомянутую команду и приложение, установленное на контроллере домена, попало в список, можете связаться с производителем приложения и спросить: безопасно клонировать контроллер домена, когда на нем установлено данное приложение, или лучше его деинсталлировать и переустановить после клонирования.

Затем нужно запустить еще один командлет. На виртуальном контроллере домена, который вы собираетесь клонировать, выполните команду `New-ADDCCloneConfigFile`. Этот командлет создает конфигурационный файл, который используется в процессе клонирования. Его запускают со следующими параметрами: имя компьютера, который является контроллером домена, IP-адрес, адрес DNS-сервера, шлюз, маска подсети, IP-адрес WINS-сервера и доменное имя.

Например, виртуальный контроллер домена, который мы хотим клонировать, называется `VMDC1`. Виртуальная машина настроена на использование статической IPv4-адресации, доменное имя — `Domain12.net`. Вот синтаксис команды для создания конфигурационного файла:

```
New-ADDCCloneConfigFile -Static -IPv4Address "192.168.1.12"  
IPv4DNSResolver "192.168.1.10" -Ipv4SubnetMask "255.255.255.0"  
-CloneComputerName "VMDC1" -IPv4DefaultGateway "192.168.1.1"  
-PreferredWINSServer "192.168.1.10" -SiteName "DOMAIN12.NET"
```

Затем клонируемая виртуальная машина выключается. Нужно щелкнуть правой кнопкой мыши на ее названии в диспетчере Hyper-V (Hyper-V Manager) и выбрать в появившемся меню команду Экспорт (Export). В диспетчере Hyper-V (Hyper-V Manager) можно будет наблюдать за состоянием экспорта. В папке, куда выполняется сохранение экспортируемой виртуальной машины, создается подпапка. Она имеет то же имя, что и виртуальная машина. В подпапке есть три папки: *Snapshots*, *Virtual Hard Disks* и *Virtual Machines*. Они хранят соответствующие данные, которые экспортируются вместе с виртуальной машиной.

Последний шаг данной процедуры заключается в импорте виртуального контроллера домена. В меню Действия (Action) диспетчера Hyper-V (Hyper-V Manager) щелкните на команде **Импорт виртуальной машины** (Import Virtual Machine). Перейдите в папку, в которой были сохранены экспортированные файлы виртуальной машины. Выберите виртуальную машину для импорта. Нажмите **Далее** (Next) и выберите тип импорта. Здесь (рис. 7.12) есть три возможности:

- *регистрировать виртуальную машину по месту* (*Register the virtual machine in-place*). Это новая возможность импорта, которая появилась в Hyper-V R3. Она позволяет использовать существующий уникальный идентификатор (ID). Если у импортируемой виртуальной машины уже есть связанные с ней файлы данных, если они расположены там, где вам нужно, и если все, что нужно сделать, — это подключить виртуальную машину к Hyper-V, воспользуйтесь этим вариантом;
- *восстановить виртуальную машину* (*Restore the virtual machine*). Если файлы виртуальной машины сохранены в сетевой папке или на внешнем диске, Hyper-V переместит их в более подходящее место и зарегистрирует виртуальную машину;

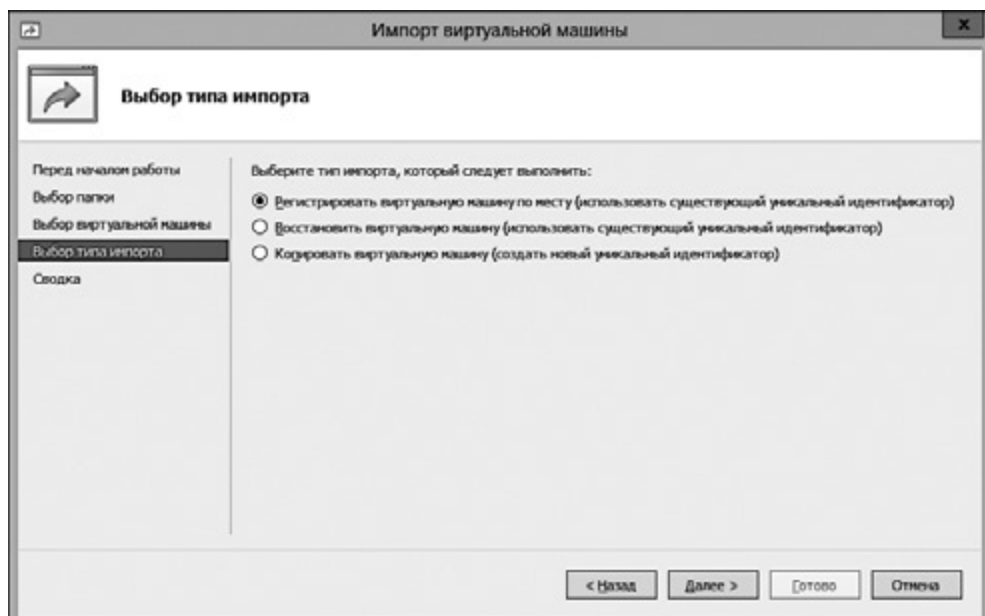


Рис. 7.12. Выбор подходящего типа импорта

- *копировать виртуальную машину (Copy the virtual machine)*. Если вам нужно импортировать виртуальную машину более одного раза, воспользуйтесь этим вариантом импорта, так как каждой виртуальной машине присваивается новый уникальный идентификатор.

Объединение мгновенных снимков

Мгновенные снимки — это файлы с данными, которые используются для восстановления более раннего состояния виртуальной машины. Их обычно используют при тестировании, но они удобны и тогда, когда вы, например, вносите в виртуальную машину какие-то изменения и сталкиваетесь с вызванными этим проблемами. Скажем, если обновление прошло неудачно, вам может понадобиться вернуть виртуальную машину в то состояние, в котором она была до обновления.

Мгновенные снимки, конечно, не новая возможность Windows 2012. А вот новое в их использовании то, что теперь их можно объединять с виртуальной машиной, не прерывая ее функционирования. Это серьезный шаг вперед по сравнению с версией Hyper-V, которая использовалась в Server 2008 R2. В частности, раньше перед объединением виртуальной машины со снимками требовалось выключать ее.

Для того чтобы вернуть работающую виртуальную машину в предыдущее состояние, в меню Действия (Actions) диспетчера Hyper-V (Hyper-V Manager) воспользуйтесь командой Возврат (Revert) для этой виртуальной машины. Откроется окно Вернуть виртуальную машину (Revert Virtual Machine), в котором можно подтвердить выполнение этого действия или отказаться от него. На рис. 7.13 вы видите возврат виртуальной машины в предыдущее состояние, который выполняется на работающей виртуальной машине.

Виртуальные машины						
Имя	Состояние	Загрузка ЦП	Назначенная пам...	Время раб...	Статус	Работоспо
Server 2012 VM	Работает	12%	512 МБ	00:00:00	Восстановление - Успеш...	Обычное

Рис. 7.13. Динамическое объединение с моментальным снимком

Производительность и управление виртуальной сетью

Помимо создания виртуальных машин и управления ими системные администраторы отвечают за мониторинг производительности, состояние виртуальных машин и за наблюдение за обычными компьютерами.

Нурег-V предлагает не только улучшения в области мониторинга виртуальных сред, но и новые возможности, которые стоят того, чтобы с ними ознакомиться.

Измерение ресурсов

Измерение ресурсов — это новая функция, которая позволяет получить сведения об уровне потребления виртуальной машиной ресурсов центрального процессора, оперативной памяти, дисковой подсистемы, сетевых ресурсов. Считайте, что это монитор производительности (Performance Monitor) для виртуализации.

Измерение ресурсов помимо контроля состояния виртуальной инфраструктуры служит еще одной важной цели — биллингу. Так как компании все чаще предоставляют клиентам некие сервисы, пользуясь облачными платформами, им нужно взимать с клиентов плату за использование этих сервисов. С помощью измерения ресурсов организация может создать собственную внутреннюю стратегию выставления клиентам счетов за использование служб на основе измерений потребленных ресурсов. Ранее при подсчете стоимости работы с облачными сервисами большинство компаний полагались на продукты сторонних разработчиков.

При измерении ресурсов можно получить следующие показатели:

- Среднее за заданный период использование центрального процессора, измеренное в мегагерцах.
- Среднее использование физической оперативной памяти, измеренное в мегабайтах.
- Минимальный уровень использования оперативной памяти (наименьшее количество физической памяти).
- Максимальный уровень использования оперативной памяти (наибольшее количество физической памяти).

- Максимальный объем дискового пространства, выделенного виртуальной машине.
- Общий входящий сетевой трафик для виртуального сетевого адаптера, измеренный в мегабайтах.
- Общий исходящий сетевой трафик для виртуального сетевого адаптера, измеренный в мегабайтах.

Для запуска измерения ресурсов выполните в PowerShell следующий командлет (рис. 7.14):

```
Get-VM -ComputerName <name of Hyper-V host machine>|Enable-VMResourceMetering
```

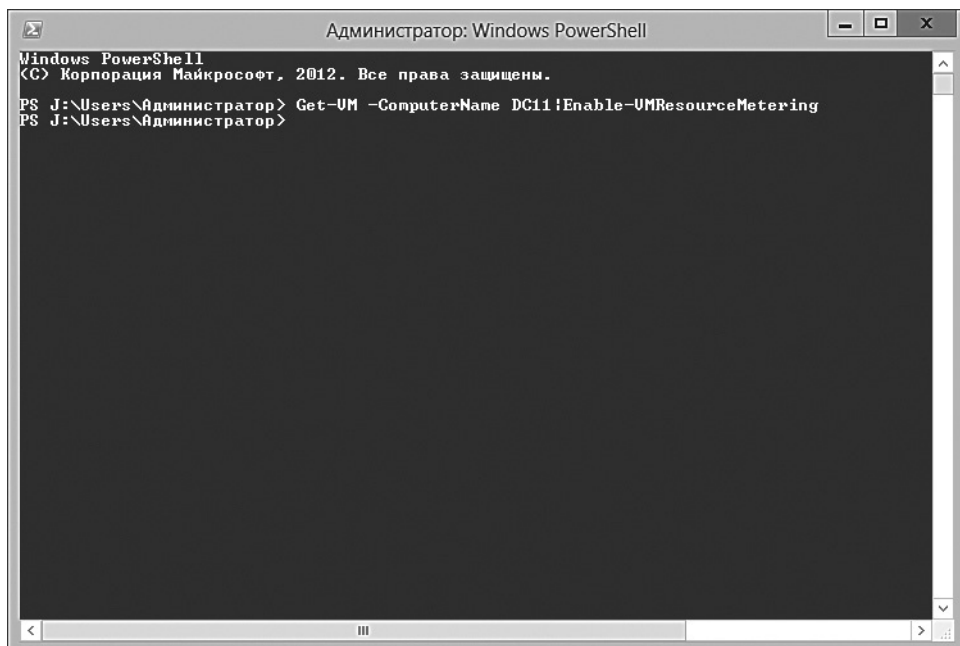


Рис. 7.14. Командлет для запуска измерения ресурсов

По умолчанию период измерения показателей равен один час. Вы можете настроить этот интервал. Следующий командлет устанавливает период сбора данных равным одной минуте:

```
Set-vmhost -computername <Hyper-V host name>  
-ResourceMeteringSaveInterval 00:01:00
```

Для того чтобы вывести данные, собранные для виртуальных машин, выполните следующую команду (рис. 7.15):

```
Get-VM -ComputerName <name of Hyper-V host>|Measure-VM
```

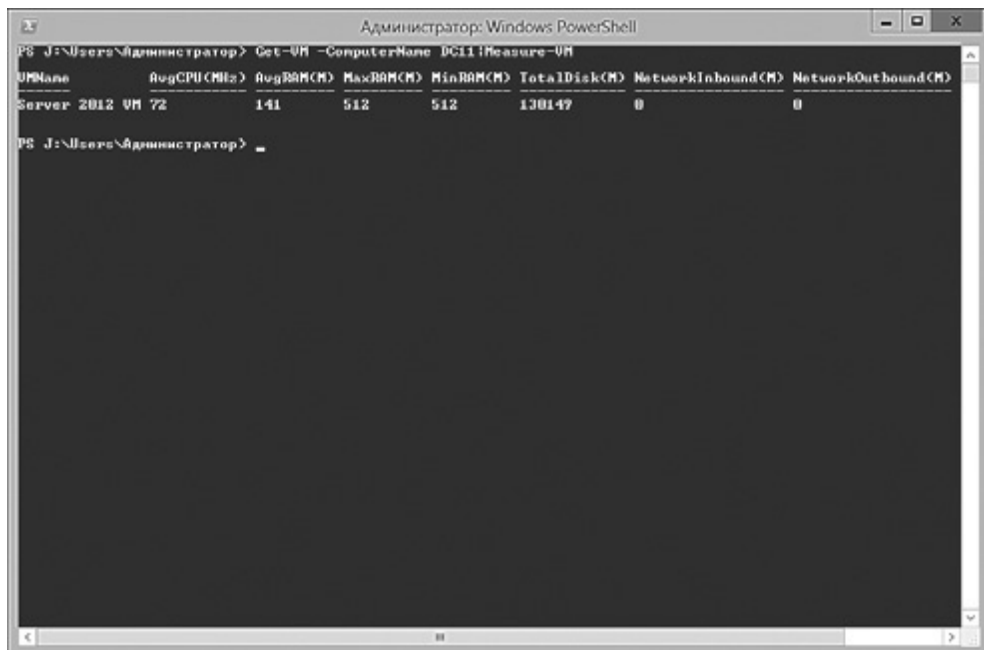


Рис. 7.15. Вывод данных измерения ресурсов

Измерения можно получать и для конкретной виртуальной машины. В следующем примере мы запрашиваем данные для виртуальной машины с именем Server2012VM на Hyper-V-хосте DC10:

```
Get-VM -ComputerName DC10 -Name "Server2012VM"|Measure-VM
```

Поскольку облачные вычисления находятся в центре внимания Server 2012 и Hyper-V R3, у организаций, имеющих платные облачные сервисы, появляется неплохая возможность поближе познакомиться с этими технологиями. Измерение ресурсов — это хороший способ отследить использование ресурсов в виртуализованном окружении, но возможности экспорта данных, которыми можно воспользоваться, запуская описанные команды, довольно слабы. Я предпочла бы компонент с графическим интерфейсом, который умеет отображать форматированные отчеты и обладает возможностями

визуализации данных. В настоящий момент наилучшим решением мне кажется извлечение данных, которые предоставляет система измерения ресурсов, с использованием команды, позволяющей формировать файлы в формате CSV (comma-separated value, значения, разделенные запятой).

Выводы

Новые возможности Hyper-V R3 обеспечивают простое, но надежное управление виртуальным окружением. Динамическая миграция, динамическое объединение моментальных снимков и Hyper-V-репликация — все это способы быстрого развертывания виртуальных машин, которые служат целям масштабируемости, решения проблем или восстановления работоспособности системы после серьезных неприятностей. Новые возможности, такие как измерение ресурсов, делают Server 2012 и Hyper-V привлекательным выбором для организаций — поставщиков услуг, работа которых основана на услугах, сдаваемых в аренду.

Многие пошаговые примеры, которые мы разбирали в этой главе, применимы и к виртуальным машинам, объединенным в кластер. Мы в основном рассматривали методы работы с графическим интерфейсом, но все, о чем здесь говорилось, в том числе динамическую миграцию и Hyper-V-репликацию, можно выполнить и с помощью PowerShell.

Как системный администратор вы просто обязаны разбираться в виртуализации. Эта глава посвящена основным, но, конечно же, не всем новым возможностям Hyper-V. В следующей главе мы рассмотрим новые сетевые возможности Server 2012, которые предназначены не только для физических сетей, но и для сетей, построенных с помощью Hyper-V.

8

Сетевые возможности

Windows Server 2012 предлагает новые возможности в области управления сетями. Они созданы для того, чтобы удовлетворить запросы компаний, которые переходят от традиционных локальных (LAN, local area network) и глобальных (WAN, wide area network) сетей к облачным инфраструктурам.

Перед тем как углубиться в изучение этих новых возможностей, важно уяснить различия между традиционными сетями и облаком. Локальная сеть — это обычно некая группа компьютеров, расположенная за брандмауэром. Эти компьютеры могут обмениваться данными посредством связывающей их проводной или беспроводной сети. На компьютерах, принадлежащих локальной сети, разворачивают серверы и приложения, которыми управляют IT-специалисты организации. Расширение локальной сети с целью ее увеличения, добавления дополнительных хранилищ информации, новых компьютеров или других ресурсов требует усилий IT-специалистов.

В случае с облачными вычислениями компоненты IT-инфраструктуры, такие как серверы, хранилища данных, память, сетевые и вычислительные ресурсы, виртуализованы внутри частной сети организации или в виде служб, которые расположены в сети провайдера услуг. Облачный подход к вычислениям позволяет быстрее разворачивать компоненты инфраструктуры, они обладают высоким уровнем масштабируемости. А так как облачные службы либо не требуют дополнительных вложений в аппаратное обеспечение, либо сводят

такие вложения к минимуму, облачные среды обладают большей экономической эффективностью, нежели традиционные локальные сети. В средах облачных вычислений ресурсы всегда предоставляются по требованию.

К термину «облачные вычисления» («cloud computing») порой относятся с иронией как к разрекламированному маркетинговому лозунгу. И хотя индустрия информационных технологий не испытывает недостатка в надоедливых маркетинговых фразах, «облачные вычисления» — это не одна из таких фраз. Облачные среды построены на базе привычных технологий. Подумайте о технологиях, которые лежат в основе облачных вычислений: высокоскоростной доступ в Интернет, хранилища информации большой емкости, виртуализация аппаратного обеспечения и сетей. Эти технологии уже некоторое время используются для решения повседневных задач. А вот что делает облачные вычисления по-настоящему новой и замечательной технологией, так это то, что они используют возможности существующих технологий и дают нам новые способы работы с масштабируемыми инфраструктурами, приложениями и службами. По популярности облачные вычисления быстро обгоняют традиционные компьютерные сети благодаря гибкости и экономичности облачных сред.

Существуют три модели обслуживания, принятые в облачных инфраструктурах:

- *IaaS (Infrastructure as a Service, инфраструктура как услуга)*. По этой модели с помощью облака предоставляется доступ к обычному аппаратному обеспечению, формирующему инфраструктуру сети. Благодаря модели IaaS потребители услуг могут арендовать серверы, хранилища, сетевые ресурсы и контролировать их конфигурацию. Amazon Web Services и Google Compute Engine — это примеры IaaS.
- *PaaS (Platform as a Service, платформа как услуга)*. При использовании этой модели потребитель благодаря облаку получает не только традиционные аппаратные компоненты, но и операционные системы, базы данных и другое серверное ПО (такое как веб-сервер). Кроме того, по модели PaaS обычно предоставляется доступ к средствам разработки программного обеспечения. К PaaS-решениям относятся Microsoft Azure и Amazon Electric Beanstalk.
- *SaaS (Software as a Service, программное обеспечение как услуга)*. Эта модель позволяет потребителю использовать приложения, доступные в облаке. Например, Microsoft Office 365 и Salesforce.com — это SaaS-решения.

Существуют три способа внедрения облачных инфраструктур: частные (private), публичные (public) и гибридные (hybrid) облака. Частные облачные

инфраструктуры, как и обычные локальные сети, разворачивают в пределах организации, они отделены от Интернета брандмауэром и закрыты для внешнего доступа. Публичные облака — это службы, которые поддерживают провайдеры услуг. Эти службы используются множеством потребителей. Компании все чаще покупают подписку на подобные службы у IaaS-провайдеров, таких как Amazon. И наконец, большинство организаций не размещают всю свою инфраструктуру в облаке. Вместо этого они реализуют гибридные облачные решения, а именно: используют для решения каких-либо задач публичные облачные службы, а некоторые системы размещают в пределах частного облака. Делается это для обеспечения конфиденциальности, настройки облачных сред в соответствии с некими внутренними требованиями организаций, решения вопросов совместимости. Например, организация может решить использовать службу Azure в качестве платформы для разработки программного обеспечения, но пользоваться ПО, созданным с помощью Azure, в частной сети.

В то время как облачные вычисления имеют множество достоинств, их использование сопряжено с решением непростых управленческих задач. Обеспечение безопасности — вот одна из задач первостепенной важности. Кроме того, необходимо эффективно выделять ресурсы и отслеживать их использование, для того чтобы облачные услуги соответствовали договорам о качестве обслуживания, заключаемым с потребителями.

Благодаря Hyper-V R3 и новым сетевым возможностям Server 2012 у организаций появляются инструменты, которые позволяют не только создавать собственные, частные облачные среды, но и предлагать услуги облачных служб сторонним потребителям. Кроме того, Server 2012 позволяет системным администраторам справиться с потенциальными сложностями в работе с облачными средами, управляя виртуальными сетями.

Важно помнить, что виртуализация — это фундаментальная технология, лежащая в основе облачных вычислений. Множество новых сетевых возможностей касаются не только физических сетей, но и виртуальных. Для начала давайте взглянем на две наиболее значительные новые сетевые возможности Server 2012.

IPAM

IPAM (Internet Protocol address management, управление IP-адресами) — это новое средство для управления IP-адресами в сети. С помощью IPAM

системные администраторы могут автоматически обнаруживать IP-адреса в инфраструктуре, выполнять аудит изменений IP-адресов и создавать отчеты по данным IP-адресов.

IPAM — это важная новая возможность, так как при возрастании уровня виртуализации сети и расширении использования облачных служб IP-адреса назначают удаленным компьютерам и виртуальным машинам, а не только физическим локальным узлам сети. Управление IP-адресами может стать несколько запутанным, учитывая то, что в одной сетевой инфраструктуре возможно существование физических, виртуальных и облачных сетей. IPAM дает администраторам средство для централизованного наблюдения за физическими и виртуальными компьютерами в пространстве сетевых IP-адресов. Кроме того, система IPAM интегрирована с DHCP (Dynamic Host Configuration Protocol, протокол динамической настройки узла), DNS (Domain Name System, система доменных имен) и Active Directory — это всеобъемлющее средство для управления сетью.

IPAM хранит во внутренней базе данных Windows информацию об IP-адресах за три года, в том числе сведения об аренде IP-адресов, о MAC-адресах, входе пользователей в систему и выходе из нее. К сожалению, в настоящее время нельзя настроить автоматическую очистку этой базы данных либо очистку по расписанию. Системные администраторы при необходимости должны выполнять эту процедуру самостоятельно.

Хотя IPAM поддерживает и IPv4, и IPv6, в работе IPAM с IPv6 есть некоторые ограничения. IPAM отслеживает тренды использования только для адресов IPv4. Кроме того, поддержка освобождения IP-адресов (IP address reclaiming) — ситуация, при которой DHCP пытается освободить неиспользуемый IP-адрес, когда клиент делает запрос, — в IPAM возможна только для IPv4-адресов.

IPAM-серверы могут быть развернуты в отдельных центрах ответственности организации, либо организация может развернуть единый центральный IPAM-сервер. Особенности развертывания зависят от размеров организации и количества сетевых узлов. Большая корпорация, имеющая филиалы и тысячи компьютеров-клиентов, вероятнее всего, развернет несколько IPAM-серверов в местах их использования. В то же время небольшая организация, имеющая сотни или меньше клиентских компьютеров, сможет довольствоваться единым централизованным IPAM-сервером. Один IPAM-сервер поддерживает до 150 DHCP-серверов, 500 серверов DNS, до 6000 областей DHCP и до 150 зон DNS.

Установка IPAM

При развертывании IPAM-сервера нужно учесть некоторые требования и ограничения.

- Установка IPAM требует 512 Мбайт оперативной памяти.
- Компьютер, на котором будет установлен IPAM, должен работать под управлением Server 2012.
- IPAM поддерживает только контроллеры домена, DHCP, DNS и NPS-серверы, работающие на уровне Windows Server 2008 и выше.
- Поддерживается только внутренняя база данных Windows.
- IPAM поддерживает использование лишь одной внутренней базы данных Windows.

Наилучшим образом IPAM работает в том случае, если он установлен на отдельном сервере, подключенном к домену, работающему под управлением Windows Server 2012 и не имеющему других ролей. Не рекомендовано устанавливать IPAM на контроллере домена или на сервере, на котором работает служба DHCP. Для развертывания IPAM выполните следующее:

1. В диспетчере серверов щелкните на ссылке **Добавить роли и компоненты** (Add Roles and Features). Выберите **Установка ролей или компонентов** (Role-based or feature-based installation). Щелкните на кнопке **Далее** (Next). Выберите сервер, на котором нужно установить IPAM. Снова щелкните на кнопке **Далее** (Next).
2. В меню, которое расположено в левой части окна **Выбор ролей сервера** (Select server roles), щелкните на пункте **Компоненты** (Features). В окне выбора компонентов установите флажок **Сервер управления IP-адресами (IPAM)** (IP Address Management (IPAM)).
3. При развертывании IPAM требуется установить некоторые дополнительные компоненты. Диспетчер серверов предложит их список, вам достаточно будет щелкнуть на кнопке **Добавить компоненты** (Add Features) в соответствующем окне. Теперь щелкните на кнопке **Далее** (Next), установите флажок для автоматического перезапуска сервера, если это потребуется. Щелкните на кнопке **Установить** (Install). После этого начнется установка IPAM.

Когда установка завершится, IPAM будет доступен в панели мониторинга диспетчера серверов.

Настройка IPAM

Когда вы в первый раз откроете IPAM в диспетчере серверов, нужно будет выполнить некоторые настройки. Это можно сделать с помощью набора мастеров (рис. 8.1).

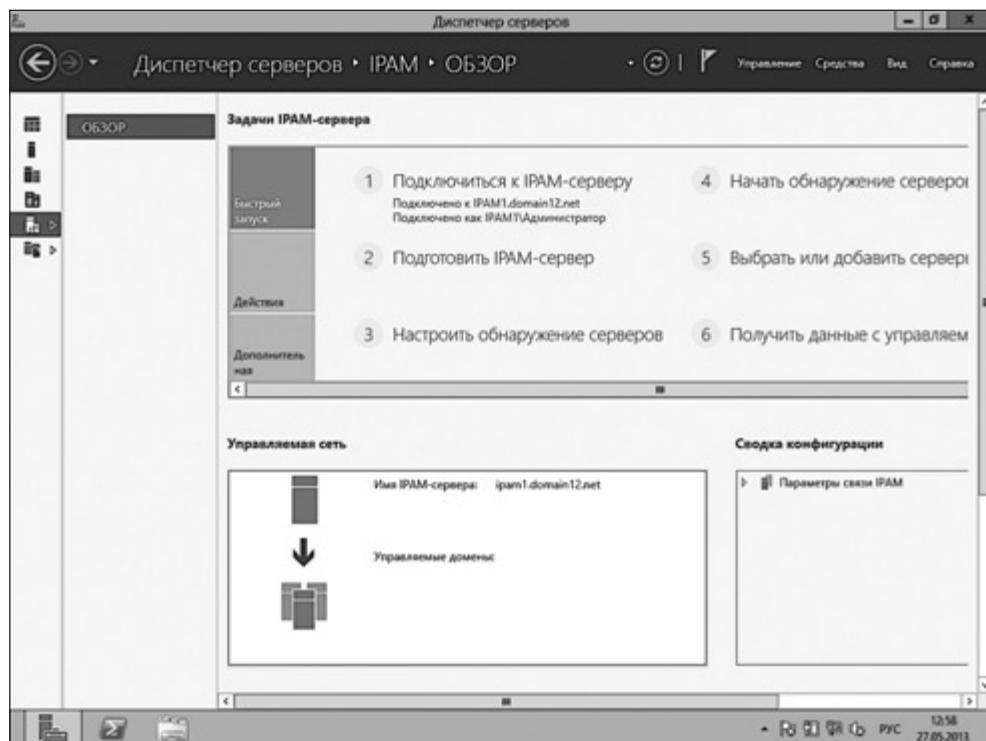


Рис. 8.1. Мастера настройки IPAM

Как только вы подключитесь к IPAM-серверу из диспетчера серверов, сделайте следующий шаг — подготовьте его к работе. Этот процесс включает в себя ручную или основанную на групповых политиках настройку доступа, необходимого для работы с управляемыми DHCP, DNS, NPS-серверами и контроллерами домена. В большинстве Windows-инфраструктур можно использовать подготовку к работе с использованием групповой политики для легкой интеграции с Active Directory.

Для того чтобы подготовить IPAM-сервер к работе с использованием групповой политики, щелкните на ссылке **Подготовить IPAM-сервер** (Provision the IPAM server) в окне **Задачи IPAM-сервера** (IPAM Server Tasks). Щелкните на

кнопке **Далее (Next)** и выберите метод подготовки — либо **Вручную (Manual)**, либо **На основе групповой политики (Group Policy Based)**.

Если вы воспользуетесь методом подготовки на основе групповой политики, то должны создать префикс имени GPO (Group Policy Object, объект групповой политики). Этот префикс используется в объектах групповой политики, добавленных к серверам, которыми будет управлять IPAM. Префикс добавляется к записям GPO на DHCP, DNS, NPS-серверах и контроллерах домена. Для каждого IPAM-сервера, который имеется в лесу Active Directory, нужен один уникальный префикс GPO.

На рис. 8.2 вы можете видеть, что в качестве префикса имени выбран GPOIPAM. То есть, например, GPO, созданный для DHCP-сервера, будет иметь вид GPOIPAM-DHCP. После проверки параметров щелкните на кнопке **Далее (Next)**, а затем на кнопке **Применить (Apply)**, для того чтобы завершить подготовку. Когда IPAM будет подготовлен к работе, отобразится окно с подтверждением выполненной операции.

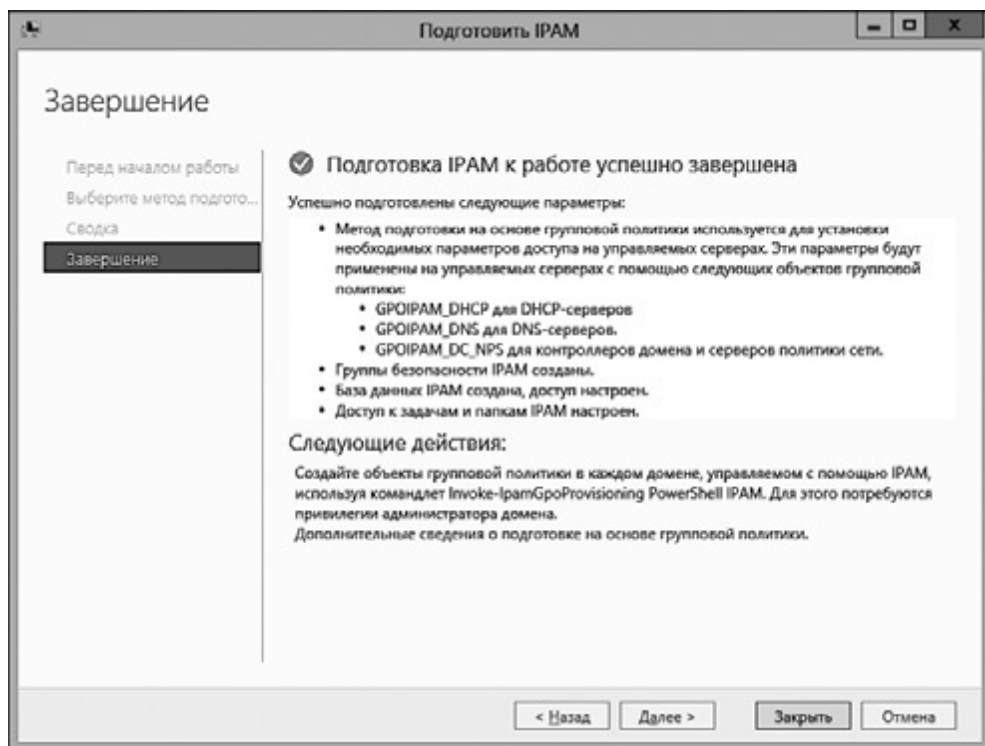


Рис. 8.2. Подготовка IPAM завершена



В многодоменных средах вы можете воспользоваться командой PowerShell `Invoke-IpamGPOProvisioning`. Этот командлет нужно выполнять после входа в систему с учетной записью, которая имеет права администратора домена. В итоге необходимые объекты GPO будут созданы в каждом домене.

Следующий после подготовки IPAM к работе шаг заключается в настройке обнаружения серверов. На экране обзора IPAM (IPAM Overview) в диспетчере серверов щелкните на ссылке **Настроить обнаружение серверов** (Configure server discovery) (рис. 8.3).

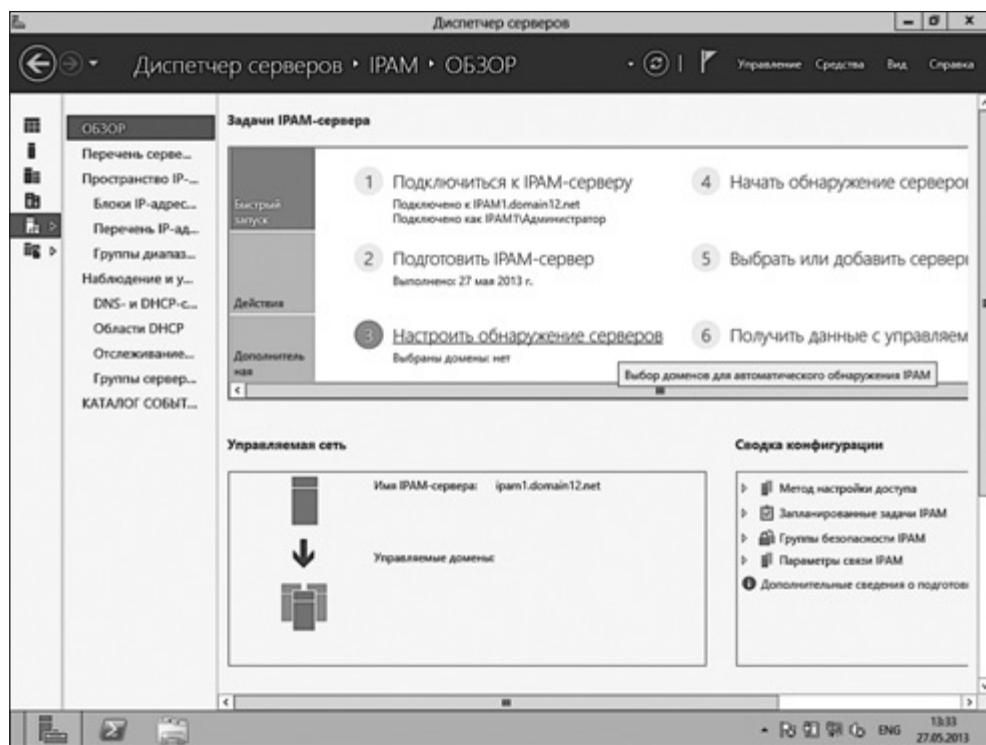


Рис. 8.3. Запуск мастера настройки обнаружения серверов IPAM

В окне **Настройка обнаружения серверов** (Configure Server Discovery) выберите домен (или домены) для обнаружения. Нажмите кнопку **Добавить** (Add), а затем **ОК** (рис. 8.4).

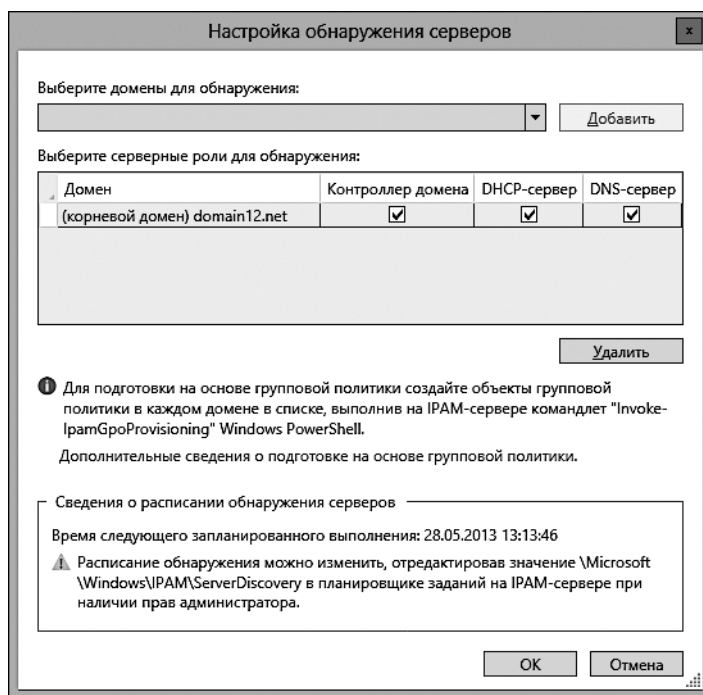


Рис. 8.4. Выбор доменов для обнаружения

Теперь щелкните на ссылке Начать обнаружение серверов (Start Server Discovery) на экране обзора IPAM (IPAM Overview) в диспетчере серверов. Диспетчер серверов выведет уведомление «В планировщике заданий выполняется одна или несколько задач IPAM. Дождитесь их завершения» (There are one or more IPAM tasks still running in the Task Scheduler. Please wait for their completion). Когда процесс обнаружения завершится, будет выведено сообщение с информацией о времени, когда были обнаружены серверы.

После завершения обнаружения щелкните на ссылке Выбрать или добавить серверы для управления и проверить доступ к IPAM (Select or add servers to manage and verify IPAM access) в окне обзора IPAM (IPAM Overview). Откроется окно с перечнем серверов по IP-адресам. Здесь должны быть перечислены контроллеры домена и DHCP-сервера. Перечисленные серверы, вероятнее всего, будут иметь статус управляемости Не определено (Unspecified) и состояние доступа к IPAM Блокировано (Blocked). Здесь нужно выполнить некоторые настройки, в частности воспользоваться средством Управление групповой политикой (Group Policy Management) на IPAM-сервере, перейти

по пути **Домены ► Объекты групповой политики (Domains ► Group Policy Object)** и убедиться в том, что там присутствуют три объекта:

- имя префикса `GPO_DC_NPS`;
- имя префикса `GPO_DHCP`;
- имя префикса `GPO_DNS`.

Если эти объекты еще не созданы, выполните (с учетной записью администратора домена) команду `Invoke-IpamGpoProvisioning` в PowerShell.

Если данные объекты присутствуют, вернитесь в диспетчер серверов, в окно **Обзор ► Перечень серверов (Overview ► Server Inventory)**, щелкните на одном из перечисленных серверов и выберите команду **Изменить сервер (Edit Server)** (рис. 8.5).

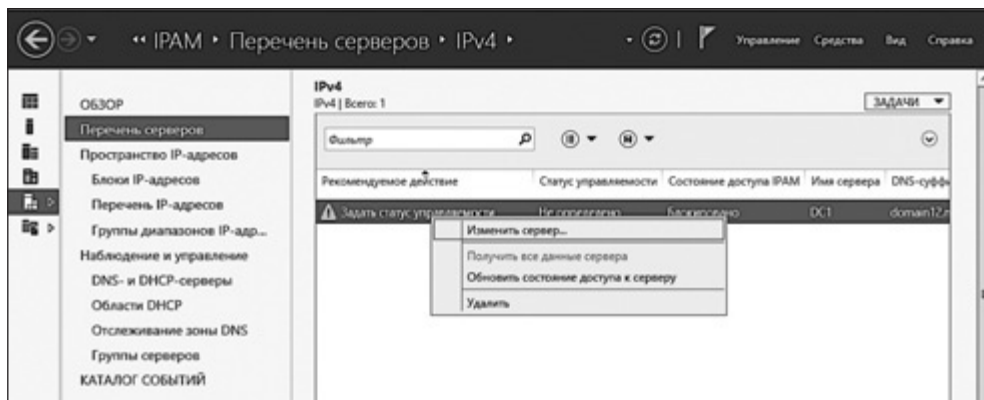


Рис. 8.5. Изменение статуса управляемости сервера

Из раскрывающегося списка для параметра **Статус управляемости (Manageability Status)** выберите **Управляемый (Managed)** и нажмите **ОК**. Сделайте это для каждого сервера, которым должен управлять IPAM.

На данном этапе настройки красный значок «х» в строке, соответствующей серверу, указывает на то, что доступ IPAM к серверу все еще заблокирован. Для того чтобы разблокировать доступ, выполните команду PowerShell `groupdate/force` на каждом сервере. После обновления групповой политики доступ IPAM будет разблокирован (рис. 8.6).



Рис. 8.6. Исправленное состояние управляемости сервера



Если доступ IPAM продолжает блокироваться, проверьте настройки брандмауэра и снова запустите `groupdate`.

На последнем шаге настройки IPAM в окне **Обзор IPAM** (IPAM Overview) нужно щелкнуть на ссылке **Получить данные с управляемых серверов** (Retrieve data from managed servers), для того чтобы получить сведения об IP-адресах с управляемых серверов.

Использование IPAM

Когда IPAM настроен, он выводит сведения о пространстве IP-адресов инфраструктуры. IPAM может автоматически обнаруживать сведения о диапазонах адресов IPv4 и IPv6 для всех активных DHCP-диапазонов на управляемых DHCP-серверах. IP-адреса на неуправляемых устройствах или на устройствах, работающих не под управлением ОС от Microsoft, могут быть добавлены вручную или импортированы из CSV-файлов (comma separated value, данные, разделенные запятой).

Если перейти в раздел **Блоки IP-адресов (IP Address Blocks)**, можно увидеть такие сведения, как начальные и конечные IP-адреса в сети, типы IP-адресов (общедоступные или частные), статические IP-адреса и количество IP-адресов, использованных в блоке адресов. Среди особенно полезных данных можно отметить уровень использования IP-адресов. Знание того, как в организации используются IP-адреса, помогает в планировании схем IP-адресации при добавлении в сеть новых узлов.

Кроме того, IPAM предоставляет централизованное рабочее место для мониторинга диапазонов и зон DHCP и DNS и управления ими. Благодаря этому вам не придется переключаться между различными окнами в диспетчере серверов. С помощью IPAM нельзя управлять серверами DNS и DHCP, однако, щелкнув правой кнопкой мыши на записи сервера в IPAM, вы можете открыть консоль управления для выбранного сервера.

Возможности IPAM

Основные возможности IPAM — это просмотр перечня серверов, управление пространством IP-адресов, вывод статистических данных, управление DHCP- и DNS-серверами и отслеживание их состояния, аудит, просмотр журнала событий.

В перечне серверов (Server inventory) показаны все серверы, работающие под управлением ОС не ниже Windows Server 2008 и управляемые IPAM. Данные о серверах собираются посредством Active Directory. По умолчанию при обнаружении серверов в перечень включаются все контроллеры домена, зарегистрированные в домене, а также DNS- и DHCP-серверы, работающие под управлением ОС от Microsoft. NPS-серверы автоматически не обнаруживаются, но их можно добавить вручную.

Серверы организованы в иерархическом виде. На первом уровне иерархии присутствует разделение по IPv4- и IPv6-адресам. На втором уровне серверы делятся по статусу управляемости (управляемые или неуправляемые). На третьем уровне признаком разделения служат подсети в средах с множеством подсетей (рис. 8.7).

Как уже было сказано, серверы в IPAM можно добавлять вручную. Для настройки управляемости сервера достаточно щелкнуть правой кнопкой мыши на группе, соответствующей нужной версии IP-адресов. На рис. 8.8 показано начало добавления NPS-сервера, работающего под управлением Windows Server 2008 R2, которому назначен статический IPv4-адрес. После щелчка появится команда **Добавить сервер (Add Server)**.

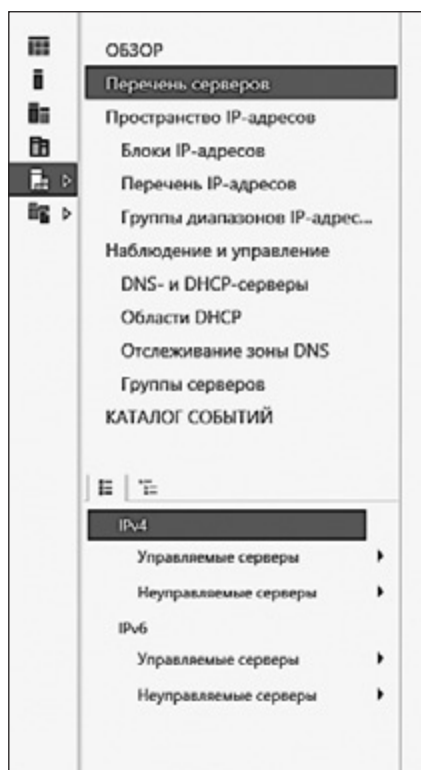


Рис. 8.7. Иерархическая классификация серверов

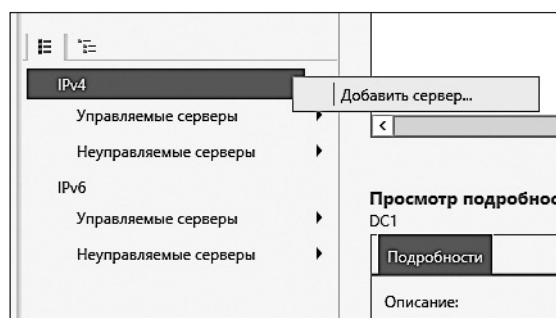


Рис. 8.8. Добавление сервера

При добавлении сервера введите в соответствующее поле IP-адрес или FQDN (fully qualified domain name, полностью определенное доменное имя), укажите тип сервера и статус его управляемости (выберите Управляемый (Managed), если данными об IP-адресах сервера можно управлять с помощью IPAM). Нажмите кнопку Проверить (Verify) (рис. 8.9).

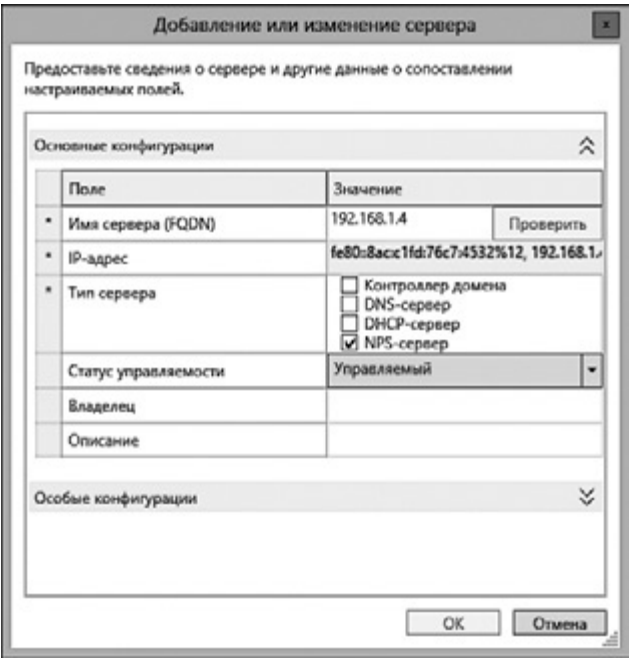


Рис. 8.9. Введение свойств при ручном добавлении сервера

Теперь NPS-сервер будет включен в перечень серверов. Для того чтобы управлять им с помощью IPAM, вам понадобится разблокировать доступ IPAM, как было рассказано ранее (рис. 8.10).

Если щелкнуть на записи, соответствующую серверу, в перечне серверов (Server Inventory) будет показано меню, с помощью которого можно получить данные сервера (то есть собрать информацию об IP-адресах), удалить сервер, отредактировать его свойства (такие как статус управляемости IPAM) или обновить состояние доступа к серверу (рис. 8.11).

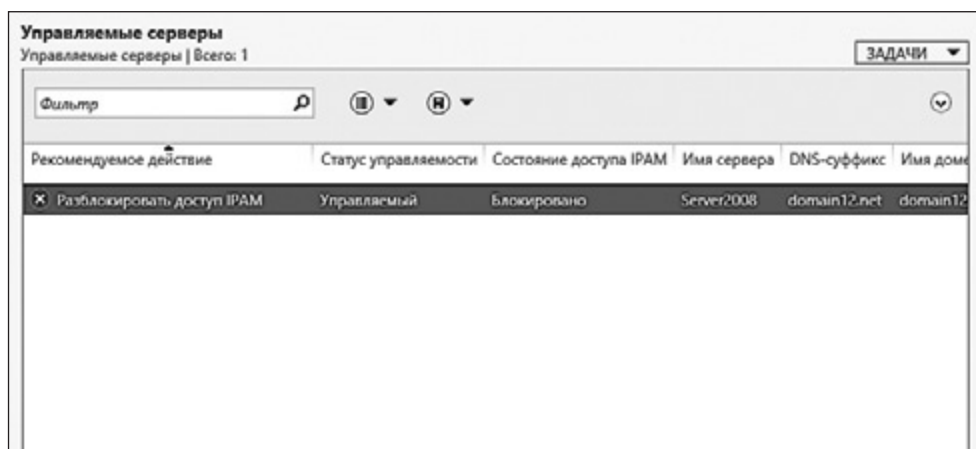


Рис. 8.10. Сервер, добавленный вручную

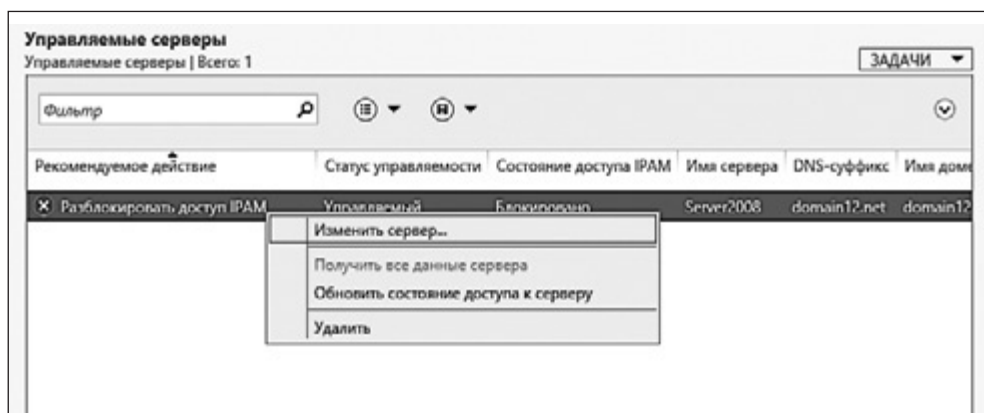


Рис. 8.11. Контекстное меню в IPAM

Средства управления пространством IP-адресов позволяют отслеживать состояние адресов, выполнять их аудит, управлять ими, строить отчеты по IP-адресам инфраструктуры. Пространство IP-адресов — это удобное средство для организации IP-адресов в сети. С помощью IPAM IP-адреса сети организуются в блоки IP-адресов. Блоки могут быть разбиты на диапазоны IP-адресов, которые, в свою очередь, можно использовать для выделения IP-адресов устройствам сети. Кроме того, крупные организации могут организовывать

диапазоны IP-адресов в группы диапазонов и размещать IP-адреса в настраиваемых группах.

В IPAM весьма просто создать блок IP-адресов — отправную точку для организации IP-адресов. Для того чтобы создать новый блок IP-адресов, выполните следующие действия:

1. Вызовите меню **Задачи (Tasks)** и выберите в нем команду **Добавить блок IP-адресов (Add IP Address Block)** (рис. 8.12).

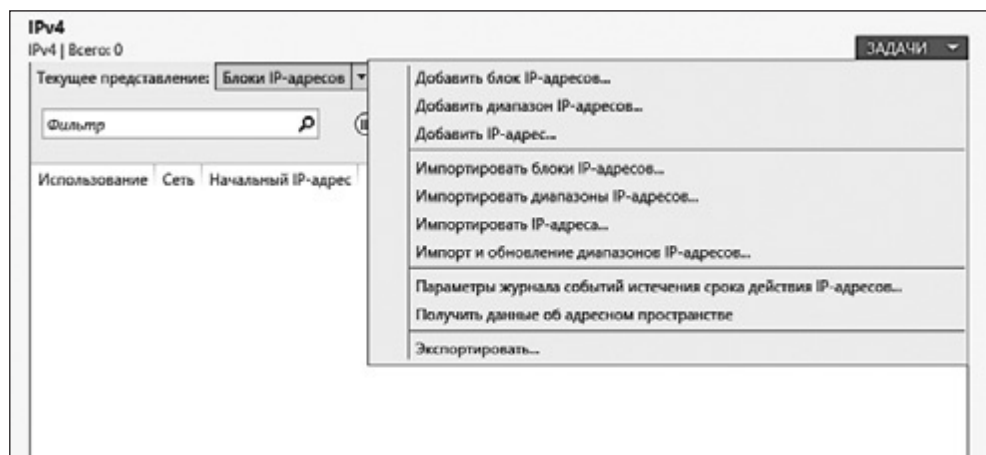


Рис. 8.12. Выбор команды **Добавить блок IP-адресов** из меню **Задачи**

2. В появившемся окне, в поле **ИД сети (Network ID)** введите начальный диапазон IP-адресов, которые требуется объединить в блок. В поле **Длина префикса (Prefix Length)** выберите 24, что позволит включить в диапазон адреса вплоть до 192.x.x.254. Нажмите кнопку **ОК**. Вы увидите заданный блок IP-адресов, а также процент адресов в блоке, которые уже используются. Выводится и уровень использования IP-адресов в блоке (рис. 8.13).

Область **Просмотр подробностей (Details View)** в IPAM содержит дополнительные сведения, такие как количество IP-адресов в блоке, назначенных в сети.

Кроме того, вы можете добавлять блоки IP-адресов для адресов IPv6 и общедоступных IP-адресов. Вы даже можете размещать адреса в других группах, заданных самостоятельно.

Использование	Сеть	Начальный IP-адрес	Конечный IP-адрес	RIR	Дата последнего назначения	Используется (%)
Недостаточное	192.168.1.0/24	192.168.1.0	192.168.1.255			0,00

Рис. 8.13. Добавленный блок IP-адресов

Пространства IP-адресов позволяют вам просматривать диапазоны и блоки IP-адресов, выделенные DHCP. Они не включают в себя статические IP-адреса, адреса устройств (таких как маршрутизаторы) сторонних производителей или мобильных устройств, которые могут быть подключены к сети. Видимо, IPAM не способен выполнять всесторонний анализ всех устройств сети с использованием SNMP (Simple Network Management Protocol, простой протокол сетевого управления), но вы можете найти подобную функциональность в некоторых сетевых утилитах сторонних производителей, таких как SolarWinds и Cisco.

Вы можете добавлять IP-адреса вручную, используя интерфейс IPAM либо импортируя их в виде CSV-файла. Например, предположим, что один из членов нашего домена — сервер, работающий под управлением Server 2008 R2, — имеет статический IP-адрес. Это не контроллер домена, поэтому IPAM не может обнаружить его самостоятельно. Но вы можете добавить этот сервер в IPAM следующим образом:

1. В разделе управления IPAM диспетчера серверов перейдите в раздел Перечень IP-адресов (IP Address Inventory). Щелкните на меню Задачи (Tasks) и выберите команду Добавить IP-адрес (Add IP Address) (рис. 8.14).
2. В окне Добавить IPv4-адрес (Add IPv4 Address) введите IP-адрес и MAC-адрес (media access control, управление доступом к среде) устройства. Здесь вы можете ввести и другие свойства, такие как тип назначения IP-адреса (динамический или статический) (рис. 8.15).

После этого вы можете увидеть добавленный вручную адрес в пространстве частных адресов (Private Address Space) IPv4 в IPAM (рис. 8.16).

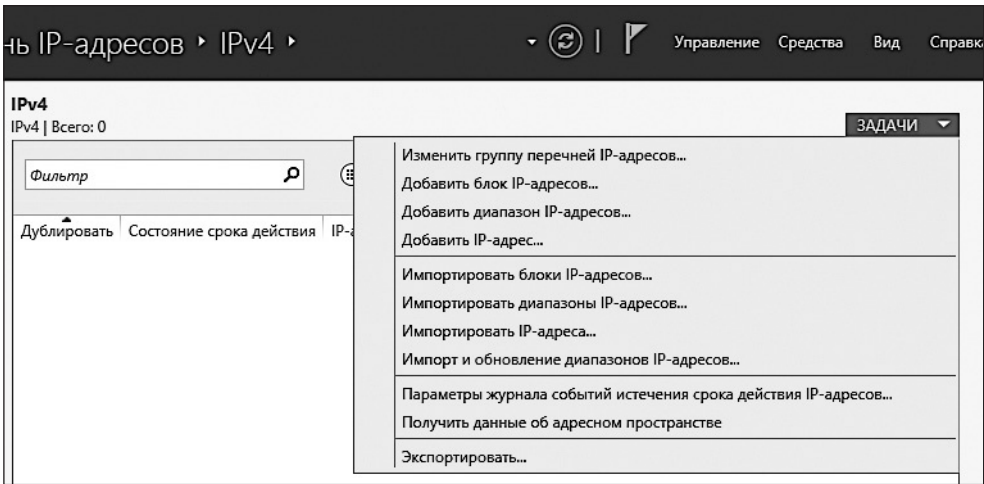


Рис. 8.14. Первый шаг добавления IP-адреса

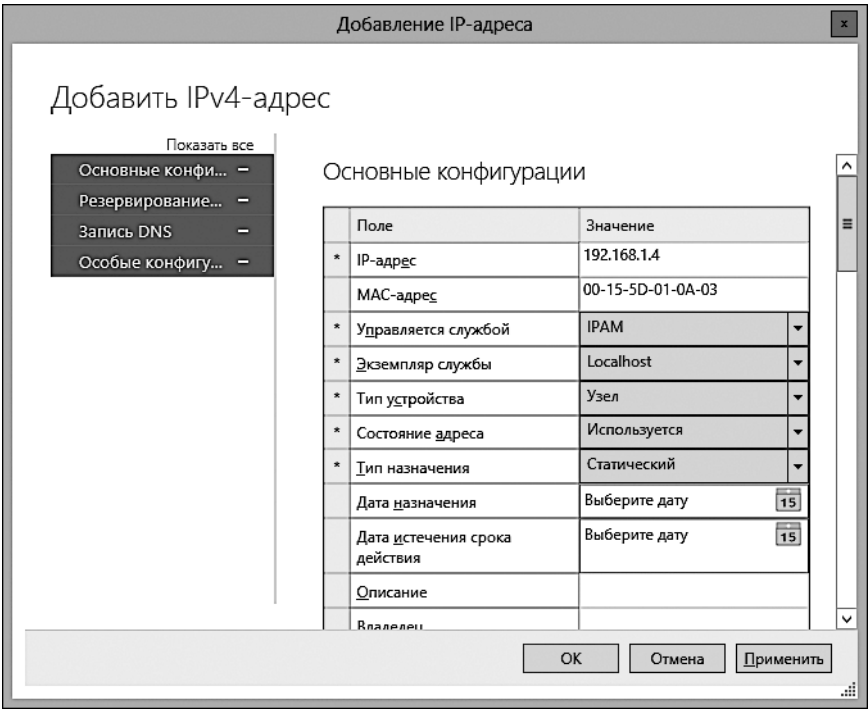


Рис. 8.15. Окно добавление IPv4-адреса

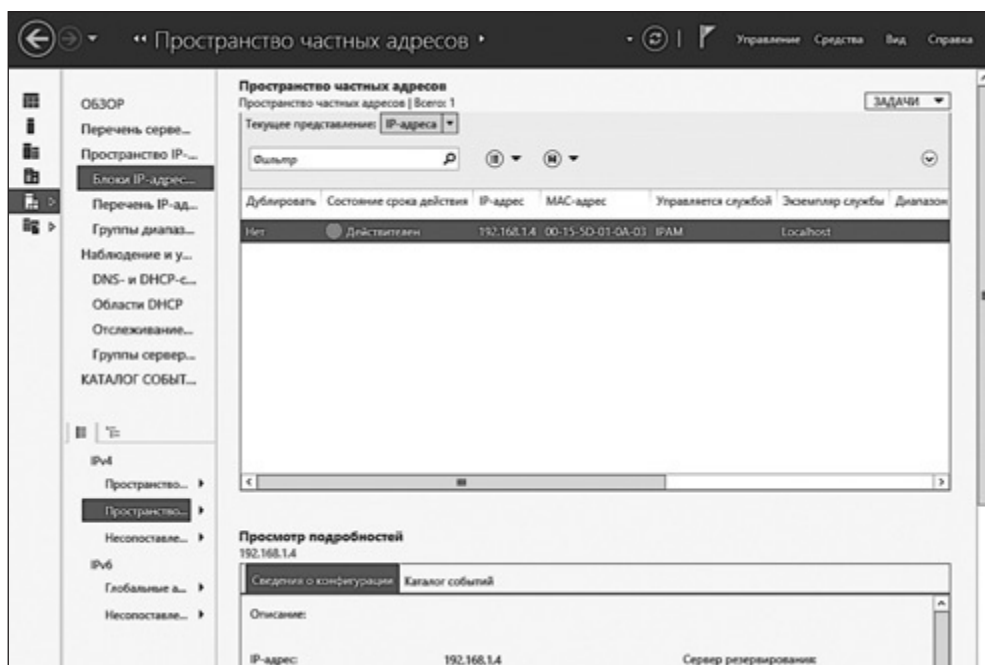


Рис. 8.16. IP-адрес, добавленный вручную

Вместо того чтобы добавлять IP-адреса в IPAM вручную, их можно импортировать из CSV-файла. Этот файл должен быть соответствующим образом подготовлен.

1. На DHCP-сервере пройдите в средство управления DHCP (DHCP Manager). В меню слева разверните папку **Арендованные адреса** (Address Leases) в группе **IPv4** или **IPv6** в зависимости от того, адреса какого типа вы хотите импортировать в CSV-файл.
2. Щелкните правой кнопкой мыши на папке **Арендованные адреса** (Address Leases) и выберите в появившемся меню команду **Экспортировать список** (Export List). Сохраните экспортируемые данные в виде CSV-файла.
3. В IPAM добавьте как минимум один IP-адрес в пространство адресов IPv4, как было показано ранее. Как только вы создадите этот IP-адрес, воспользуйтесь меню **Задачи** (Tasks) и выберите из него команду **Экспортировать** (Export). Эта команда позволяет экспортировать IP-адреса в правильно подготовленный CSV-файл.

Теперь вы готовы к импорту данных в IPAM.

4. Скопируйте содержимое файла, полученного после экспорта данных, из DHCP в файл, экспортированный из IPAM. На рис. 8.17 данные, экспортированные из IPAM, находятся выше пустого пространства, а данные, скопированные из файла, экспортированного из DHCP, — ниже.

```

"Duplicate", "Expiry Status", "IP Address", "MAC Address", "Managed by Service", "Service Instance", "IP Range",
"Device Name", "Device Type", "IP Address State", "Assignment Type", "Expiry Date", "DHCP Reservation Sync",
"DNS Host Record Sync", "DNS PTR Record Sync", "Assignment Date", "Owner", "Serial Number", "Asset Tag", "Description",
"Reservation Name", "Reservation Description", "Reservation Type", "Reservation Server", "Reservation Scope Name",
"Reservation Scope Details", "Forward Lookup Primary Server", "Forward Lookup Zone", "Reverse Lookup Primary Server",
"Reverse Lookup Zone", "AD Site", "Country or Region", "Microsoft Server Role", "Region", "RIR", "Type of Network",
"VMM DNS Suffix", "VMM IP Pool Name", "VMM Logical Network"
"No", "Not expired", "192.168.1.4", "00-15-5D-01-0A-03", "IPAM", "Localhost", "", "", "Host", "In-Use", "Static", "", "Not Att

Client IP Address, Name, Lease Expiration, Type, Unique ID, Description, Network Access Protection, Probation Expiration,
192.168.1.2,, 8/13/2012 1:25:16 AM, DHCP, b407f9ae54a1,, Full Access, N/A, None,
192.168.1.27, Client8.DOMAIN1.NET, 8/12/2012 9:00:28 AM, DHCP, 00155d010a00,, Full Access, N/A, None,
192.168.1.28, Client7.DOMAIN1.NET, 8/12/2012 5:41:44 PM, DHCP, 00155d010a01,, Full Access, N/A, None,
192.168.1.29, android_cdf93ef3465b4113.DOMAIN1.NET, 8/12/2012 6:35:28 PM, DHCP, c8aa21410bdf,, Full Access, N/A, None,
192.168.1.40, Slynn.DOMAIN1.NET, 8/12/2012 3:12:56 AM, DHCP, 002710af4f5c,, Full Access, N/A, None,
192.168.1.42, HP-HP.DOMAIN1.NET, 8/12/2012 3:13:34 AM, DHCP, 0015005d12b0,, Full Access, N/A, None,

```

Рис. 8.17. Данные, экспортированные из IPAM, находятся выше пустого пространства, данные из DHCP — ниже

5. Нам нужно импортировать шесть IP-адресов, которые имеются в данных, полученных из DHCP, поэтому следует скопировать строку, описывающую параметры адреса 192.168.1.4, импортированного из IPAM, и сделать пять ее копий. Затем вставить в эти строки IP-адреса и MAC-адреса, полученные из DHCP. После этого сохранить полученный файл в формате *.csv*.
6. Теперь импортируем эти шесть IP-адресов, отражающих данные, хранящиеся в DHCP (в данном примере в моей небольшой тестовой среде есть лишь шесть адресов, назначенных DHCP; вы можете импортировать любое количество адресов, назначенных DHCP-сервером, работающим в вашей сети). Напоминаю, нужно сделать пять копий строки адреса 192.168.1.4 из данных, полученных с IPAM-сервера, после чего скопировать в соответствующие места этих строк IP-адреса и MAC-адреса, полученные из DHCP (рис. 8.18). Не забудьте сохранить файл в формате *.csv*.

```

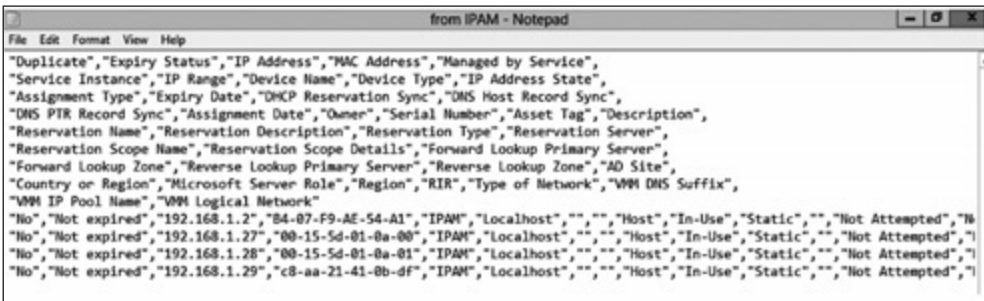
"Duplicate","Expiry Status","IP Address","MAC Address","Managed by Service","Service Instance","IP Range",
"Device Name","Device Type","IP Address State","Assignment Type","Expiry Date","DHCP Reservation Sync",
"DNS Host Record Sync","DNS PTR Record Sync","Assignment Date","Owner","Serial Number","Asset Tag","Description",
"Reservation Name","Reservation Description","Reservation Type","Reservation Server","Reservation Scope Name",
"Reservation Scope Details","Forward Lookup Primary Server","Forward Lookup Zone","Reverse Lookup Primary Server",
"Reverse Lookup Zone","AD Site","Country or Region","Microsoft Server Role","Region","RIR","Type of Network",
"WMM DNS Suffix","WMM IP Pool Name","WMM Logical Network"
"No","Not expired","192.168.1.4","00-15-5D-01-8A-03","IPAM","Localhost","","","Host","In-Use","Static","","Not Att
"No","Not expired","192.168.1.2","b4-07-f9-ae-54-a1","IPAM","Localhost","","","Host","In-Use","Static","","Not Att
"No","Not expired","192.168.1.4","00-15-5D-01-8A-03","IPAM","Localhost","","","Host","In-Use","Static","","Not Att
"No","Not expired","192.168.1.4","00-15-5D-01-8A-03","IPAM","Localhost","","","Host","In-Use","Static","","Not Att
"No","Not expired","192.168.1.4","00-15-5D-01-8A-03","IPAM","Localhost","","","Host","In-Use","Static","","Not Att
"No","Not expired","192.168.1.4","00-15-5D-01-8A-03","IPAM","Localhost","","","Host","In-Use","Static","","Not Att

Client IP Address,Name,Lease Expiration,Type,Unique ID,Description,Network Access Protection,Probation Expiration,
192.168.1.2,,8/13/2012 1:25:16 AM,DHCP,b407f9ae54a1,Full Access,N/A,None,
192.168.1.27,Client8.DOMAIN1.NET,8/12/2012 9:00:28 AM,DHCP,00155d010a00,Full Access,N/A,None,
192.168.1.28,Client7.DOMAIN1.NET,8/12/2012 5:41:44 PM,DHCP,00155d010a01,Full Access,N/A,None,
192.168.1.29,android_cdf93ef3465b4113.DOMAIN1.NET,8/12/2012 6:35:28 PM,DHCP,c8aa21410bdf,Full Access,N/A,None,
192.168.1.40,5lynn.DOMAIN1.NET,8/12/2012 3:12:56 AM,DHCP,002710af4f5c,Full Access,N/A,None,
192.168.1.42,HP-PP.DOMAIN1.NET,8/12/2012 3:13:34 AM,DHCP,0015005d12b0,Full Access,N/A,None,

```

Рис. 8.18. Подготовка файла для импорта данных в IPAM

Файл, готовый к импорту в IPAM, показан на рис. 8.19.



```

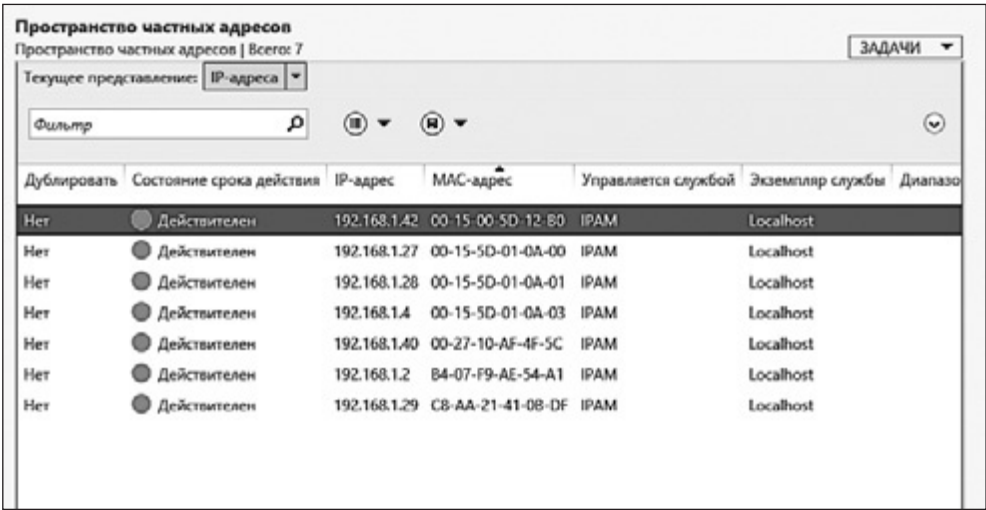
File Edit Format View Help
from IPAM - Notepad
"Duplicate","Expiry Status","IP Address","MAC Address","Managed by Service",
"Service Instance","IP Range","Device Name","Device Type","IP Address State",
"Assignment Type","Expiry Date","DHCP Reservation Sync","DNS Host Record Sync",
"DNS PTR Record Sync","Assignment Date","Owner","Serial Number","Asset Tag","Description",
"Reservation Name","Reservation Description","Reservation Type","Reservation Server",
"Reservation Scope Name","Reservation Scope Details","Forward Lookup Primary Server",
"Forward Lookup Zone","Reverse Lookup Primary Server","Reverse Lookup Zone","AD Site",
"Country or Region","Microsoft Server Role","Region","RIR","Type of Network","WMM DNS Suffix",
"WMM IP Pool Name","WMM Logical Network"
"No","Not expired","192.168.1.2","b4-07-f9-ae-54-a1","IPAM","Localhost","","","Host","In-Use","Static","","Not Attempted","N
"No","Not expired","192.168.1.27","00-15-5d-01-8a-00","IPAM","Localhost","","","Host","In-Use","Static","","Not Attempted","I
"No","Not expired","192.168.1.28","00-15-5d-01-8a-01","IPAM","Localhost","","","Host","In-Use","Static","","Not Attempted","I
"No","Not expired","192.168.1.29","c8-aa-21-41-0b-df","IPAM","Localhost","","","Host","In-Use","Static","","Not Attempted","I

```

Рис. 8.19. Файл, готовый к импорту

- Теперь импортируем CSV-файл в IPAM. В диспетчере серверов IPAM-сервера выберите пункт Перечень IP-адресов (IP Address Inventory), для того чтобы выделить его, после чего в нижней части меню щелкните либо на пункте IPv4, либо на пункте IPv6 в зависимости от того, адреса какого типа вы импортируете. В меню Задачи (Tasks) выберите команду Импортировать IP-адреса (Import IP Addresses) и найдите подготовленный ранее CSV-файл.

IPAM выдаст подтверждение после завершения импорта адресов. Если в ходе этой операции произошли какие-либо ошибки, об этом также будет сообщено. Теперь вместо одного IP-адреса, который мы добавили ранее вручную, в представлении Пространство частых адресов (Private Address Space) IPv4 появились адреса из CSV-файла (рис. 8.20).



Пространство частных адресов
Пространство частных адресов | Всего: 7

Текущее представление: IP-адреса

Фильтр

Дублировать	Состояние срока действия	IP-адрес	MAC-адрес	Управляется службой	Экземпляр службы	Диапазо
Нет	● Действителен	192.168.1.42	00-15-00-5D-12-80	IPAM	Localhost	
Нет	● Действителен	192.168.1.27	00-15-5D-01-0A-00	IPAM	Localhost	
Нет	● Действителен	192.168.1.28	00-15-5D-01-0A-01	IPAM	Localhost	
Нет	● Действителен	192.168.1.4	00-15-5D-01-0A-03	IPAM	Localhost	
Нет	● Действителен	192.168.1.40	00-27-10-AF-4F-5C	IPAM	Localhost	
Нет	● Действителен	192.168.1.2	B4-07-F9-AE-54-A1	IPAM	Localhost	
Нет	● Действителен	192.168.1.29	C8-AA-21-41-08-DF	IPAM	Localhost	

Рис. 8.20. IP-адреса, добавленные из CSV-файла

Конечно, неэффективно импортировать IP-адреса в сети, в которой имеются сотни клиентских систем. В то время как Microsoft предоставляет достойные средства для управления IP-адресами, организации могут воспользоваться (или продолжить пользоваться) средствами сторонних разработчиков для управления IP-адресами. Подобные средства можно применять и при выполнении обзора сети вместе с IPAM для организации дифференцированного управления всеми IP-адресами сети. Небольшие организации, имеющие менее 100 сетевых узлов, вполне смогут довольствоваться возможностями IPAM по импорту IP-адресов и другими его возможностями для управления IP-адресами.

Сведения об использовании IP-адресов в IPAM

Одна из ключевых возможностей IPAM заключается в визуализации использования IP-адресов. IPAM предоставляет сведения об использовании диапазонов IP-адресов, блоков адресов и групп диапазонов адресов.

Для групп диапазонов IP-адресов в IPAM можно просматривать сведения об уровне использования адресов — он может быть недостаточным, избыточным либо находиться в оптимальном состоянии. Кроме того, в области Просмотр подробностей (Details View) можно построить линейный график. Он показывает тренд использования адресов в заданный период (рис. 8.21).

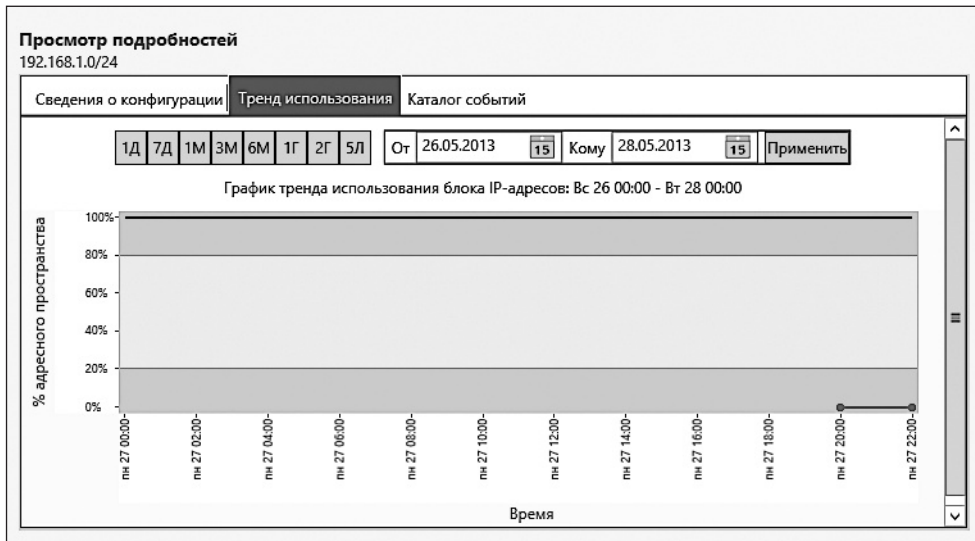


Рис. 8.21. Тренд использования IP-адресов

Команду Найти и выделить доступный IP-адрес (Find and Allocate Available IP Address) по достоинству оценит любой системный администратор, который тратил время на то, чтобы выяснить, какой именно IP-адрес свободен, чтобы выделить его новому устройству. Щелчок правой кнопкой мыши на группе диапазона IP-адресов позволит вам воспользоваться упомянутой командой для поиска и выделения доступного IP-адреса. Когда вы выбираете эту команду, появляется окно Поиск и выделение доступного IP-адреса (Find and Allocate Available IP Address) (рис. 8.22). IPAM отправляет запросы по неиспользуемым IP-адресам и пытается разрешить их с помощью DNS.

Так же полезно, как и нахождение неиспользуемых IP-адресов, будет нахождение доступных адресов, которые вы можете зарезервировать в DHCP, добавить в область DHCP или для которых выполнить другие задачи, такие как создание в DNS записи для IP-адреса. Причем все это можно сделать в IPAM, без необходимости работать с DNS- или DHCP-сервером.

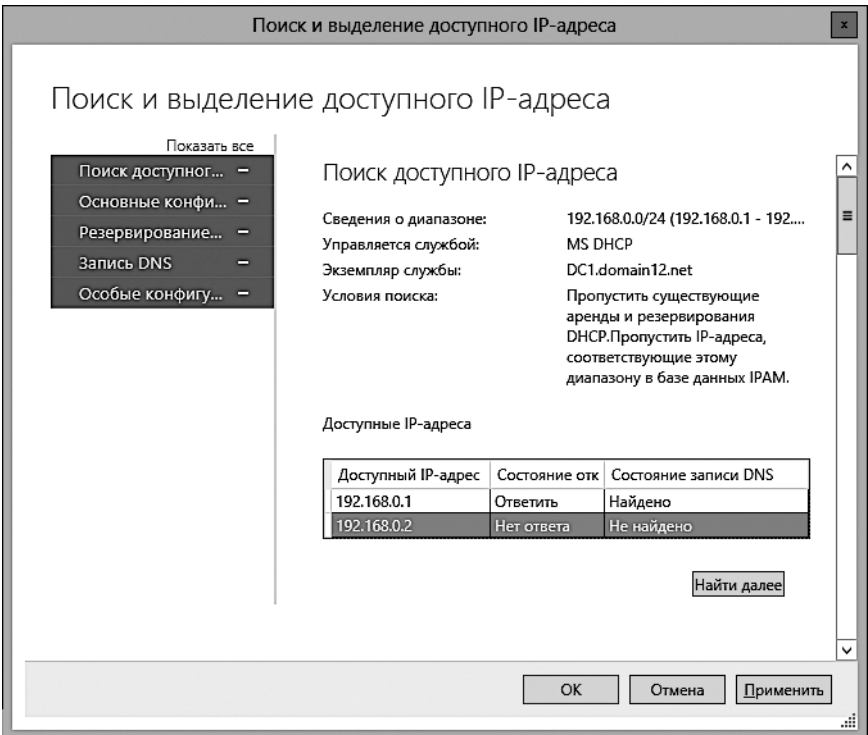


Рис. 8.22. Поиск и выделение неиспользуемых IP-адресов

IPAM позволяет также освобождать неиспользуемые арендованные IP-адреса. Это можно сделать, щелкнув правой кнопкой мыши на соответствующей группе IP-адресов и выбрав команду Освободить IP-адреса (Reclaim IP Address).

Управление DHCP- и DNS-серверами и их мониторинг с помощью IPAM

Как уже сказано, IPAM позволяет управлять DHCP- и DNS-серверами с помощью собственной консоли, что помогает экономить время на администрирование системы. В консоли IPAM вы можете создавать или отменять DHCP-резервирование для IP-адресов, работать с DNS-записями.

Среди других задач, которые можно выполнить с помощью IPAM, — редактирование параметров DHCP-сервера и создание областей DHCP.

Аудит и события

Аудит IP-адресов реализован в IPAM с помощью двух важных функций: отслеживания IP-адресов и каталога событий. Используя систему отслеживания, можно строить и исполнять запросы, которые выполняют поиск по IP- и MAC-адресам, именам компьютеров или именам пользователей. Отслеживание позволяет выполнять поиск по заданным событиям, связанным с IP-адресами, которые произошли в указанный период.

Кроме того, IPAM записывает в журнал события, например такие, как сведения об изменениях, внесенных в конфигурацию DHCP- и IPAM-серверов.

Как и в случае с другими ролями Windows Server, вы можете управлять IPAM удаленно, используя IPAM-клиент. Он является частью средств удаленного управления, которые можно загрузить, воспользовавшись службой загрузок Microsoft, и установить на любом клиентском компьютере, работающем под управлением Windows 8. Удаленный администратор должен быть членом группы WinRMRemoteWMIUsers на IPAM-сервере и членом соответствующей группы безопасности IPAM (или локальной группы администраторов).

Объединение сетевых карт

Объединение сетевых карт (NIC (network interface card) teaming) теперь является собственной возможностью Windows Server 2012. С помощью объединения несколько сетевых карт могут быть сгруппированы для обеспечения балансировки нагрузки и создания отказоустойчивых сетевых соединений без использования программного или аппаратного обеспечения сторонних разработчиков.

Балансировка нагрузки, выполняемая благодаря объединению сетевых карт, позволяет агрегировать пропускную способность сети. Например, система, работающая под управлением Server 2012 с двумя сетевыми адаптерами, каждый из которых имеет пропускную способность 1 Гбит/с, при их объединении получает пропускную способность 2 Гбит/с.

Технология объединения сетевых адаптеров Windows Server 2012 создана из расчета на работу с сетевыми картами любых производителей. Для агрегации пропускной способности или обеспечения отказоустойчивости оба адаптера должны поддерживать одну и ту же скорость соединения.

Выполнить объединение сетевых карт довольно просто. В следующем примере мы создадим группу сетевых адаптеров в системе, объединив встроенную сетевую карту с дополнительной картой, каждая из которых поддерживает скорость передачи данных 1 Гбит/с. Для того чтобы подготовить карты к объединению, нужно сделать следующее:

- 1. В окне Локальный сервер (Local Server) в панели мониторинга диспетчера серверов нажать ссылку Отключено (Disabled), которая расположена напротив пункта Объединение сетевых карт (NIC Teaming) (рис. 8.23).

Имя компьютера	DC1
Домен	domain12.net
Брандмауэр Windows	Домен: Отключено
Удаленное администрирование	Включено
Удаленный рабочий стол	Отключено
Объединение сетевых карт	Отключено
Ethernet	192.168.0.1, Поддержка IPv6
Ethernet_1	IPv4-адрес назначен DHCP, Поддержка IPv6
Версия операционной системы	Майкрософт Ознакомительная версия Windows Server 2012 Datacenter
Сведения об оборудовании	Gigabyte Technology Co., Ltd. GA-990FXA-D3

Рис. 8.23. Включение объединения сетевых карт в диспетчере серверов

- 2. Будет открыто окно Объединение сетевых карт (NIC Teaming). В области Группы (Teams) вызовите раскрывающееся меню Задачи (Tasks) и выберите команду Создать группу (New Team) (рис. 8.24).

Дайте группе имя и выберите адаптеры для включения в нее (рис. 8.25).

При создании группы можно настроить ее дополнительные свойства. В частности, свойство Не зависит от коммутатора (Switch Independent), которое означает, что дополнительных настроек не понадобится и адаптеры можно подключить к различным коммутаторам для объединения в группу. Параметр Хэш адреса (Address Hash) позволяет включить балансировку нагрузки и агрегацию пропускной способности. Параметр Резервный адаптер (Standby Adapter) позволяет для обеспечения отказоустойчивости системы задать сетевую карту, которая примет на себя нагрузку в том случае, если одна из карт откажет.

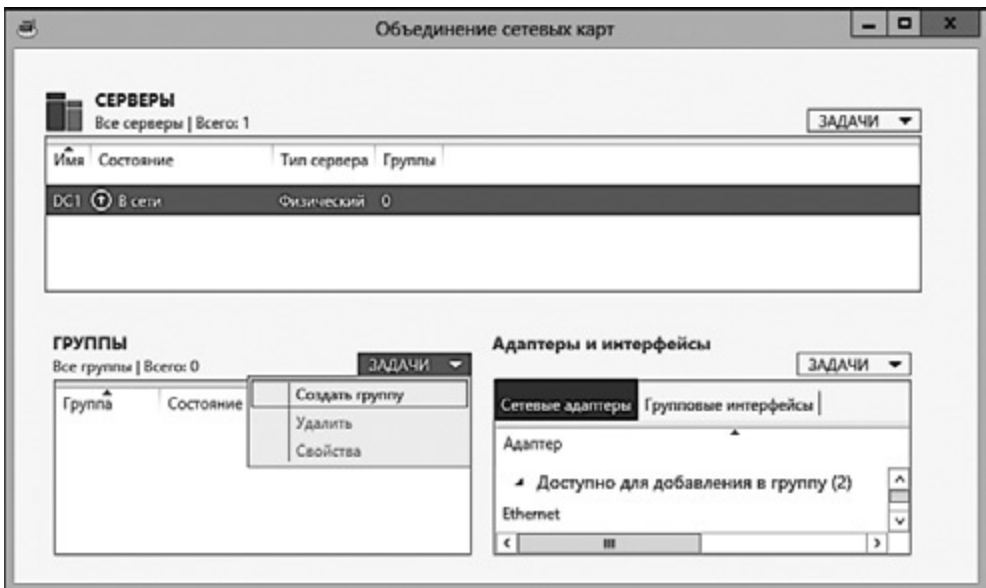


Рис. 8.24. Создание новой группы

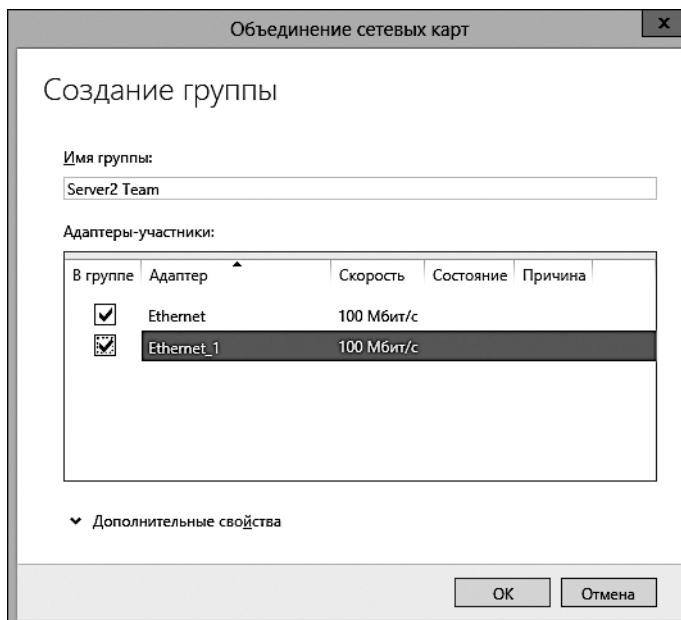


Рис. 8.25. Настройка группы сетевых карт

В этом примере перед объединением в группу к коммутатору Ethernet 10/100 были подключены две сетевые карты, пропускная способность каждой из которых 100 Мбит/с.

После объединения с параметрами Не зависит от коммутатора (Switch Independent) и Хэш адреса (Address Hash) сервер отображает карты в виде группы, агрегированная пропускная способность которой равняется 200 Мбит/с (рис. 8.26).

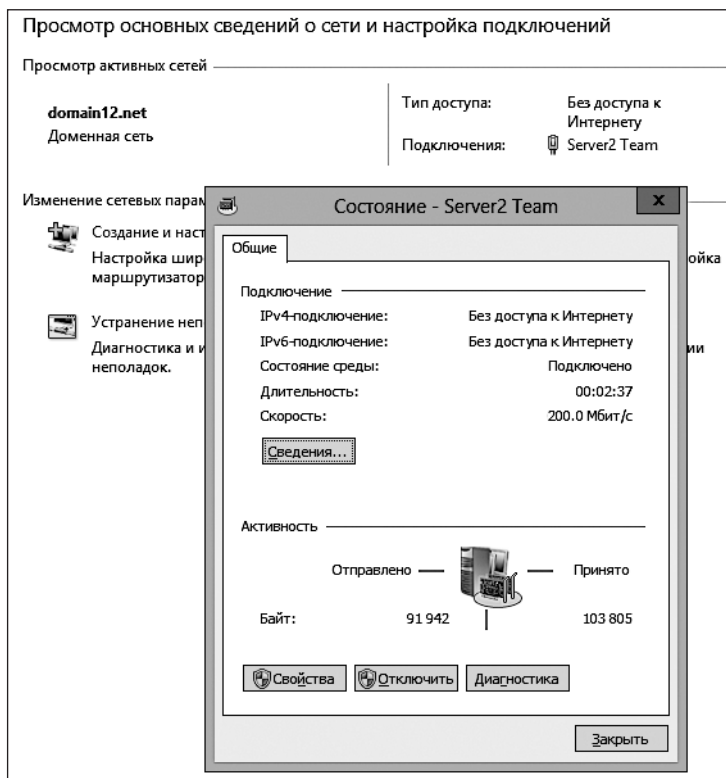


Рис. 8.26. Сетевые карты объединены для агрегации пропускной способности

Кроме того, можно объединять сетевые карты и для виртуальных машин. Например, вы можете подключить к коммутатору Нурег-V несколько виртуальных адаптеров для обеспечения отказоустойчивости в том случае, если один из адаптеров будет отключен.

Качество обслуживания

Управление качеством обслуживания (QoS, Quality of Service) — это функция, которую обычно связывают с сетевым аппаратным обеспечением, таким как маршрутизаторы. QoS в Windows Server 2012 работает так же, как на маршрутизаторах. Эта технология используется для указания приоритетности трафика. Например, в сетях, в которых развернута система VoIP (Voice over IP, передача голоса по протоколу IP), параметры QoS могут быть установлены для того, чтобы VoIP-трафик обладал приоритетом, что позволяет улучшить качество связи при совершении звонков с использованием VoIP. Сетевые администраторы могут использовать QoS для регулирования расхода трафика и измерения пропускной способности сети.

Нельзя сказать, что QoS впервые появилась в Server 2012. И в Server 2008 R2 можно было управлять качеством обслуживания, создавая соответствующие политики. Однако новым является набор возможностей управления QoS, которыми обладает Hyper-V. Существует два варианта использования QoS в Hyper-V. В корпоративных сетях эта технология может помочь в решении проблем с производительностью. Организациям, которые предоставляют клиентам доступ к облачным сервисам, использование QoS может помочь выполнять соглашения о качестве обслуживания (SLA, service-level agreement), закрепленные в договорах с потребителями услуг.

Система политик QoS в Hyper-V позволяет задавать минимальную пропускную способность и управлять сетевым трафиком. В Server 2008 R2 управление сетью с помощью QoS было ограничено указанием максимальной пропускной способности, что означало вероятность столкнуться с проблемами производительности в том случае, если различные типы сетевого трафика превысят этот уровень. При наличии возможности указания минимальной полосы пропускания установленный уровень не может быть уменьшен. задается конкретный уровень полосы пропускания.

Для того чтобы приступить к разворачиванию системы QoS в Hyper-V, настраивая виртуальную машину, установите флажок **Включить управление пропускной способностью** (Enable bandwidth management) и задайте минимальную и максимальную пропускную способность в мегабитах в секунду (рис. 8.27).

Установить минимальную полосу пропускания QoS можно и аппаратно. Для настройки уровня качества обслуживания некоторых видов трафика можно использовать сетевой адаптер, который поддерживает технологию моста для центра обработки данных (DCB, data center bridging).

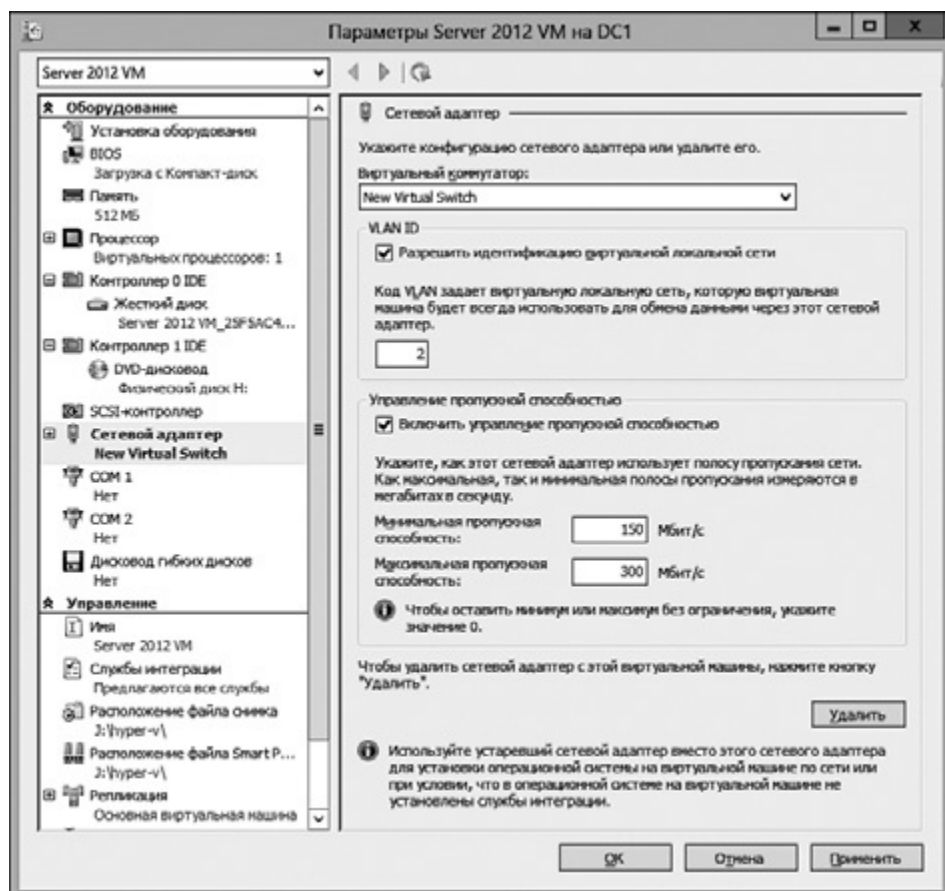


Рис. 8.27. Включение управления пропускной способностью

Групповые политики QoS

Групповые политики QoS в Windows Server 2012 можно создавать с помощью мастера групповых политик (Policy wizard) или PowerShell. Для того чтобы создать новую политику QoS с помощью мастера, сделайте следующее.

1. Запустите средство управления групповой политикой (Group Policy Management), щелкните правой кнопкой мыши на объекте Default Domain Policy (Групповая политика домена по умолчанию) и выберите команду для его правки. Разверните либо узел Конфигурация

компьютера (Computer Configuration), либо узел Конфигурация пользователя (User Configuration) в зависимости от того, для какого объекта вы собираетесь настроить групповую политику качества обслуживания (пользователя или компьютера). Обычно групповые политики QoS применяются к серверам. Затем пройдите по пути Политики ► Конфигурация Windows ► QoS на основе политики (Policies ► Windows Settings ► Policy-based QoS).

- Щелкните правой кнопкой мыши на объекте QoS на основе политики (Policy-based QoS) и выберите команду Создать новую политику (Create a QoS Policy). Задайте значение DSCP (differentiated services code point, точка кода дифференцированных услуг). Это значение позволяет назначать различные уровни качества обслуживания данным, передаваемым по сети. Здесь можно задавать значения от 0 до 63. Маршрутизаторы используют DSCP для классификации сетевых пакетов и постановки их в очередь на обслуживание. Чем больше значение, тем выше приоритет пакетов. Например, если данные, передаваемые по сети организации, включают в себя видеопотоки, причем такой трафик обладает высоким приоритетом, вы можете создать политику для видеоприложения и установить DSCP в значение 34 (рекомендованное значение для видеоданных). Также нужно будет создать другую политику для всех остальных данных, установив DSCP в значение по умолчанию, равное 0.

Теперь задайте частоту передачи исходящего трафика (outbound throttle rate). Если трафик обладает высоким приоритетом, очистите это поле — ограничение будет выключено. В противном случае оставьте для него значение по умолчанию. Щелкните на кнопке Далее (Next) и выберите приложение (или приложения), к которым будет применяться данная политика. Задайте исходный и конечные IP-адреса, к которым следует применять политику, укажите протокол и номер порта и нажмите Готово (Finish).

Помните о том, что параметры QoS можно настраивать и с помощью PowerShell.

Расширяемый управляемый коммутатор Hyper-V

Расширяемый коммутатор (Extensible Switch) Hyper-V R3 — это еще один ключевой компонент сетевых возможностей Windows Server 2012. С его

помощью сторонние разработчики могут создавать подключаемые модули для расширения возможностей управления Hyper-V. Даже раньше, чем был выпущен финальный релиз Windows Server 2012, производители начали разрабатывать и предлагать на рынке расширения для Hyper-V, которые способны выполнять широкий спектр задач — от помощи системным администраторам при монтировании виртуальных дисков до обеспечения безопасности виртуализированных окружений.

Настройка частных виртуальных локальных сетей

Виртуальный коммутатор Hyper-V, как и его физические аналоги, имеет средства для управления сетью. Например, одни виртуальные машины могут быть изолированы от других, что позволяет организациям разворачивать мультиарендные облачные службы. Изолировать виртуальные машины можно, поместив их в частные виртуальные локальные сети (PVLAN, Private Virtual Local Area Network). Частные виртуальные локальные сети служат не только для изоляции виртуальных сред, арендованных различными клиентами. Их можно использовать и для обеспечения безопасного доступа к сетевым ресурсам и безопасной передачи данных в сети между виртуальными машинами на физическом несущем компьютере.

На рис. 8.28 показан хост Hyper-V с четырьмя виртуальными машинами, подключенными к одному виртуальному коммутатору Hyper-V.

На виртуальных машинах 1 и 2 расположены данные и приложения, которыми пользуются отделы продаж и маркетинга. Таким образом, эти две виртуальные машины активно участвуют во взаимном обмене данными. Виртуальная машина 3 поддерживает функционирование базы данных, доступ к которой нужен остальным виртуальным машинам, подключенным к виртуальной сети. Виртуальная машина 4 используется для финансовых и бухгалтерских приложений, другие виртуальные машины не обмениваются с ней данными. Для того чтобы правильно настроить эти четыре виртуальные машины для работы в частных виртуальных локальных сетях, нужно выполнить следующее:

1. Назначить каждой виртуальной машине параметр VLAN ID (код виртуальной сети). Для того чтобы реализовать описанный сценарий, мы настроим все виртуальные машины на использование одной и той же виртуальной локальной сети с параметром VLAN ID, равным 2. Для того чтобы назначить виртуальной машине параметр VLAN ID, можно воспользоваться одним из двух способов. Первый заключается

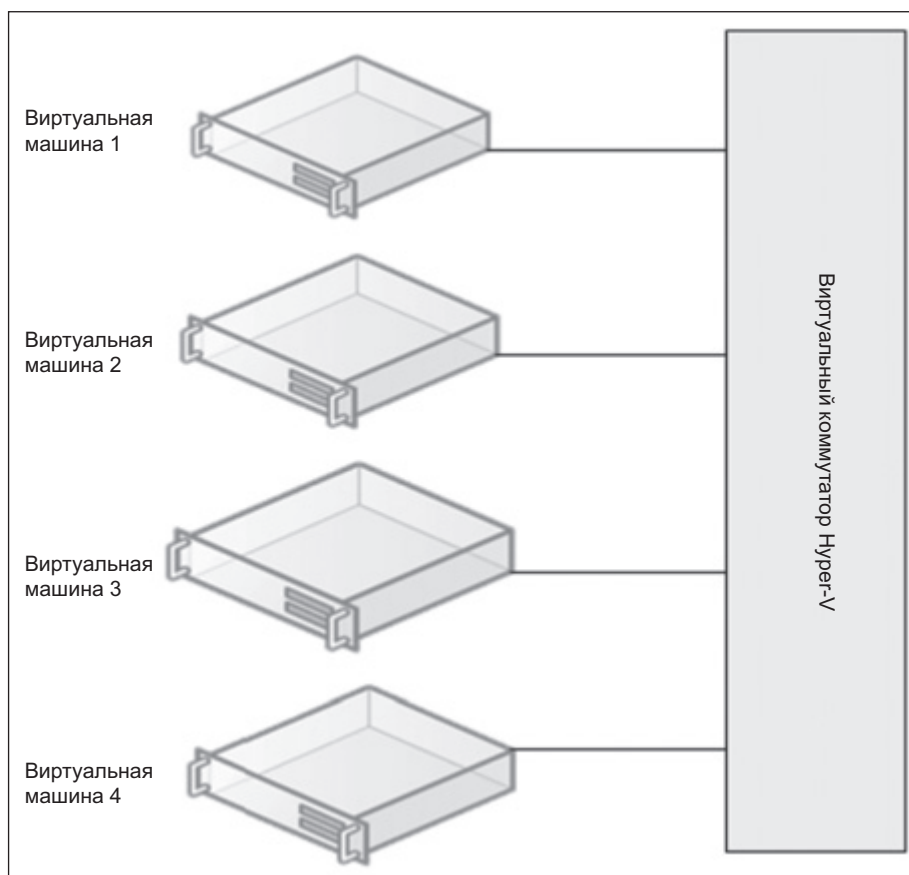


Рис. 8.28. Четыре виртуальных сервера, подключенных к виртуальному коммутатору Hyper-V

в том, чтобы зайти в окно настройки параметров виртуальной машины и разрешить идентификацию виртуальной локальной сети. По умолчанию код сети (ID) установлен в значение 2, но его можно изменить (рис. 8.29).



Параметр VLAN ID можно установить с помощью следующего командлета PowerShell:

```
Set-VMNetworkAdapterVlan -VMName <VM name> -Access -Vlan <номер  
VLAN ID>
```

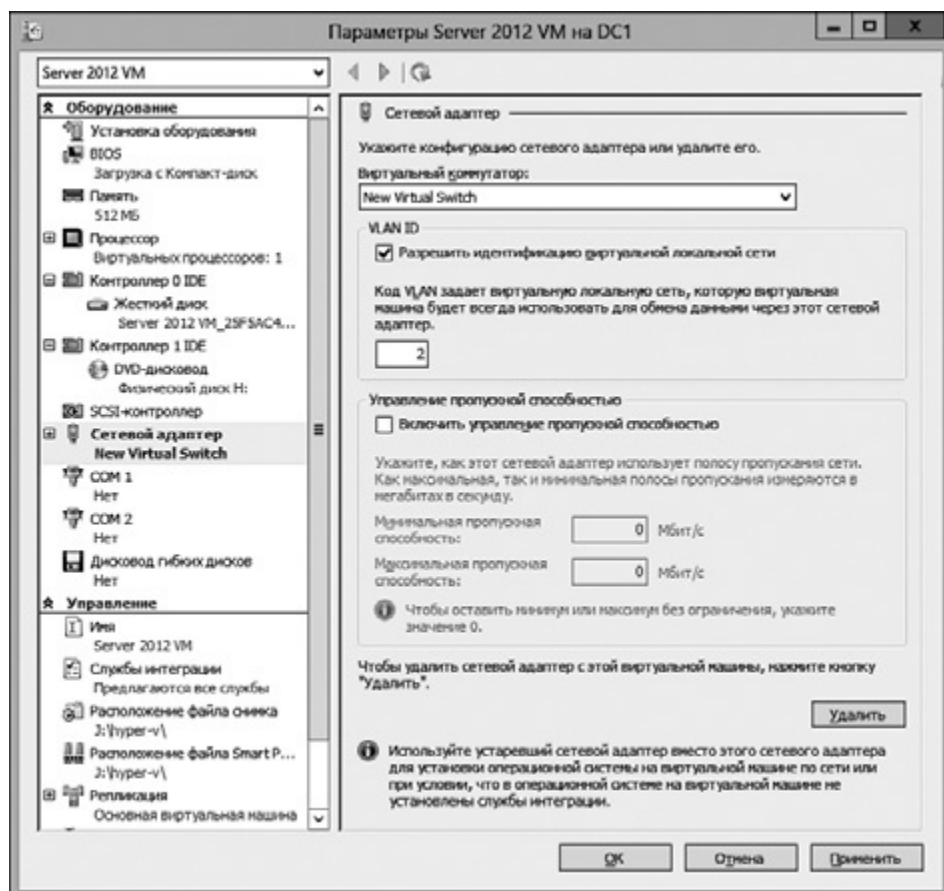


Рис. 8.29. Настройка параметра VLAN ID

2. Далее нужно назначить каждой виртуальной машине вторичный (secondary) VLAN ID, который соответствует режиму PVLAN. Частные виртуальные локальные сети поддерживают три режима работы:
 - *смешанный (Promiscuous)*. Виртуальная машина может обмениваться данными с любыми другими виртуальными машинами, в том числе с изолированными;
 - *общий (Community)*. Виртуальная машина может обмениваться данными с другими общими портами и с портами, работающими в смешанном режиме;
 - *изолированный (Isolated)*. Виртуальная машина изолирована. Трафик направляется только на смешанные порты.

Предположим, нужно, чтобы виртуальные машины 1 и 2 могли взаимодействовать друг с другом, так как в отделах продаж и маркетинга используют приложения, при работе с которыми нужно обмениваться данными. Мы установим эти виртуальные машины в **Общий (Community)** режим и дадим им вторичный VLAN ID 5. Сделать это можно, воспользовавшись следующей командой PowerShell (в примере имя виртуальной машины VM1) для каждой из виртуальных машин:

```
Set- VMNetworkAdapterVlan -VMName VM1 -Community -PrimaryVlanID 2  
-SecondaryVlanId5
```

Так как другие виртуальные машины не обмениваются данными с виртуальной машиной 4, мы настроим ее на использование **Изолированного (Isolated)** режима и поместим ее в отдельную виртуальную локальную сеть, задав ID 4:

```
Set- VMNetworkAdapterVlan -VMName VM4 -Isolated -PrimaryVlanID 2  
-SecondaryVlanId4
```

Виртуальной машине 3 нужно обмениваться данными со всеми виртуальными машинами, включая изолированную машину 4. Поэтому мы настроим ее на работу в **Смешанном (Promiscuous)** режиме, установим для нее два ID PVLAN — 4 и 5:

```
Set- VMNetworkAdapterVlan -VMName VM3 -Promiscuous -PrimaryVlanID 2  
-SecondaryVlanIdList 4-5
```

Знайте, что виртуальный коммутатор поддерживает и другие возможности, такие как частные списки контроля доступа (private accesscontrol lists, (PACLs)) и функции защиты. Они включают в себя защиту от ARP-спуфинга, перенаправления трафика с подставных DHCP-серверов. Они поддерживают зеркалирование портов и работу в магистральном (trunk) режиме, в котором возможна консолидация трафика нескольких виртуальных локальных сетей.

Выводы

Благодаря новым сетевым возможностям Windows Server 2012 предоставляет организациям инструменты, которые нужны для развертывания облачных сред. Основа облачных вычислений — виртуализация. Многие из этих новых возможностей относятся к виртуальным сетям.

Одна из наиболее значительных новых возможностей — это IPAM-сервер, который помогает IT-специалистам собрать все аспекты управления IP-адресами в единой централизованной консоли. Объединение сетевых карт — это долгожданная функция, которая позволяет системным администраторам связывать несколько сетевых адаптеров для обеспечения агрегации пропускной способности и повышения отказоустойчивости системы.

Новые возможности, обеспечивающие управления качеством обслуживания (QoS), позволяют профилировать трафик и предоставлять приоритет в полосе пропускания наиболее важным приложениям, которыми пользуется организация.

И наконец, расширяемый виртуальный коммутатор Huper-V позволяет сторонним разработчикам создавать подключаемые модули, которые способны увеличить возможности управления инфраструктурой Huper-V. Собственные свойства виртуального коммутатора позволяют выполнять те же настройки, которые характерны для аппаратных коммутаторов. Виртуальные машины можно разместить в частных виртуальных локальных сетях для целей изоляции этих виртуальных машин и управления их взаимодействием с другими системами. В виртуальный коммутатор встроены механизмы обеспечения безопасности, которые позволяют оградить виртуальные сети от различных угроз.

9

Удаленный доступ

Одна из наиболее распространенных подсистем, развертываемых в инфраструктурах, работающих под управлением Windows Server, — это подсистема удаленного доступа. Сотрудники нуждаются в механизме, который позволяет им работать в корпоративной сети даже тогда, когда они находятся вне офиса. В среде Windows удаленный доступ реализован с использованием двух технологий: RRAS (Routing and Remote Access, маршрутизация и удаленный доступ) и DirectAccess.

RRAS использовался еще со времен Windows Server 2000, он вырос из технологии RAS (Remote Access Service, служба удаленного доступа), которая позволяла подключаться к Windows NT 4.0-системам с использованием модемных соединений. RRAS не только поддерживает VPN (Virtual Private Networking, виртуальные частные сети) и модемные соединения в ОС семейства Windows Server, но и способен работать как программный маршрутизатор, реализуя службы маршрутизации в локальных и глобальных сетях, а также в Интернете.

Технология DirectAccess впервые появилась в Windows Server 2008 R2. Она предоставляла сравнительно простой способ удаленного подключения систем — членов домена, работающих под управлением Windows 7, к корпоративной сети. Также она позволяла IT-специалистам управлять подключенными с ее помощью клиентскими компьютерами, не утруждая себя настройкой

традиционных VPN. Microsoft Forefront UAG (Unified Access Gateway, шлюз унифицированного доступа) — это принадлежащий Microsoft продукт для организации VPN и обеспечения функциональности обратного прокси-сервера (reverse proxy). Он появился в 2010 году, и с его помощью можно упростить развертывание системы удаленного доступа и улучшить управление ею. С помощью DirectAccess клиенты при выходе в Интернет легко подключаются к сети организации — даже раньше, чем проходят проверку подлинности. DirectAccess предоставляет возможности VPN для клиентов, работающих под управлением Windows 7 и Windows 8. RRAS реализует технологию VPN для устаревших клиентских систем.

Унифицированный удаленный доступ

Благодаря технологии унифицированного удаленного доступа (Unified Remote Access) Server 2012 делает значительный шаг вперед в области удаленного доступа. В Server 2012 RRAS и DirectAccess собраны в одной серверной роли Удаленный доступ (Remote Access). И в DirectAccess и в RRAS, используемых в Server 2012, появилось множество улучшений. Вот наиболее значительные из них:

- Совместное существование DirectAccess и RRAS на одном сервере. Ранее из-за конфликтов систем безопасности наличие на одном и том же сервере RRAS и DirectAccess приводило к проблемам с DirectAccess-соединениями. Случалось это преимущественно по причине нестыковок в системах безопасности этих технологий. DirectAccess использовал IPv6 для установления соединения с клиентом. Это не означает, что данную возможность нельзя использовать в IPv4-сетях, так как DirectAccess задействовал технологию перехода между IPv4 и IPv6. Однако RRAS блокировал такой сетевой трафик, что приводило к проблемам функционирования DirectAccess. Также DirectAccess имел встроенные механизмы обеспечения безопасности для защиты внутренней сети от DoS-атак (denial of service, отказ в обслуживании), что приводило к проблемам при развертывании RRAS. Технология унифицированного удаленного доступа решает проблемы, которые возникают при развертывании DirectAccess и RRAS на одном сервере.
- Упрощенное развертывание благодаря новому мастеру установки и уменьшению количеству компонентов для развертывания. Одно из требований, которое было упразднено, — необходимость развертывания PKI (public key infrastructure, инфраструктура открытых ключей)

для авторизации сертификатов. Вместо этого DirectAccess использует протокол Kerberos, основанный на HTTPS. Вам необязательно вникать в тонкости работы прокси-сервера Kerberos, основанного на HTTPS, так как новый мастер установки автоматически настраивает данный метод проверки подлинности.

- Теперь не нужно разворачивать UAG для того, чтобы разрешить доступ к ресурсам в корпоративной сети, которые используют только IPv4. Встроенная система трансляции протокола IPv6 в протокол IPv4 позволяет осуществлять такой доступ.
- Улучшенное удаленное управление. Клиенты DirectAccess подключаются к корпоративной сети сразу же, как только устанавливают соединение с Интернетом. Таким образом, системные администраторы могут удаленно управлять компьютерами. Управление включает в себя установку исправлений и обновлений и применение корпоративных требований к удаленным клиентам.
- Балансировка нагрузки. В Windows Server 2012 появилась встроенная поддержка системы балансировки сетевой нагрузки Windows (Network Load Balancing, NLB). Это позволяет добиться высокого уровня доступности и масштабируемости DirectAccess и RRAS. Балансировку нагрузки можно настроить с помощью нового мастера установки.
- Поддержка системы защиты доступа к сети (Network Access Protection, NAP). NAP — это платформа, которая позволяет обеспечить соответствие клиента правилам, определенным компанией, до того, как ему будет разрешен доступ к корпоративной сети. Например, в соответствии с правилами вашей компании может требоваться, чтобы на компьютере клиента была установлена определенная версия антивируса, прежде чем он получит полный доступ к сети. С помощью NAP, интегрированного с Windows Server 2012 DirectAccess, правила NAP могут быть применены на удаленных клиентах. NAP можно настроить, воспользовавшись мастером настройки удаленного доступа.
- Систему унифицированного удаленного доступа можно развернуть на сервере, на котором установлены основные серверные компоненты. Управлять ею можно, используя PowerShell v3.
- Новая консоль управления сервера удаленного доступа предоставляет сведения о производительности системы, об активности пользователей, о ресурсах, потребляемых удаленными клиентами.
- Новые средства диагностики включают в себя запись событий в журнал и отслеживание пакетов.

- Система унифицированного удаленного доступа Windows Server 2012 предоставляет встроенные возможности создания отчетов и сбора информации, такие как статистические сведения о работе пользователей. Это возможно при использовании данной системы совместно с сервером RADIUS или внутренней базой данных Windows (Windows Internal Database, WID).

Есть несколько сценариев, при которых с использованием удаленных соединений все еще нельзя работать с IPv4-ресурсами:

- Ресурсы (например, общие папки) расположены на устаревших системах, которые не полностью поддерживают IPv6, например таких, как файловые серверы, работающие под управлением Windows Server 2003.
- В сетях, где протокол IPv6 отключен.
- IPv4-ресурсы в приложениях, которые не поддерживают IPv6.

Среди других новых и улучшенных функций можно отметить возможность развертывания DirectAccess за NAT-устройством и поддержку нескольких доменов и многосайтового развертывания.

Требования

Развертывание системы унифицированного удаленного доступа на Windows Server 2012 требует наличия сервера, подключенного к домену, развертывания роли Удаленный доступ (RemoteAccess) и наличия клиентов, работающих под управлением Windows 7 или Windows 8. По крайней мере, Microsoft заявляет именно о таких требованиях. Однако в момент написания этого материала DirectAccess демонстрирует полную функциональность только на клиентских системах с установленной ОС Windows 8 корпоративная (Enterprise) или на системах под управлением Windows Server 2012, действующих в роли клиента.

DirectAccess

Система DirectAccess предъявляет собственные требования к системе. Так, ей нужно, чтобы на брандмауэре был открыт TCP-порт 443.

Для обеспечения безопасности транспортного уровня (TLS, transport layer security) DirectAccess может использовать сертификат проверки подлинности сервера, выпущенный центром сертификации (certificate authority, CA), которому доверяют клиенты DirectAccess. Центр сертификации выпускает цифровые сертификаты. Они используются для обеспечения безопасности и удостоверяют, что открытый ключ, связанный с цифровым сертификатом, действителен для организации, для которой он выпущен. Это система публичной проверки подлинности.

Коммерческие центры сертификации берут плату за выпуск сертификатов, общедоступные центры сертификации выпускают сертификаты бесплатно. DirectAccess поддерживает сертификаты, выпущенные общедоступными центрами сертификации.



Если у организации нет сертификата, DirectAccess способен справиться с этой проблемой. Система установки DirectAccess в Windows Server 2012 настроит необходимый сертификат IP-HTTPS и KDS-прокси (key distribution center, центр распределения ключей) как самозаверяющийся сертификат.

Развертывание DirectAccess

Первый шаг в развертывании DirectAccess — это *планирование*. Определите, какие клиенты и серверы будут использовать DirectAccess. По умолчанию при установке DirectAccess создаются объекты групповой политики DirectAccess. Политики применяются к мобильным устройствам, которые входят в группу компьютеров домена Active Directory. Обычно клиенты DirectAccess — это мобильные устройства, но если речь идет о настольных компьютерах, вам нужно создать группу DirectAccess в Active Directory и добавить их туда.

В соответствии с рекомендациями устанавливайте роль **Удаленный доступ** (Remote Access) на сервере, подключенном к домену, который не имеет других ролей.

Для установки DirectAccess выполните следующее.

1. На панели мониторинга диспетчера серверов щелкните на ссылке **Добавить роли и компоненты** (Add roles and features), выберите роль **Удален-**

ный доступ (Remote Access), щелкните на кнопке **Добавить компоненты** (Add features) и кнопке **Далее** (Next).

2. Мастер установки предложит установить службы ролей **DirectAccess** и **VPN (RAS)** и **Маршрутизация (Routing Service)**. Флажок, соответствующий **DirectAccess**, установлен по умолчанию. Щелкните на кнопке **Далее** (Next) три раза, затем нажмите **Установить** (Install).



Установите роль **Маршрутизация (Routing Service)** для того, чтобы сделать компьютер, работающий под управлением Windows Server, маршрутизатором. Например, в небольших и тестовых сетях часто используют серверы, подключенные к нескольким сетям. Такой сервер может иметь две сетевые карты, которые для целей тестирования подключены к двум подсетям.

В дополнение к **DirectAccess** и **VPN** при развертывании роли **Удаленный доступ (Remote Access)** устанавливаются и следующие компоненты:

- управление групповой политикой (Group Policy Management);
- пакет администрирования диспетчера RAS-подключений (RAS Connection Manager Administration Kit (CMAK));
- средства удаленного администрирования сервера (Remote Server Administration Tools (RSAT));
- веб-сервер (IIS);
- внутренняя база данных Windows (Windows Internal Database).

После успешной установки в панели мониторинга диспетчера серверов появятся компоненты **Удаленный доступ** и **IIS** (рис. 9.1).

Настройка DirectAccess

Настроить **DirectAccess** можно, воспользовавшись новым мастером начальной настройки (Getting Started wizard). Ссылку для открытия этого мастера можно найти после установки **DirectAccess** в области уведомлений диспетчера серверов (рис. 9.2).

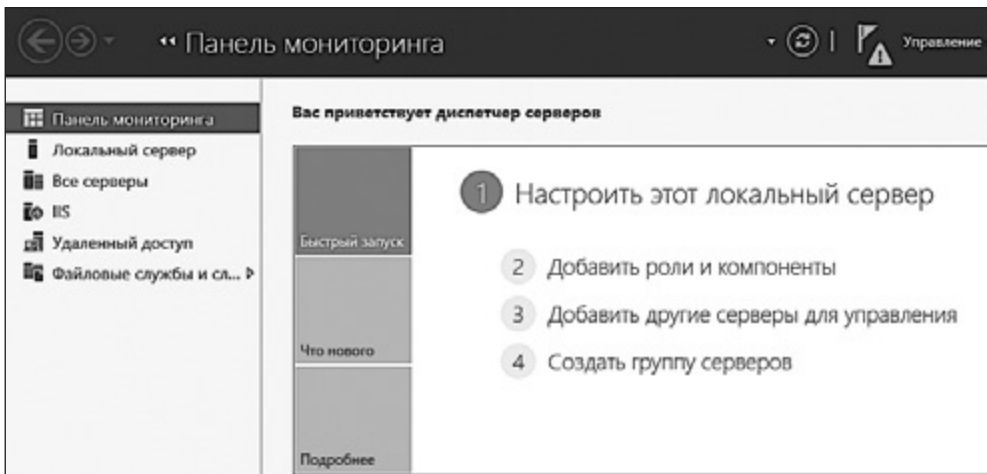


Рис. 9.1. Успешная установка Удаленного доступа и IIS

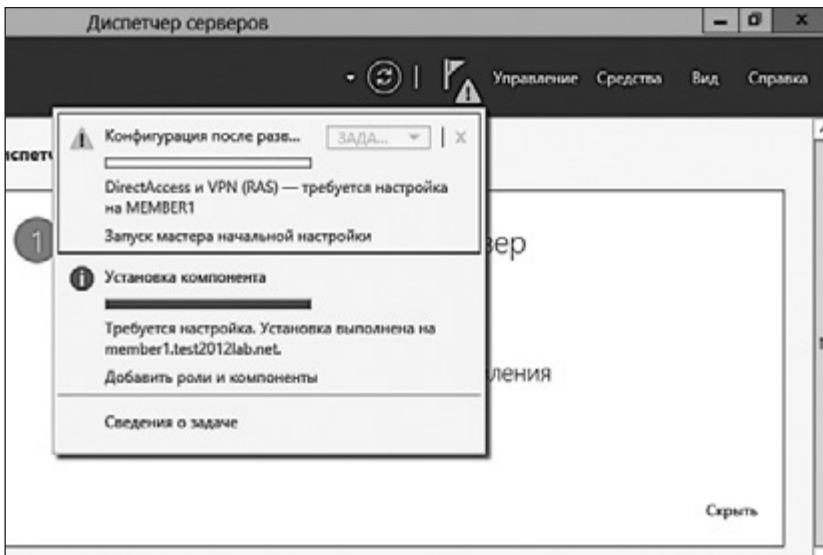


Рис. 9.2. Ссылка для запуска мастера начальной настройки

Запустить этот мастер можно также, воспользовавшись командой Управление удаленным доступом (Remote Access Management) из меню Средства (Tools) диспетчера серверов.

В мастере настройки удаленного доступа (Remote Access Setup) есть две ссылки. Первая служит для запуска мастера начальной настройки (Getting Started). Он позволяет установить DirectAccess с рекомендованными параметрами по умолчанию. Вторая ссылка, Запустить мастер настройки удаленного доступа (Run the Remote Access Setup Wizard), запускает средство, которое позволяет задать собственные параметры настройки. Вероятно, вы только начинаете осваивать работу в Windows Server 2012, поэтому можете решить воспользоваться мастером начальной настройки (Getting Started), а позже подстроить некоторые параметры самостоятельно.

Щелчок на ссылке запуска мастера начальной настройки (Getting Started) приведет к открытию окна, в котором доступны возможности установки DirectAccess и VPN, а также только DirectAccess или только VPN. Если в вашей инфраструктуре имеются различные компьютеры, для работы с которыми могут понадобиться и VPN, и DirectAccess (устаревшие Windows-клиенты, которые не поддерживаются DirectAccess, должны использовать VPN), выберите вариант развертывания DirectAccess и VPN. Если все системы в вашей инфраструктуре используют устаревшие версии Windows, выполните развертывание VPN. А в тех редких случаях, когда все системы работают под управлением Windows 8 и Windows Server 2012, достаточно будет DirectAccess. Здесь мы выберем вариант развертывания DirectAccess и VPN в соответствии с рекомендациями Microsoft.

На следующем шаге вам будет предложено указать, как развернут сервер удаленного доступа (Remote Access server). Здесь возможны три варианта. Если сервер удаленного доступа оснащен двумя сетевыми адаптерами и один из них подключен к Интернету, а второй — к внутренней сети, это означает, что сервер развернут на границе внутренней сети. При наличии такой конфигурации выберите вариант Граница (Edge). Для сервера с двумя сетевыми картами, который развернут за пограничным устройством (таким как брандмауэр), выберите вариант За пограничным устройством (Behind an edge device). И наконец, если сервер удаленного доступа подключен лишь к внутренней сети одной сетевой картой, выберите вариант За пограничным устройством (с одним сетевым адаптером) (Behind an edge device (with a single network adapter)). Введите общедоступное имя компьютера или IP-адрес, который клиентские системы будут использовать для подключения к серверу удаленного доступа.

На данном этапе установки вы можете настроить дополнительные параметры, в том числе параметры групповой политики, группы Active Directory, параметры сетевого адаптера, свойства DNS. Например, вы можете решить развернуть DirectAccess не для всех пользователей домена, как установлено

по умолчанию, а только для сотрудников отдела продаж, которые постоянно в разъездах. Все это можно настроить в разделе дополнительных параметров.

Если вам не нужно выполнять дополнительные настройки, нажмите кнопку Готово (Finish).

Об успешной установке и настройке можно судить по зеленым значкам рядом с компонентами на экране Состояние операций (Operations Status) консоли управления удаленным доступом (Remote Access Management Console), которую можно открыть из диспетчера серверов (рис. 9.3).

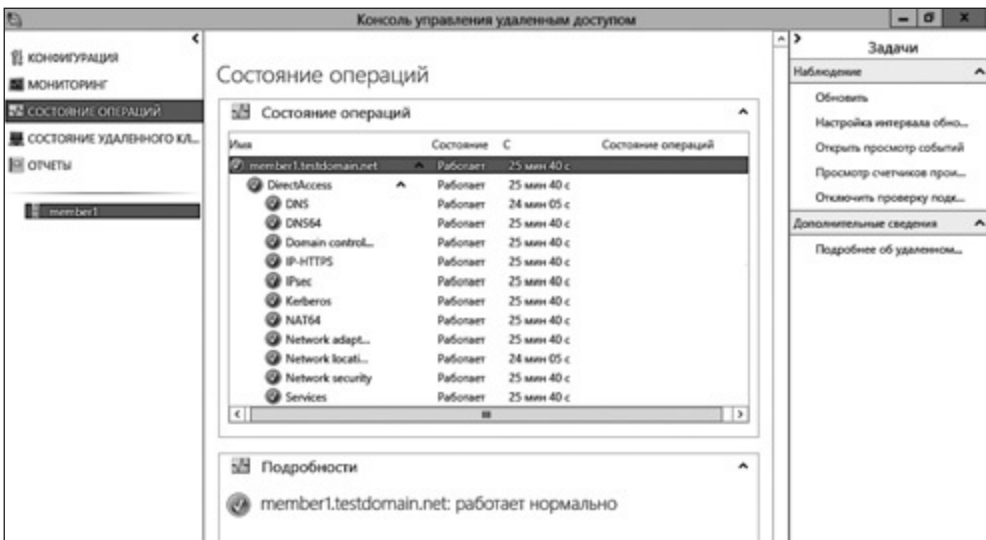


Рис. 9.3. Просмотр состояния DirectAccess в консоли управления удаленным доступом после установки

Если вы видите около компонента знак вопроса или сообщение об ошибке, то можете просмотреть и отредактировать настройки DirectAccess, воспользовавшись командой Конфигурация (Configuration) в консоли управления удаленным доступом (Remote Access Management Console).

В консоли можно просмотреть графическое руководство, показывающее шаги, которые необходимо выполнить для настройки удаленного доступа (рис. 9.4).

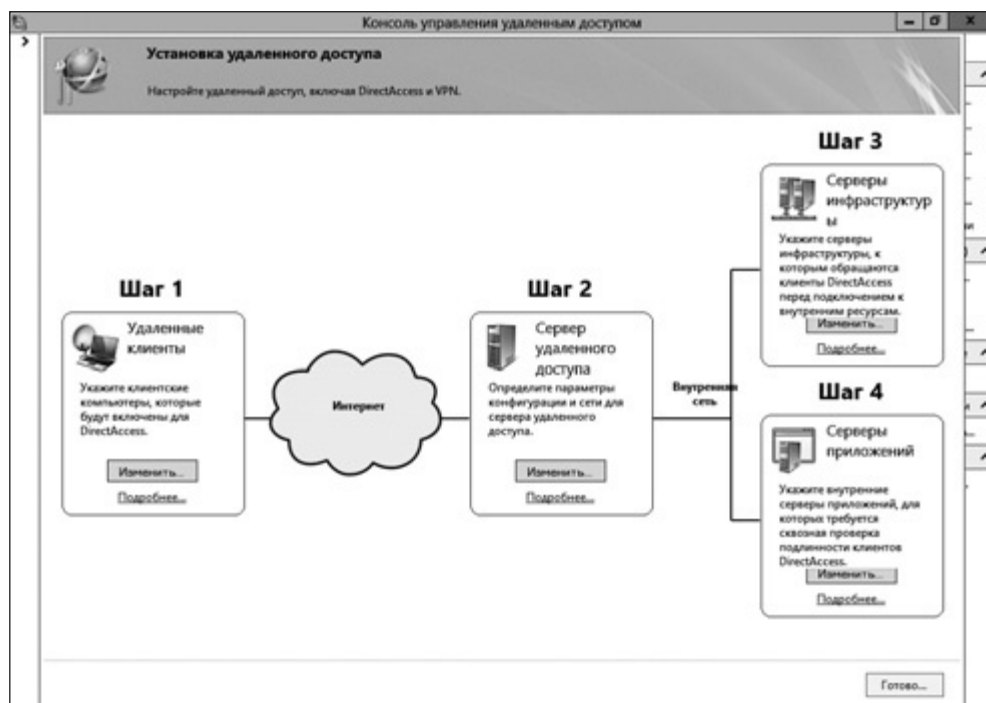


Рис. 9.4. Этапы настройки удаленного доступа

Далее вы можете подключить к корпоративной сети мобильных клиентов, использующих DirectAccess, и присоединить любые настольные системы, в которых применяется DirectAccess, к группе DirectAccess, которую создали в Active Directory.

Для того чтобы проверить подготовку клиентов к работе с DirectAccess, можете использовать несколько командлетов, которые исполняются на стороне клиента:

- **Get-DNSClientNrptPolicy.** Позволяет вывести для DirectAccess таблицу NRPT (Name Resolution Policy Table, таблица политики разрешения имен). Это хороший способ проверки того, что мастер начальной настройки создал верные DNS-записи для DirectAccess и сервера сетевого расположения (Network Location Server);
- **Get-NCSPolicyConfiguration.** Выводит настройки подключения клиентов DirectAccess, включая URL-адрес расположения домена организации (выводится как *DomainLocationDeterminationURL*), который

клиенты используют, находясь за пределами корпоративной сети. Когда вы настраиваете DirectAccess, этот URL должен соответствовать следующей структуре: *https://DirectAccess-NLS.domainname*.

- Для того чтобы проверить подключение клиентов, используйте команду **Get-DAConnectionStatus**. Он сообщит о том, подключен клиент локально или удаленно. С помощью DirectAccess клиенты могут получить доступ к ресурсам корпоративной сети независимо от способа подключения.

Вместо использования мастера начальной настройки можете настроить DirectAccess вручную. Может показаться, что DirectAccess проще развернуть с помощью мастера, однако вы можете использовать методику ручной настройки параметров для того, чтобы в ходе решения проблем, которые могут возникнуть после автоматической установки, проверить настройки, выполненные мастером.

Ручная настройка

Ручную настройку DirectAccess можно выполнить, воспользовавшись разделом Конфигурация (Configuration) в консоли управления удаленным доступом (Remote Access Management console). Этот процесс включает в себя четыре основных этапа:

1. Выбор сценария развертывания. Средство управления удаленным доступом предоставляет два варианта развертывания DirectAccess. Первый заключается в выполнении полного развертывания для клиентов и развертывания удаленных средств управления. Это сценарий, который, весьма вероятно, реализуют большинство организаций. Он не только позволяет выполнить развертывание DirectAccess для клиентов, организовав их подключение к корпоративной сети, но и дает администратору возможность удаленно управлять клиентами, подключенными к Интернету. Вторым вариантом является управление только клиентами, подключенными к Интернету. Для того чтобы продемонстрировать полный набор возможностей DirectAccess, установим DirectAccess для подключения клиентов и удаленного управления ими, то есть в первом из упомянутых вариантов (рис. 9.5).

Теперь выберем группы компьютеров, с которыми нужно работать с использованием DirectAccess. Именно здесь можно указать группу DirectAccess для настольных компьютеров в дополнение к группе Компьютеры домена (Domain Computers), заданной по умолчанию. Если вы

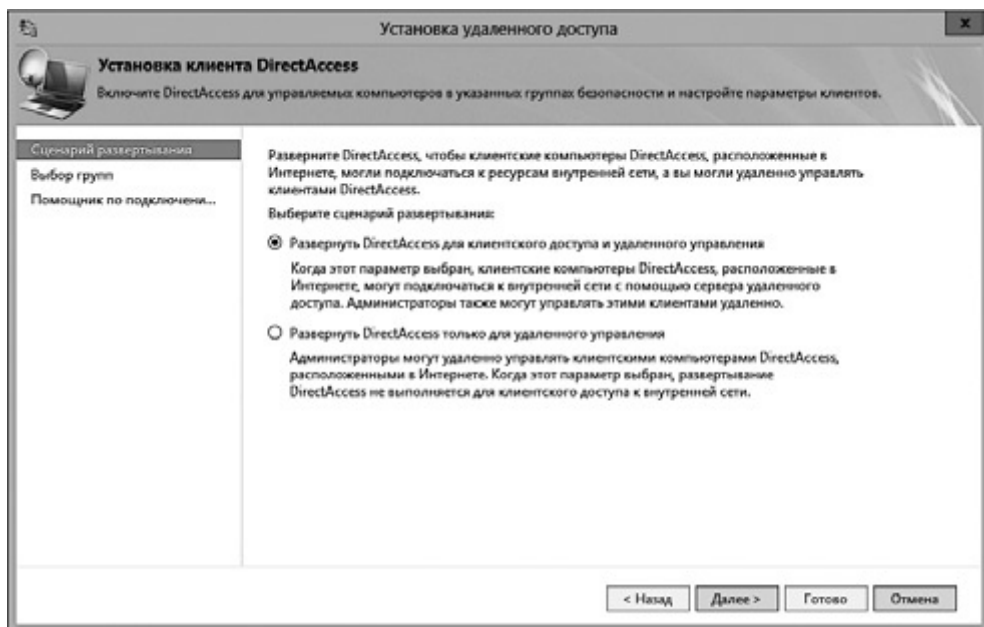


Рис. 9.5. Выбор сценария развертывания DirectAccess

планируете использовать DirectAccess на настольных компьютерах, не забудьте снять флажок **Разрешить DirectAccess только для мобильных компьютеров** (Enable DirectAccess for mobile computers only).

Кроме того, на данном экране вы можете указать использование принудительного туннелирования (рис. 9.6). Используйте эту возможность, чтобы организовать подключение клиентских компьютеров через Интернет с использованием веб-прокси-сервера.

На следующем экране можно задать URL ресурса, используя который клиенты будут подключаться к внутренней сети. На этих клиентах будет работать помощник по подключению к сети (Network Connectivity Assistant, NCA), который позволяет получать сведения о подключении клиента к сети, диагностическую информацию и данные о поддержке. Дополнительные параметры на данной странице позволяют настроить адрес электронной почты, по которому клиенты могут направлять запросы в службу поддержки. Здесь есть также поле для ввода названия DirectAccess-соединения. Клиентским системам можно позволить пользоваться локальным разрешением имен для подключения.

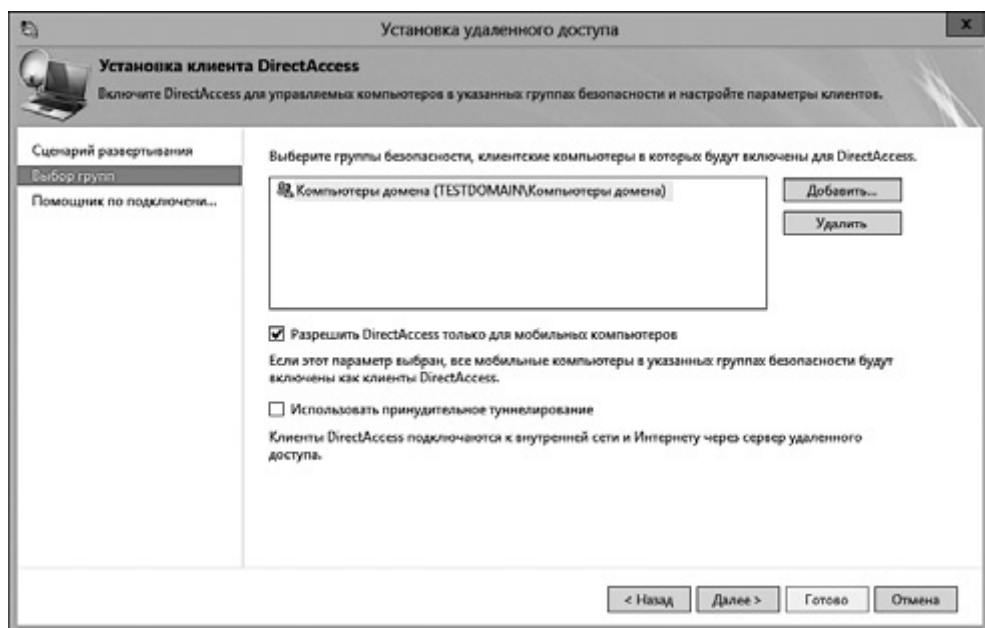


Рис. 9.6. Настройка параметров групп DirectAccess

2. Настройка сервера удаленного доступа. Мы выполнили настройки данного этапа ранее, при развертывании DirectAccess. Знайте, однако, что вы можете развернуть систему удаленного доступа, не настраивая DirectAccess, и вернуться к этому шагу позднее.
3. Указание серверов, к которым клиенты DirectAccess должны получать доступ перед подключением к ресурсам в корпоративной сети. Например, администратор может решить, что DirectAccess-клиенты должны подключаться к серверу сетевых расположений. Этот сервер используется клиентами для подтверждения их подключения к корпоративной сети, он может упростить управление подключениями и решение проблем с ними, особенно в тех случаях, когда речь идет о большом количестве клиентов. Здесь вы, кроме того, можете указать DNS-серверы, которыми должны пользоваться подключенные DirectAccess-клиенты, и серверы, которые могут использоваться для обновления удаленных клиентов или управления ими.
4. Настройка серверов приложений. Здесь вы можете настроить модель проверки подлинности «узел — узел» для DirectAccess-клиентов, которые подключаются к серверам приложений. Это полезно, если нужно

предоставить клиентам доступ к серверам, которые содержат конфиденциальные данные, требующие повышенного уровня безопасности.

Учтите, что хотя в Server 2012 процесс развертывания DirectAccess довольно прост (за счет того, что процессы установки и настройки практически полностью автоматизированы), для успешного развертывания системы нужна правильная настройка DNS и системы IP-адресов. Поэтому, прежде чем развертывать DirectAccess, убедитесь, что ваши DNS-серверы функционируют правильно.

BranchCache

Технология унифицированного удаленного доступа позволяет организовывать подключения типа «сеть — сеть». Многие организации и деловые сообщества имеют территориально удаленные друг от друга и от центрального офиса филиалы. Вы можете настроить системы RRAS и DirectAccess в Windows Server 2012 для создания VPN типа «сеть — сеть». Скорость соединения сетей во многом зависит от типа WAN-сети, которая используется для связи сетей офисов. Например, канал связи типа T1 обладает фиксированной полосой пропускания 1,5 Мбит/с, но комбинация линий связи типа T1 и линий, использующих для построения Ethernet-соединений медный кабель (Ethernet-over-Copper), позволяет достичь большей пропускной способности.

Однако, если даже канал связи между сетями обладает достаточной пропускной способностью, в подобной инфраструктуре все еще возможно возникновение проблем, вызванных задержками сигнала, ограничениями, связанными с производительностью системы и синхронизацией файлов. BranchCache — это компонент, который впервые появился в Server 2008 R2. Он призван решить проблемы производительности, вызванные интенсивным обменом данными между сетями. С помощью BranchCache данные основной сети кэшируются в удаленной сети, поэтому пользователи этой сети работают с данными локально, вместо того чтобы обращаться к ним посредством WAN-сети.

Улучшения BranchCache, которые появились в Windows Server 2012, включают в себя возможность развертывания в сети нескольких серверов кэширования, а также управление BranchCache с помощью PowerShell и инструментария управления Windows (Windows Management Instrumentation, WMI).

Кроме того, теперь развертывание данной системы упростилось, так как сейчас не нужно создавать отдельные объекты групповой политики для каждой

сети. Все, что нужно, — это один общий объект групповой политики. Клиенты, которые подключаются к серверам BranchCache, автоматически настраиваются в качестве клиентов кэша, в результате чего настройка со стороны клиента становится предельно простой. В системе BranchCache есть улучшения, касающиеся шифрования данных. Теперь не требуется использовать PKI-сертификаты или другие дополнительные технологии шифрования.

Новые возможности BranchCache поддерживаются не только серверами, работающими под управлением Windows Server 2012, и Windows 8-клиентами, но и ОС Server 2008 R2. Таким образом, вы в основной сети можете развернуть BranchCache на сервере, работающем под управлением Server 2012, и связать его с компьютером, на котором установлена ОС Server 2008 R2. К BranchCache-серверам, развернутым на Windows Server 2012, могут подключаться и Windows 7-клиенты, если на них установлены сертификаты, поддерживающие TLS. Серверы с ОС Server 2008 R2 и Windows 7-клиенты не могут воспользоваться возможностями хэширования данных и возможностями, относящимися к разбиению файлов на фрагменты, доступными в Server 2012. Эти функции предназначены для оптимизации репликации данных между сетями.

Требования

BranchCache можно использовать для обеспечения работы удаленных клиентов с данными веб-серверов, файловых серверов и серверов приложений.

- Для использования BranchCache с веб-серверами требуется настройка IIS с использованием HTTP или HTTPS.
- Работа с файловыми серверами с помощью BranchCache требует наличия развернутых ролей **Файловые службы (File Service)** и службы BranchCache для сетевых файлов (BranchCache for Network File Services).
- Серверы приложений, которые планируется использовать с BranchCache, нуждаются в установке службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service, BITS) и службы BranchCache. Например, сервер приложений, на котором работают службы обновления Windows (Update Services), может использоваться в сценарии, предусматривающем применение BranchCache для того, чтобы системы в удаленных сетях могли получать с него обновления Windows.

Интеграция групповой политики с BranchCache и использование автоматического обнаружения хранимого кэша требуют наличия Active Directory-домена, но домен не нужен для отдельных компьютеров, использующих BranchCache. Для настройки автоматического обнаружения серверов, хранящих кэшированные данные, клиент и сервер должны принадлежать одному и тому же сайту Active Directory.

Развертывание BranchCache

Прежде чем начинать установку BranchCache, вы должны решить, как сделать это наилучшим образом. BranchCache поддерживает два режима установки. Если вы знакомы с BranchCache в Server 2008 R2, это значит, что вы знакомы и с его установкой, так как ее режимы остались прежними: режим распределенного кэша (distributed cache) и режим размещенного кэша (hosted cache).

Небольшим компаниям, имеющим несколько филиалов, больше подойдет режим распределенного кэша, так как для его организации требуется меньшее аппаратное обеспечение. При работе в режиме распределенного кэша сервер BranchCache расположен в главном офисе. Клиентские компьютеры филиалов получают кэшированные файлы с сервера в главном офисе.

Второй режим развертывания — это режим размещенного кэша. При его использовании в дополнение к BranchCache-серверу главного офиса в филиале разворачивают еще один сервер, на котором и размещается кэш. Клиенты пользуются его ресурсами для работы с кэшированными данными. Использование этого режима обеспечивает более высокую производительность для крупных организаций и тех организаций, которые вынуждены передавать по WAN-каналам большие объемы данных. Но он требует более значительного аппаратного и программного обеспечения, используемого в филиале.

Для развертывания системы BranchCache выполните следующее.

1. На контроллере домена откройте окно Управление групповой политикой (Group Policy Management). Перейдите к целевому домену или организационной единице (organizational unit, OU), щелкните на выбранном объекте правой кнопкой мыши и выберите из появившегося меню команду Создать объект групповой политики в этом домене и связать его (Create a GPO in this domain, and Link it here).

2. Дайте имя новому объекту групповой политики (Group Policy object, GPO) и нажмите ОК. В списке политик домена щелкните на созданном объекте правой кнопкой мыши и выберите команду Изменить (Edit) (рис. 9.7).

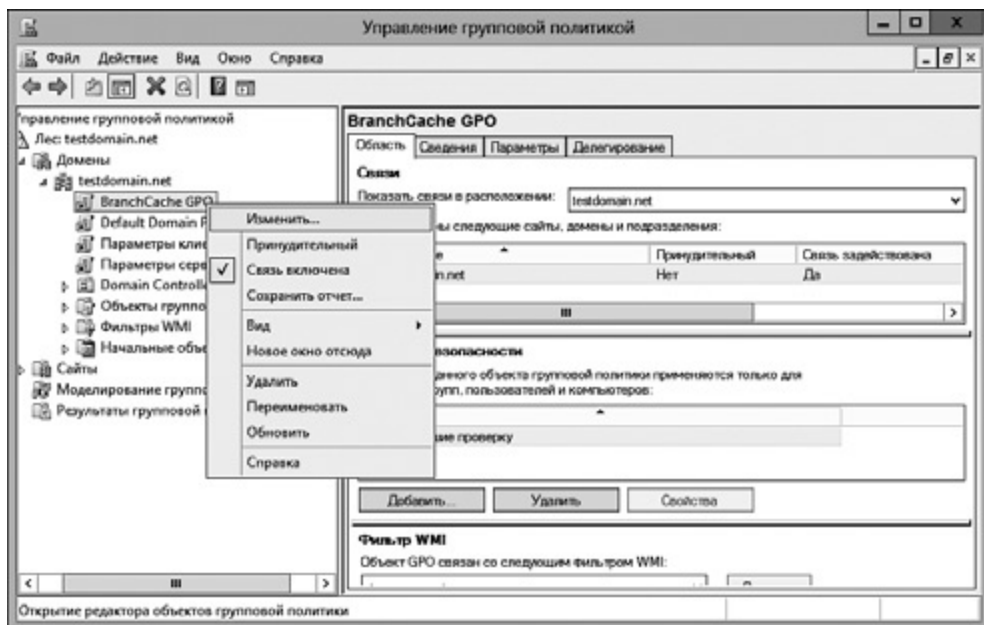


Рис. 9.7. Редактирование объекта групповой политики BranchCache

3. Теперь в окне редактирования групповой политики пройдите по пути Конфигурация компьютера ► Политики ► Административные шаблоны: получены определения политик (ADMX-файлы) с локального компьютера ► Сеть ► BranchCache (Computer Configuration ► Policies ► Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer ► Network ► BranchCache) (рис. 9.8).

В настройках объекта групповой политики BranchCache есть девять параметров. В случае первоначальной установки включите параметр Включить BranchCache (Turn on BranchCache). Для этого нужно щелкнуть на нем правой кнопкой мыши, в открывшемся меню выбрать команду для его изменения, в появившемся окне выбрать Включено (Enabled), нажать кнопку Применить (Apply) и кнопку ОК. То же самое нужно сделать для параметров Включить режим распределенного кэша BranchCache (Set BranchCache Distributed Cache mode) и Включить автоматическое обнаружение размещенного кэша по

точке размещения службы (Enable Automatic Hosted Cache Discovery Service Connection Point).

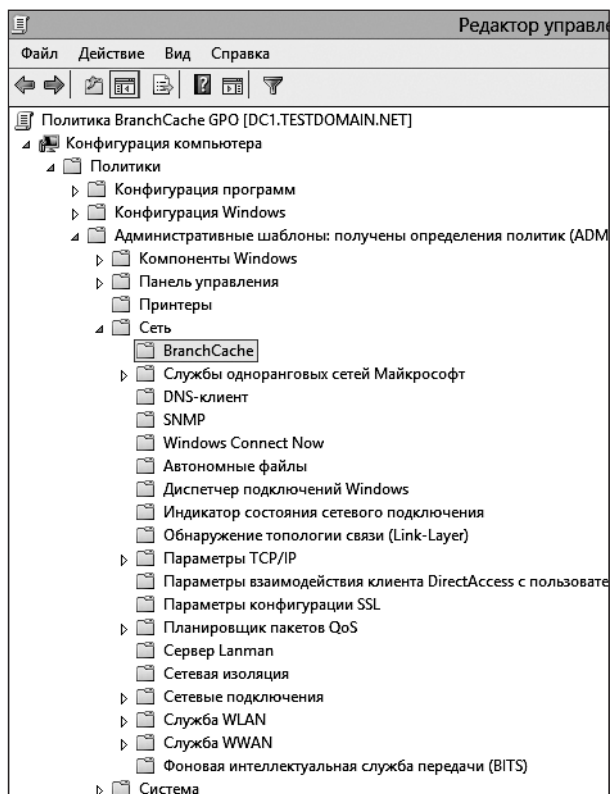


Рис. 9.8. Переход к настройкам политики BranchCache



Для BranchCache на файловых серверах включите в настройках объекта групповой политики параметр Настройка BranchCache для сетевых файлов (Configure BranchCache for network files). Для режимов с использованием размещенного кэша включите вместо параметра Включить режим распределенного кэша BranchCache (Set BranchCache Distributed Cache mode) параметр Включить режим размещенного кэша BranchCache (Set BranchCache Hosted Cache mode).

Настройка брандмауэра Windows

Для того чтобы брандмауэр Windows пропускал трафик BranchCache, он тоже нуждается в настройке. В панели управления (Control Panel) откройте раздел Система и безопасность (System and Security), затем раздел Брандмауэр Windows (Windows Firewall). В открывшемся окне нажмите кнопку Дополнительные параметры (Advanced Settings) и сделайте двойной щелчок на группе Правила для входящих подключений (Inbound Rules).

Среди правил для входящих подключений имеется автоматически созданное правило для BranchCache. Найдите правило Получение содержимого BranchCache (входящий трафик HTTP (BranchCache Content Retrieval (HTTP-In) Rule). Щелкните на этом правиле правой кнопкой мыши и выберите в появившемся меню команду Свойства (Properties). В открывшемся окне установите флажок в поле включения правила и выберите в качестве действия Разрешить подключение (Allow the connection) (рис. 9.9).

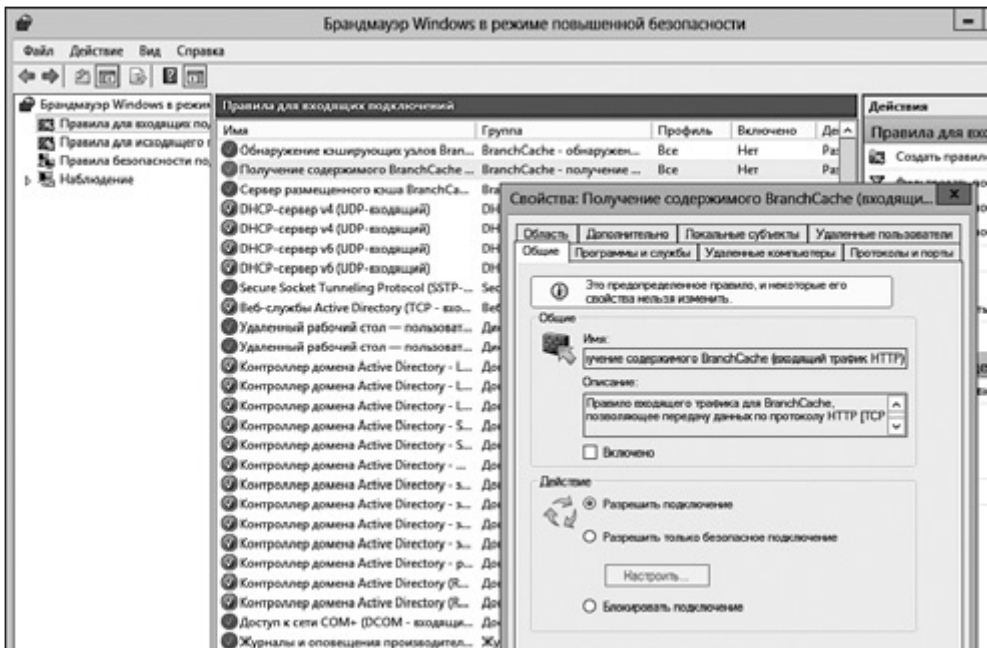


Рис. 9.9. Настройка брандмауэра Windows для работы BrandCache

Нажмите кнопку Применить (Apply), затем ОК. Сделайте то же самое для правила Обнаружение кэширующих узлов BranchCache (входящий трафик WDS) (BranchCache Peer Discovery (WDS-In)).

Развертывание роли BranchCache с помощью диспетчера серверов

Вы можете развернуть роль BranchCache так же, как и другие серверные роли, с помощью диспетчера серверов или PowerShell. Для того чтобы развернуть роль BranchCache с помощью диспетчера серверов как часть процесса развертывания системы удаленного доступа, сделайте следующее.

1. На сервере, работающем под управлением Windows Server 2012, который планируется использовать либо как сервер для размещения кэша BranchCache, либо как сервер содержимого, нажмите в диспетчере серверов ссылку **Добавить роли и компоненты** (Add Roles and Features). Три раза щелкните **Далее** (Next), для того чтобы попасть в окно **Выбор ролей сервера** (Select Server roles). Выберите здесь роль **Удаленный доступ** (Remote access) и согласитесь с добавлением необходимых компонентов. Щелкните на кнопке **Далее** (Next). В окне **Выбор компонентов** (Select Features) установите флажок напротив компонента BranchCache.
2. Нажмите **Далее** (Next). На следующем экране выберите службу **DirectAccess и VPN** (DirectAccess and VPN) для установки BranchCache. Кроме того, здесь же вы можете включить установку службы маршрутизации. Еще раз щелкните на кнопке **Далее** (Next), а затем на кнопке **Установить** (Install).

Развертывание роли BranchCache с помощью PowerShell

На компьютере, который будет играть роль сервера, поддерживающего размещенный кэш, компонент BranchCache можно установить с помощью PowerShell. Я предпочитаю пользоваться именно этим способом, так как он позволяет установить BranchCache, не развертывая при этом дополнительные службы удаленного доступа. Такой способ установки следует избрать в том случае, если вы, например, хотите развернуть BranchCache и DirectAccess или VPN на разных серверах.

Вот что нужно сделать для того, чтобы выполнить установку BranchCache с помощью PowerShell:

1. Запустить PowerShell от имени администратора.
2. Выполнить следующие командлеты:

```
Import-Module ServerManager  
Add-WindowsFeature -name BranchCache
```

Результат их успешного выполнения приведен на рис. 9.10.

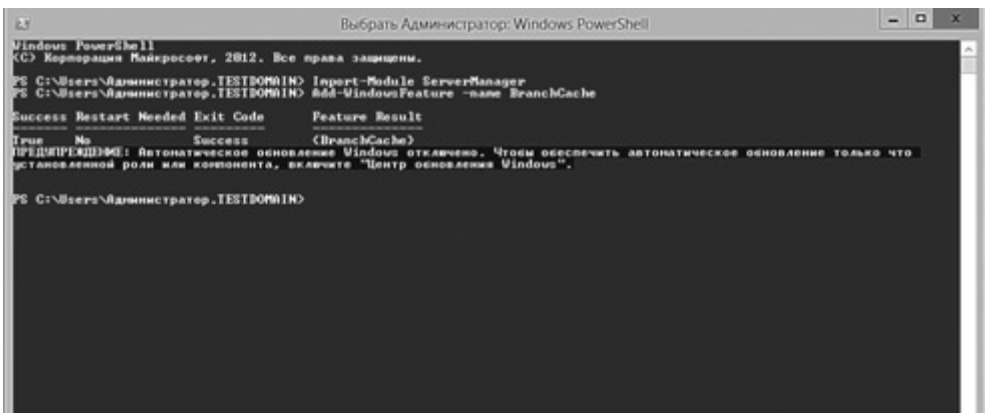


Рис. 9.10. Установка BranchCache с помощью PowerShell

На данном этапе работы PowerShell может вывести предупреждения и советы относительно установки. Например, на рис. 9.10 подобное сообщение касается включения службы обновления Windows.

1. Теперь выполните команду `Import-Module BranchCache`.
2. Если вы настраиваете сервер BranchCache в расчете на использование в режиме поддержки размещенного кэша, для включения автоматического обнаружения клиентов выполните команду `Enable-BCHosted-Server -RegisterSCP`.

После выполнения этих команд вы можете проверить состояние только что установленного BranchCache с помощью PowerShell, выполнив команду `Get-BCStatus`.

На рис. 9.11 показан результат исполнения этого командлета.

```

BranchCacheIsEnabled      : True
BranchCacheServiceStatus  : Running
BranchCacheServiceStartType : Automatic

ClientConfiguration:
    CurrentClientMode      : DistributedCache
    HostedCacheServerList   :
    HostedCacheDiscoveryEnabled : True

ContentServerConfiguration:
    ContentServerIsEnabled : True

HostedCacheServerConfiguration:
    HostedCacheServerIsEnabled : False
    ClientAuthenticationMode    : Domain
    HostedCacheScpRegistrationEnabled : False

NetworkConfiguration:
    ContentRetrievalUriReservationEnabled : True
    HostedCacheHttpUriReservationEnabled : True
    HostedCacheHttpsUriReservationEnabled : True
    ContentRetrievalFirewallRulesEnabled : True
    PeerDiscoveryFirewallRulesEnabled : True
    HostedCacheServerFirewallRulesEnabled : True
    HostedCacheClientFirewallRulesEnabled : True

HashCache:
    CacheFileDirectoryPath : C:\Windows\ServiceProfiles\NetworkService\AppData\Local\PeerDistPub
    MaxCacheSizeAsPercentageOfDiskVolume : 1
    MaxCacheSizeAsNumberOfBytes : 5242879959
    CurrentSizeOnDiskAsNumberOfBytes : 29433856
    CurrentActiveCacheSize : 0

DataCache:
    CacheFileDirectoryPath : C:\Windows\ServiceProfiles\NetworkService\AppData\Local\PeerDistRepub

```

Рис. 9.11. Просмотр сведений о состоянии BranchCache



Если вы устанавливаете сервер BranchCache на контроллер домена и этот сервер будет использоваться для поддержки размещенного кэша, контроллер домена должен быть настроен только для чтения. В противном случае командлет (Enable-BCHostedServer - RegisterSCP) сообщит об ошибке, ссылаясь на то, что работа ведется с контроллером домена для записи и он не может быть настроен как сервер для размещенного кэша.

Подготовка и тестирование клиентских подключений

После того как вы установите BranchCache либо в распределенном режиме, либо в режиме размещенного кэша, подключенные к сети клиенты должны получить обновления групповой политики, необходимые для работы с кэшем. Так как обновления групповой политики производятся с некоторой

периодичностью, вы можете принудительно запустить обновление на клиентах и проверить состояние BranchCache на клиентах, воспользовавшись PowerShell-командлетом `Get-BCStatus`. Например, на рис. 9.11 клиент настроен на подключение к BranchCache-серверу, настроенному на работу в режиме распределенного кэша.

Инфраструктура виртуальных Рабочих столов

Службы удаленных Рабочих столов (Remote Desktop Services, RDS) — это развитие служб терминалов (Terminal Services). Впервые они появились в Server 2008 R2, являясь ключевой технологией инфраструктуры виртуальных Рабочих столов (Virtual Desktop Infrastructure, VDI). В то время как технологии DirectAccess и RRAS позволяют удаленным клиентам подключаться к серверам, технология VDI нацелена на организацию рабочих мест пользователей на клиентских системах.

Microsoft внесла в VDI значительные улучшения, так как поступить иначе было просто нельзя. В соответствии с современными тенденциями сотрудники компаний, консультанты и другие конечные пользователи сетей используют персональные устройства для того, чтобы выполнять задачи, имеющие отношение к их работе. Все больше таких устройств оснащено сенсорными экранами, поэтому технология виртуальных Рабочих столов Windows обновлена для обеспечения поддержки сенсорных устройств и других гаджетов, которые могут подключаться к Windows-сетям. Технологии удаленных Рабочих столов и виртуальных Рабочих столов теперь предназначены не только для обычных ПК или ноутбуков, но и для планшетных компьютеров и смартфонов.

VDI — это технология виртуализации Рабочего стола. Хотя и та и другая технологии позволяют достичь одной и той же цели — создать экономичные Рабочие места, удаленные Рабочие столы (Remote Desktops) и инфраструктура виртуальных Рабочих столов (VDI) — это не одно и то же. Технология удаленного Рабочего стола является последней версией служб терминалов и использует удаленное подключение к серверу, который поддерживает рабочее окружение пользователя. VDI — это виртуализованная настраиваемая рабочая среда, развертывание которой напоминает создание виртуальной машины в Hyper-V. Вы можете создавать различные VDI-образы, рассчитанные на конкретные потребности конечных пользователей.

Улучшения, которые появились в Server 2012, направлены на возможность создания удобных и единообразных рабочих мест на любых устройствах,

например на тонком клиенте или планшете, работающем под управлением Windows 8. Создание подобного рабочего окружения возможно благодаря набору технологий, входящих в VDI. Hyper-V и службы удаленных Рабочих столов — это составные части VDI, но имеются и другие компоненты, которые можно использовать в Server 2012 для создания удобной пользовательской VDI-среды. В частности, это следующие компоненты.

- *UE-V*. Технология виртуализации пользовательской среды (User Experience Virtualization, UE-V) впервые появилась в бета-версии Windows Server 2012. Она позволяет пользователям синхронизировать настройки рабочей среды при работе на различных устройствах. UE-V включена в состав Microsoft Desktop Optimization Pack (MDOP, пакет Microsoft для оптимизации рабочей среды), который можно загрузить здесь: <https://www.microsoft.com/Licensing/servicecenter/default.aspx>. Будучи объединенной с технологией перенаправления папки (Folder Redirection), данная система позволяет пользователям поддерживать настройки рабочего места и приложений при работе на различных устройствах.
- *App-V 5.0*. Эта технология обеспечивает виртуализацию приложений. App-V 5.0 позволяет организовывать потоковую передачу пакетов приложений, хранить их и централизованно управлять ими.
- *Microsoft RemoteApp*. Данная технология предназначена для публикации приложений с использованием технологий удаленных Рабочих столов или Hyper-V.
- *System Center*. Хотя рассказ о данном продукте выходит за рамки этой книги, вы должны знать, что имеется возможность организовать дополнительное управление VDI с использованием диспетчера виртуальных машин (Virtual Machine Manager, VMM) System Center 2012. Задачи по управлению VMM включают в себя мониторинг состояния и производительности VDI-окружения и создание отчетов. Кроме того, System Center расширяет возможности управления в Server 2012, например, при работе с Hyper-V.

Быстрое развертывание (Quick Deploy) — это новый способ установки VDI. IT-специалисты могут управлять сеансами связи и виртуальными машинами из одной консоли. Технологии интеллектуальной установки исправлений и сканирования позволяют добиться того, что исправления не будут развертываться на всех клиентах одновременно, так как это может негативно сказаться на производительности. Благодаря Server 2012 у технологии VDI появляется высокий уровень масштабируемости, ее производительность улучшена благодаря системе FairShare. Это нечто вроде системы балансировки нагрузки

для VDI, которая отвечает за равномерное распределение полосы пропускания сети между виртуальными машинами и пользователями.

Перед развертыванием VDI очень важно решить, как именно это будет сделано. В частности, существует три сценария развертывания.

- *Session (сеансы)*. При развертывании среды VDI, основанной на сеансах (session), вы устанавливаете операционную систему виртуального сервера и позволяете некоторому количеству пользователей работать с этой операционной системой. Преимущества развертывания, основанного на сеансах, заключаются в том, что конечные пользователи работают с одной стандартной средой VDI. Подобный подход хорош тогда, когда вы хотите подготовить экономичную Рабочую среду для пользователей, которым достаточно ограниченных возможностей настройки рабочего места. Кроме того, средой VDI, основанной на сеансах, легче управлять, так как администратору приходится заботиться лишь об одном экземпляре операционной системы. Обратной стороной такого сценария является использование серверной операционной системы. Это означает, что у некоторых приложений возможны проблемы с совместимостью. Приложения, спроектированные для работы на клиентских компьютерах, могут попросту не установиться в серверной ОС.
- *Pooled VM (пулы виртуальных машин)*. Используя виртуальные машины, объединенные в пулы, вы можете назначить одну виртуальную машину множеству пользователей. Это хороший выбор, если, например, в вашей организации имеются группы пользователей, которым нужны одинаковые рабочие места. Возможно, вы развернете одну виртуальную Рабочую среду для сотрудников службы работы с клиентами, а другую — для сотрудников отдела продаж. Преимущества такого подхода заключаются в уменьшении количества образов виртуальных машин, которыми нужно управлять, что позволяет экономить дисковое пространство. Виртуальная машина, с которой работает пользователь, представляет собой клиентскую операционную систему. Поэтому при таком подходе меньше вероятность возникновения проблем с совместимостью приложений, которые нужно установить на клиентскую ОС. Кроме того, доступно больше возможностей для настройки виртуальных машин, объединенных в пул. Возвращаясь к нашему примеру: рабочая среда, предназначенная для сотрудников службы работы с клиентами, может быть настроена не так, как среда для сотрудников отдела продаж.

Минус этого подхода заключается в том, что вам придется поддерживать большее количество образов виртуальных машин, чем при сценарии развертывания VDI, основанном на сеансах. Кроме того, поскольку

с виртуальным рабочим местом могут работать множество пользователей, у отдельно взятых пользователей не всегда будут одинаковые рабочие места.

- *Personal VM (персональные виртуальные машины).* Сценарий развертывания персональных виртуальных машин позволяет создавать рабочие места, настроенные с учетом потребностей каждого пользователя. Настройки системы передаются на каждое устройство, с которым работает пользователь. Минус этого подхода заключается в том, что чем больше персональных виртуальных машин используется в вашей организации, тем больше дискового пространства понадобится для их хранения.

Службы удаленных Рабочих столов (RDS)

Пользовательский интерфейс в стиле Windows 8 не ограничен лишь интерфейсом Server 2012, он встроен в интерфейс нового клиента службы удаленных Рабочих столов (Remote Desktop). Как и интерфейс Windows 8, он поддерживает работу с сенсорными экранами. Эта возможность, конечно, предлагается для того, чтобы удовлетворить растущую потребность сотрудников в использовании для работы их персональных мобильных устройств.

Как и в большинстве компонентов Windows Server, в службе удаленных Рабочих столов имеются некоторые улучшения. Так, теперь легче задействовать режим единого входа (single sign-on). Если все клиенты поддерживают протокол удаленного Рабочего стола (Remote Desktop Protocol, RDP) версии 8 и если пользователь работает с приложениями RemoteApp, которые опубликованы посредством службы веб-доступа к удаленным Рабочим столам (Remote Desktop Web Access, RD Web Access), в Windows Server 2012 и VDI виртуальных машин Windows 8 автоматически включается режим единого входа.

Режим единого входа можно включить для пользователей, подписанных на службу RemoteApp и подключение к Рабочему столу. И наконец, при добавлении роли Шлюз удаленного Рабочего стола (Remote Desktop Gateway, RD Gateway) режим единого входа через Интернет поддерживается по умолчанию.

Удаленный Рабочий стол теперь поддерживает список избранного (Favorities), который хранит записи обо всех RDP-соединениях. Клиентский интерфейс, основанный на вкладках, поддерживает одновременную работу с несколькими сеансами.

Технология RemoteFX используется для обеспечения поддержки мультимедийных и графических возможностей, таких как потоковая передача видео на

удаленные рабочие места. В Server 2012 благодаря RemoteFX можно выводить и трехмерную графику с использованием поддерживающей DirectX 11 видеокарты, установленной на хост-сервере Hyper-V. Кроме того, использование RemoteFX в сеансе работы с удаленным Рабочим столом позволяет организовать перенаправление USB-устройств и взаимодействие с сенсорными дисплеями, способными реагировать на несколько точек касания.

Установка служб удаленного Рабочего стола

В этом примере мы развернем службы удаленного Рабочего стола на основе сеансов. Здесь также показан пример публикации удаленного приложения.

Для целей развертывания нам понадобятся четыре сервера. Это контроллер домена, два сервера, на которых установлены службы ролей Узел сеансов удаленных Рабочих столов (Remote Desktop Session Host), а также сервер, на котором развернуты следующие службы ролей: Посредник подключений к удаленному Рабочему столу (Remote Desktop Connection Broker), Сервер удаленного управления Рабочими столами (Remote Desktop Management server), Веб-доступ к удаленным Рабочим столам (Remote Desktop Web Access). На контроллере домена развернуты службы DNS и DHCP, кроме того, он настроен в качестве корневого центра сертификации (Enterprise Root Certificate Authority).

Роль Узел сеансов удаленных Рабочих столов (Remote Desktop Session Host) используется для размещения приложений Windows или Рабочих столов Windows, предназначенных для клиентов удаленных Рабочих столов. Клиенты подключаются к Узлу сеансов удаленных Рабочих столов (Remote Desktop Session Host) и могут удаленно выполнять те же действия, которые выполняются локально, например запускать приложения, сохранять файлы и работать с серверными ресурсами.

Для настройки Узла сеансов удаленных Рабочих столов (Remote Desktop Session Host) выполните следующие действия.

1. В диспетчере серверов воспользуйтесь ссылкой **Добавить роли и компоненты** (Add Roles and Features). В качестве типа установки выберите **Установка ролей или компонентов** (Role-based or feature-based installation). Два раза щелкните на кнопке **Далее** (Next), для того чтобы добраться до окна **Выбор ролей сервера** (Select Server roles). Выберите здесь роль **Службы удаленных Рабочих столов** (Remote Desktop Services) и щелкните на кнопке **Далее** (Next) на следующих трех экранах.

- В окне Выбор служб ролей (Select role services) выберите службу ролей Узел сеансов удаленных Рабочих столов (Remote Desktop Session Host) (рис. 9.12).

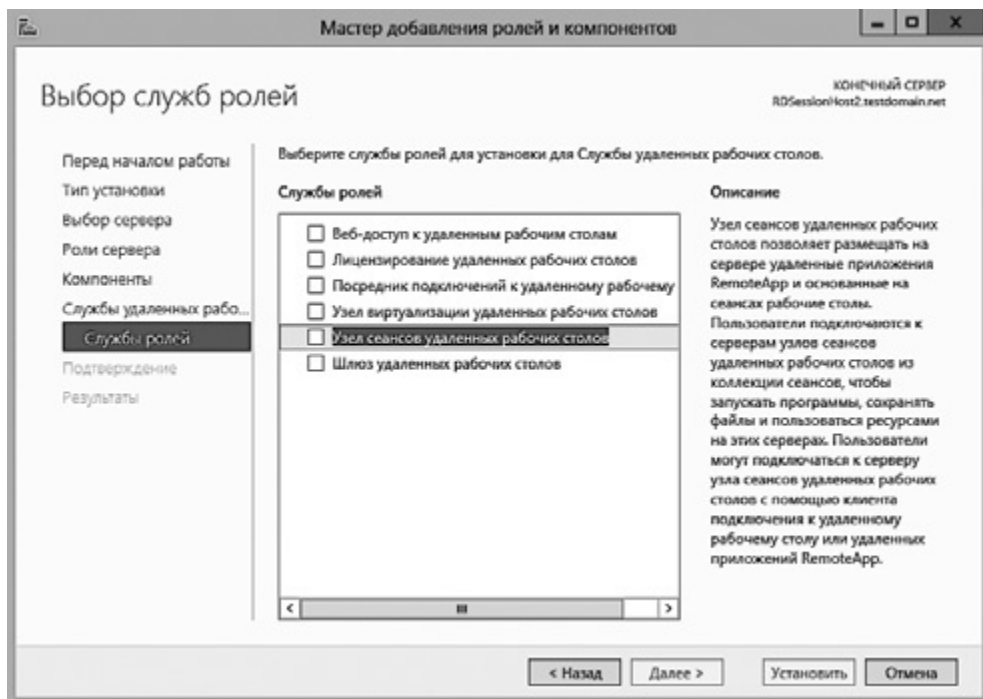


Рис. 9.12. Установка службы ролей Узел сеансов удаленных Рабочих столов

- Согласитесь с установкой предлагаемого набора дополнительных компонентов и щелкните на кнопках **Далее** (Next) и **Установить** (Install).

Для настройки сервера, обладающего ролями Посредник подключений к удаленному Рабочему столу (Remote Desktop Connection Broker) и Веб-доступ к удаленным Рабочим столам (Remote Desktop Web Access server), выполните ту же последовательность действий, только выберите соответствующие службы ролей в окне для их выбора.

Для установки сервера управления удаленными Рабочими столами (RD Management server) и служб удаленных Рабочих столов (RD Services) выполните следующие действия на сервере, на котором установлена роль Посредник подключений к удаленному Рабочему столу (Remote Desktop Connection Broker).

1. В диспетчере серверов воспользуйтесь ссылкой **Добавить роли и компоненты** (Add Roles and Features), щелкните на кнопке **Далее** (Next) и выберите **Установка служб удаленных Рабочих столов** (Remote Desktop Services Installation), снова щелкните на кнопке **Далее** (Next).

В окне **Выбор типа развертывания** (Select Deployment Type) системой будет автоматически определен посредник подключений (Connection Broker) (рис. 9.13).



Посредник подключений не должен располагаться на том же сервере, где развернуты сервер управления удаленными Рабочими столами (RD Management server) и службы удаленных Рабочих столов (RD Services). Этот сервер должен быть установлен лишь на компьютере, подключенном к домену.

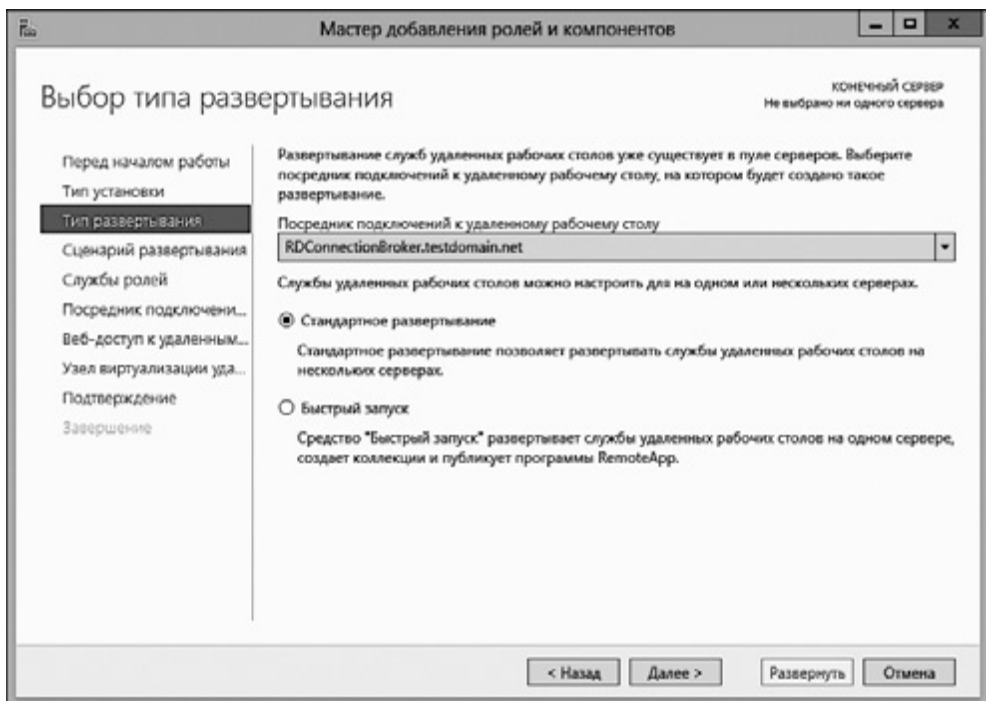


Рис. 9.13. Выбор типа развертывания



Обратите внимание на то, что на рис. 9.13 нужно сделать выбор между Стандартным развертыванием (Standard deployment) и Быстрым стартом (Quick Start). Выбор типа развертывания Быстрый старт позволяет осуществить автоматическую установку всех служб удаленных Рабочих столов на одном сервере. Данный вариант лучше всего использовать при тестовом развертывании RDS.

2. Выберите здесь параметр Стандартное развертывание (Standard deployment), его использование подойдет для большинства сценариев установки. Щелкните Далее (Next). В окне Выбор сценария развертывания (Select deployment scenario) есть возможность выбрать сценарий, основанный на использовании виртуальных машин, либо сценарий развертывания Рабочих столов на основе сеансов. В этом примере воспользуемся сценарием развертывания Рабочих столов на основе сеансов (рис. 9.14).

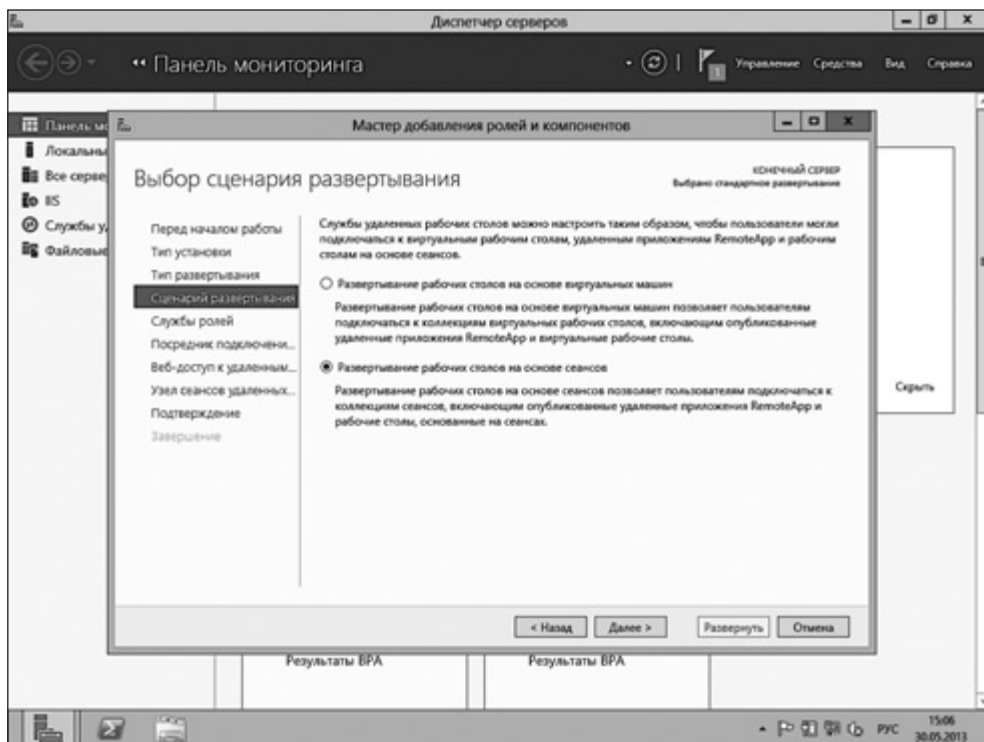


Рис. 9.14. Выбор сценария развертывания Рабочих столов на основе сеансов

3. Так как роль Посредник подключений к удаленному Рабочему столу (Remote Desktop Connection Broker) уже установлена, в процессе установки будет обнаружено, что сервер-посредник уже существует и все, что вам остается сделать, — щелкнуть на кнопке **Далее (Next)** (рис. 9.15).

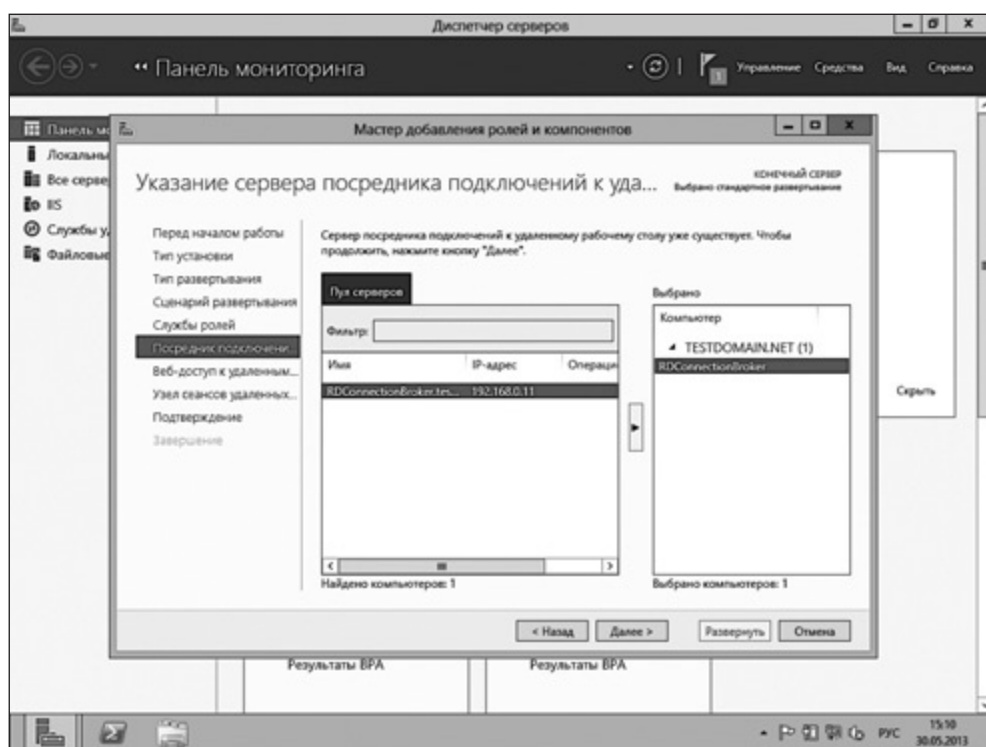


Рис. 9.15. Указание посредника подключений к удаленному Рабочему столу

4. Установите службу роли Веб-доступ к удаленным Рабочим столам (Remote Desktop Web Access server) на сервер с установленной ролью Посредник подключений к удаленному Рабочему столу (Remote Desktop Connection Broker) (рис. 9.16).
5. Щелкните на кнопке **Далее (Next)**, в окне **Указание серверов узлов сеансов удаленных Рабочих столов (Specify RD Session role)** укажите серверы, на которых должна быть развернута служба роли узла сеансов удаленных Рабочих столов. Щелкните на кнопке **Далее (Next)** и завершите установку.

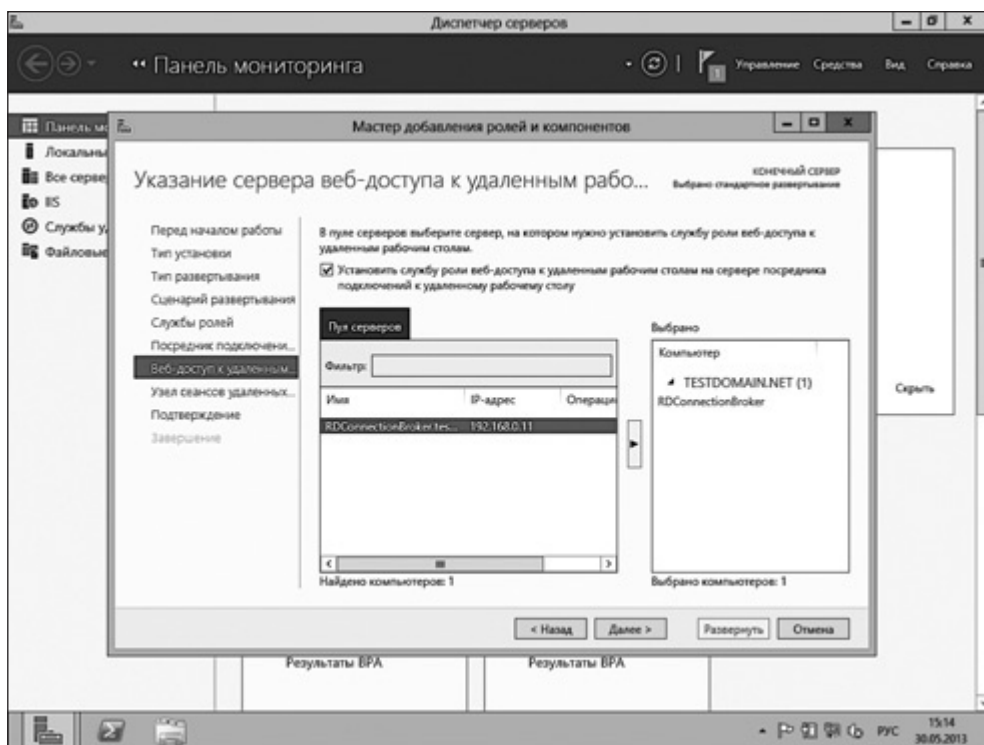


Рис. 9.16. Установка службы веб-доступа к удаленным Рабочим столам

Управление службами удаленных Рабочих столов

После развертывания вы можете воспользоваться консолью управления службами удаленных Рабочих столов в диспетчере серверов компьютера, на котором установлена роль Посредник подключений к удаленному Рабочему столу (Remote Desktop Connection Broker) (рис. 9.17).

Здесь можно создать коллекцию сеанса (session collection) — описание набора приложений, которое можно передать пользователям. Пользователям или группам пользователей Active Directory, которым нужен доступ к этим приложениям, разрешается доступ к данной коллекции. Для того чтобы создать коллекцию, в RDS-окружении должен присутствовать сервер узла сеансов удаленных Рабочих столов (RD Session Host server), который не добавлен в коллекцию.

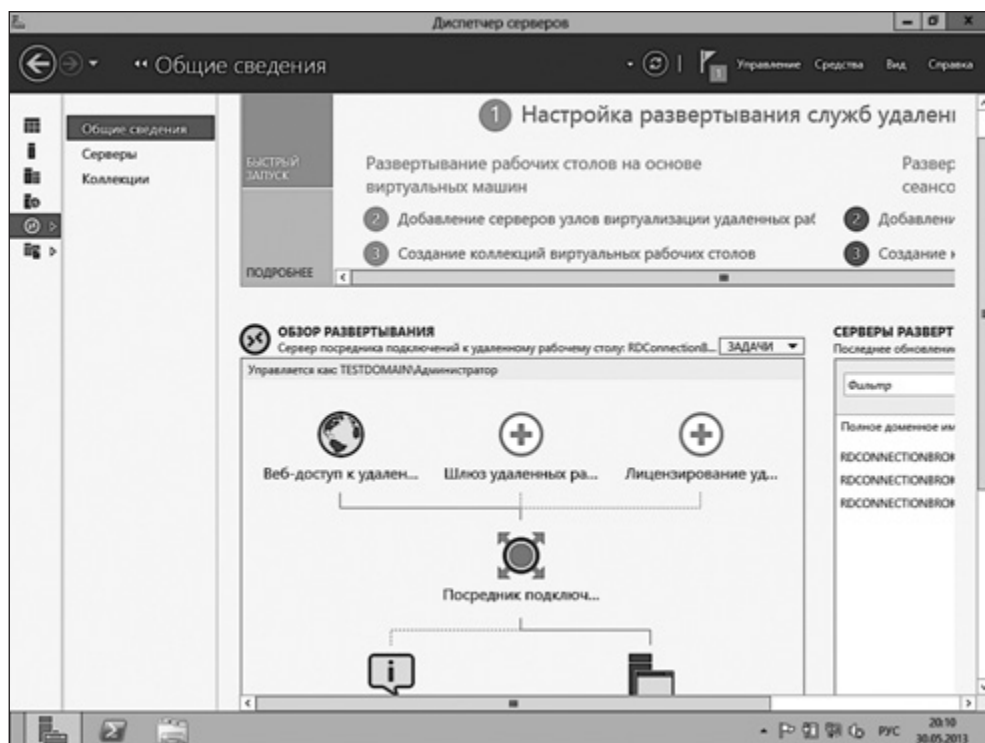


Рис. 9.17. Консоль управления службами удаленных Рабочих столов

Для того чтобы создать коллекцию, выполните следующие действия.

1. В окне настройки служб удаленных Рабочих столов (Remote Desktop Services) диспетчера серверов нажмите ссылку **Создание коллекций сеансов** (Create session collection) (рис. 9.18).
2. Будет запущен мастер создания коллекции (Create Collection wizard). Задайте имя коллекции и, если хотите, добавьте ее описание (рис. 9.19).
3. Выберите сервер узла сеансов удаленных Рабочих столов (RD Host Session server), который нужно добавить в коллекцию. Щелкните на кнопке **Далее** (Next) и добавьте пользователей или группы Active Directory, которым должен быть разрешен доступ к коллекции (по умолчанию здесь присутствует группа **Пользователи домена** (Domain Users)).
4. Щелкните на кнопке **Далее** (Next). Вы можете подключить диски профилей пользователей, тогда пользовательские настройки и данные будут храниться в центральном хранилище.

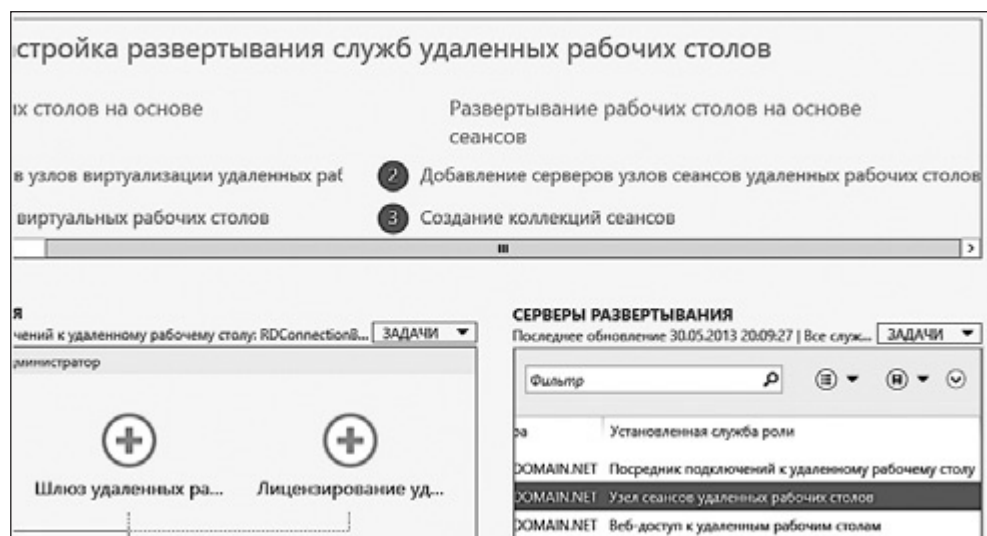


Рис. 9.18. Создание коллекции сеанса

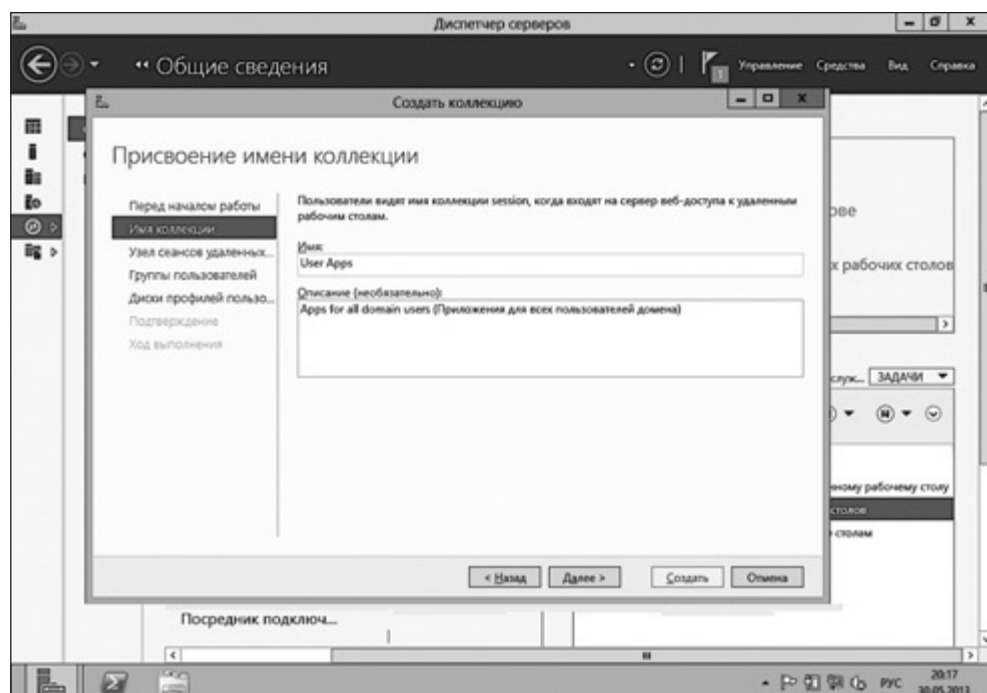


Рис. 9.19. Указание имени коллекции

- Щелкните на кнопке **Далее (Next)**, а затем на кнопке **Создать (Create)**. После создания новая коллекция сеансов будет видна в группе **Коллекции (Collections)** в левом меню окна **Службы удаленных Рабочих столов (Remote Desktop Services)**.

Привязка приложений к коллекции и публикация удаленных приложений

После того как коллекция создана, в нее можно добавлять приложения, к которым пользователям нужен удаленный доступ, и публиковать эти приложения. Для того чтобы это сделать, выполните следующее.

- В диспетчере серверов сервера, который является посредником подключений (**Connection Broker**), откройте окно **Службы удаленных Рабочих столов (Remote Desktop Services)**, затем перейдите в группу **Коллекции (Collection)** и щелкните на коллекции, которая только что была создана. На рис. 9.20 показана выделенная коллекция **User Apps**.

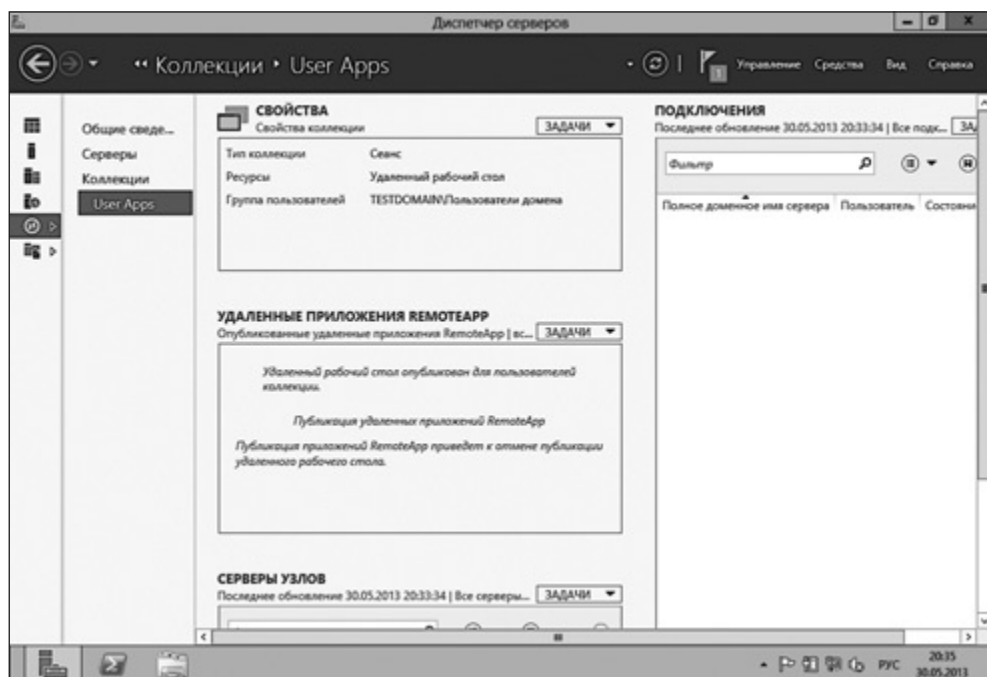


Рис. 9.20. Новая коллекция сеанса

2. Для того чтобы выбрать приложения для публикации, нажмите ссылку Публикация удаленных приложений RemoteApp (Publish RemoteApp programs) в разделе Удаленные приложения RemoteApp (RemoteApp Programs). В коллекцию можно добавлять и приложения, которые не перечислены в списке, используя кнопку Добавить (Add).
3. Выберите приложения для публикации в коллекции (рис. 9.21).

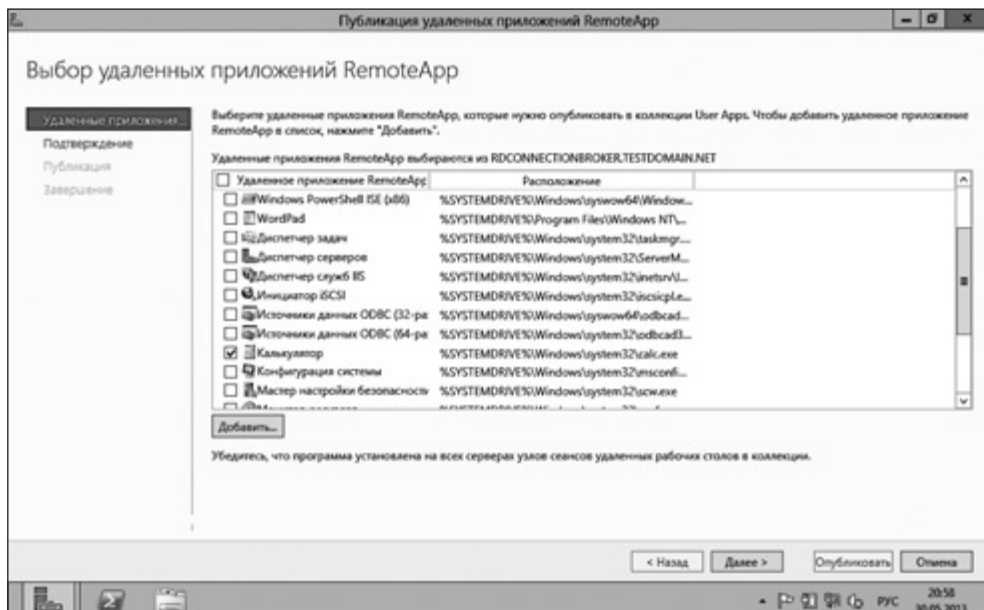


Рис. 9.21. Выбор удаленных приложений RemoteApp

4. Щелкните на кнопке Далее (Next). Подтвердите правильность выбора приложений и щелкните на кнопке Опубликовать (Publish).

Добавление опубликованных приложений в веб-папку удаленного Рабочего стола

Вы можете добавлять приложения на сервер веб-доступа к удаленным Рабочим столам (RD Web Access server), для того чтобы клиенты могли работать с ними с использованием браузера. Эти приложения нужно добавить в веб-папку удаленного Рабочего стола (RD Web folder).

Для того чтобы добавить приложения, в диспетчере серверов сервера, который является посредником подключений (Connection Broker), выполните следующее.

1. Откройте окно Службы удаленных Рабочих столов (Remote Desktop Services), перейдите в раздел Коллекции (Collections) и выберите нужной коллекции.
2. В разделе Удаленные приложения RemoteApp (RemoteApp Programs) щелкните правой кнопкой мыши на нужном приложении и выберите в появившемся меню команду Изменить свойства (Edit Properties).
3. В окне Свойства (Properties) выводятся имя и псевдоним удаленного приложения RemoteApp, а также сведения о его расположении. Оставьте значение по умолчанию для свойства Показывать удаленное приложение RemoteApp в службе веб-доступа к удаленным Рабочим столам (Show the RemoteApp program in RD Web Access) и введите имя папки, в которой данное приложение будет отображаться на сервере веб-доступа к удаленным Рабочим столам (RD Web Access server). В данном примере мы назвали папку User Apps (рис. 9.22).
4. Нажмите кнопку Применить (Apply), затем нажмите ОК.

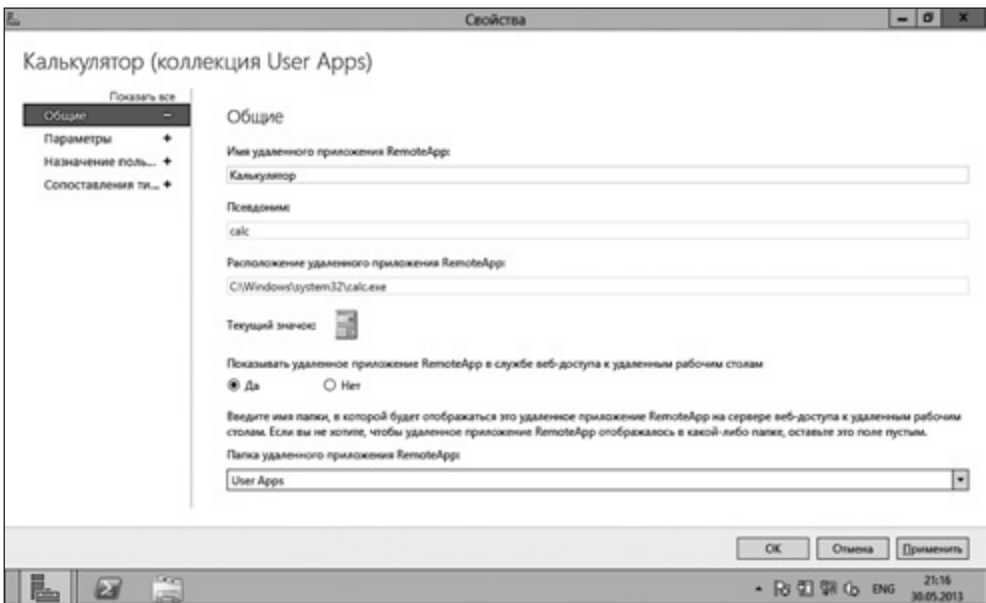


Рис. 9.22. Добавление приложения в папку сервера веб-доступа к удаленным Рабочим столам

Подключение клиентов к удаленным приложениям

После установки системы RDS и публикации приложений на сервере веб-доступа к удаленным Рабочим столам (RD Web Access server) клиенты могут получить доступ к рабочим ресурсам, введя в веб-браузере URL следующего формата: *https://<имя сервера-посредника RD>.<domain name>/RDWeb* (рис. 9.23).

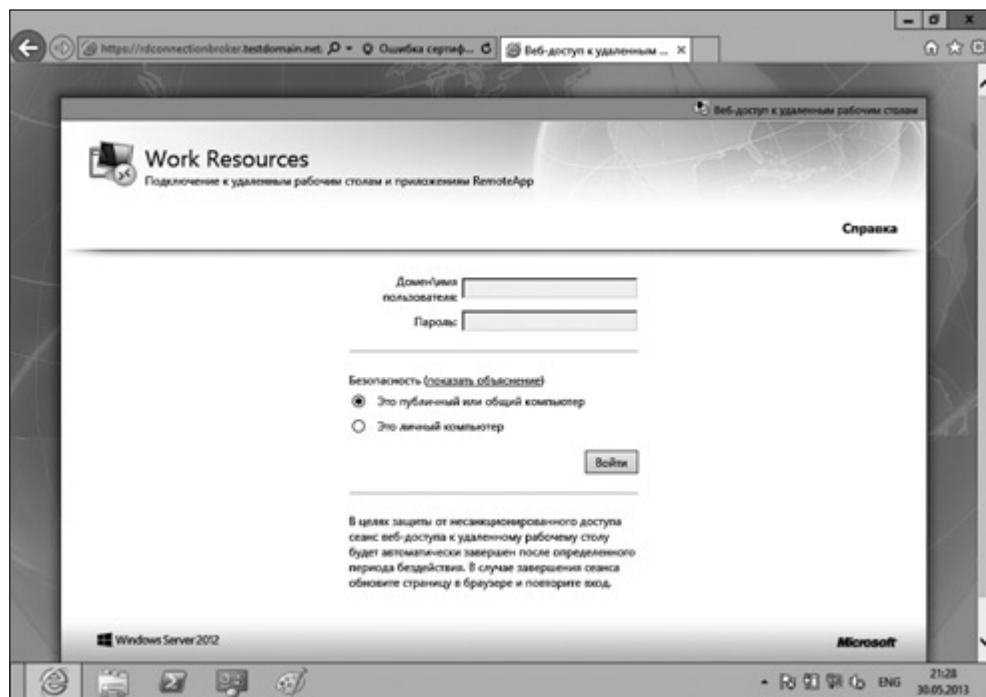


Рис. 9.23. Клиентский интерфейс для подключения к опубликованным приложениям

На рис. 9.24 показана папка, содержащая опубликованные приложения, которые готовы к удаленной работе.

Установка RemoteFX

Для того чтобы вы смогли добавить мультимедийные возможности удаленным Рабочим столам, RemoteFX требуется видеокарта, поддерживающая

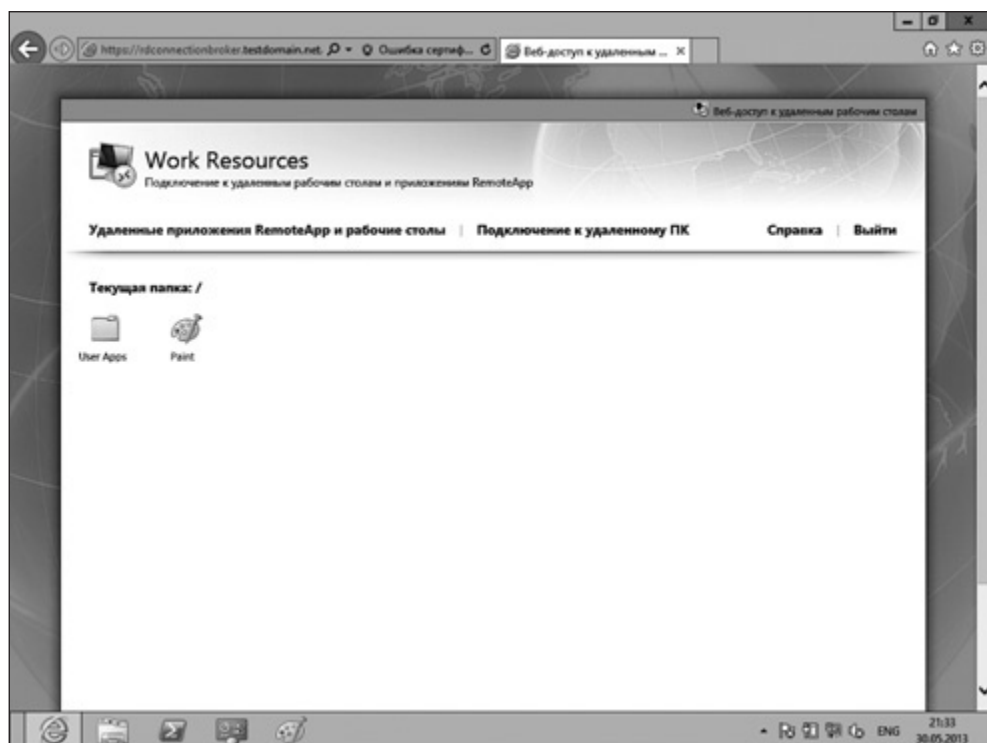


Рис. 9.24. Клиент получил возможность работать с удаленными приложениями

DirectX 11, такая как карта от AMD серии FirePro, установленная на сервере RemoteFX.

На клиентах RemoteFX требуется наличие процессора, который поддерживает технологию SLAT (second-level address translation, трансляция адресов второго уровня). В применении к серверам с процессорами от AMD эту технологию называют EPT (extended page tables), в применении к серверам с процессорами от Intel — NPT (nested page tables).

Установить RemoteFX можно, развернув роль Виртуализация удаленных Рабочих столов (Remote Desktop Virtualization). В нашем примере установка производится на том же сервере, который служит посредником подключений к удаленным Рабочим столам (RD Connection Broker).

1. В диспетчере серверов нажмите ссылку **Добавить роли и компоненты** (Add roles and features). На экране выбора типа установки выберите

Установка служб удаленных Рабочих столов (Remote Desktop Services Installation), щелкните на кнопке **Далее** (Next).

2. Выберите **Стандартное развертывание** (Standard Deployment), щелкните на кнопке **Далее** (Next) и в окне **Выбор сценария развертывания** (Select deployment scenario) установите переключатель в значение **Развертывание Рабочих столов на основе виртуальных машин** (Virtual machine-based desktop deployment). Щелкайте на кнопке **Далее** (Next) до тех пор, пока не доберетесь до окна **Указание сервера узла виртуализации удаленных Рабочих столов** (Specify RD Virtualization Host server). Укажите здесь сервер, который нужно сделать узлом виртуализации удаленных Рабочих столов, щелкните на кнопке **Далее** (Next) и на кнопке **Развернуть** (Deploy).
3. Кроме того, RemoteFX нужно включить в Hyper-V. В окне настроек Hyper-V выберите физическую видеокарту для использования с RemoteFX и установите флажок **Использовать этот графический процессор с RemoteFX** (Use this GPU with RemoteFX).

Выводы

Server 2012 поддерживает возможность подключения клиентов, находящихся в корпоративной сети и за ее пределами, к сетевым ресурсам с помощью технологии унифицированного удаленного доступа (Unified Remote Access). Для организации подключения внешних клиентов и удаленных сетей к сетям главных офисов применяются такие технологии, как DirectAccess, RRAS, VPN и BranchCache. Все они являются частями технологии унифицированного удаленного доступа.

Для подготовки удаленных Рабочих столов, сеансов удаленных Рабочих столов и предоставления доступа к удаленным приложениям можно использовать службы удаленных Рабочих столов (Remote Desktop Services), которые включают в себя множество новых компонентов и возможностей. Все это позволяет предоставить пользователям удаленные рабочие места, уровень оснащения которых превосходит все, что ранее было реализовано в ОС семейства Windows Server. Это достигнуто во многом благодаря обновленной технологии RemoteFX, возможности легко публиковать веб-приложения и упрощению развертывания VDI-окружения удаленных Рабочих столов.

10

Решение проблем, безопасность и мониторинг

После довольно длительного тестирования Windows Server 2012 я очень хорошо поняла две вещи. Во-первых, это наиболее развитый серверный продукт от Microsoft, а во-вторых, о его зрелости можно будет говорить после выхода первого пакета обновлений. Например, у меня не возникло проблем с драйверами, причем не только тогда, когда я устанавливала простой внешний USB-диск, но даже при добавлении в систему современной видеокарты, для которой были доступны лишь драйверы, рассчитанные на Windows 7.

Кроме того, Windows Server 2012 вызывает ощущение и самой рационально устроенной серверной операционной системы от Microsoft. Она быстро устанавливается как в варианте основных серверных компонентов, так и в варианте сервера с графическим интерфейсом. А если принять во внимание производительность системы, можно сказать, позаимствовав любимое выражение Microsoft, что Server 2012 — это «быстрая и динамичная» ОС.

Тем не менее существуют некоторые проблемы, требующие внимания. Я обнаружила, что некоторые службы медленно загружаются при перезапуске, а некоторые из них остаются в приостановленном состоянии до тех пор, пока не будут запущены принудительно. В окне просмотра событий периодически появляются необъяснимые ошибки, например, одна неприятная ошибка Netlogon, которая указывала на проблемы с DNS. С DNS-сервером все было нормально, и эта ошибка исчезла после очередной перезагрузки.

Конечно, с ростом числа пользователей и системных администраторов, работающих с системой, и увеличением количества организаций, где развертывается Windows Server 2012, проявятся и другие ошибки. Многие из этих проблем будут характерны для конкретного аппаратного обеспечения или каких-либо уникальных конфигураций, которые могут существовать в различных сетевых инфраструктурах. Мы постоянно сталкиваемся с этим в работе с новыми операционными системами, впервые представленными ИТ-сообществу. Такая операционная система напоминает свежий хлеб, который вытащили из печи слегка непропеченным. Все дело в том, что разработчикам, инженерам и менеджерам практически невозможно спрогнозировать детали каждого из возможных сценариев развертывания Windows Server 2012.

То, что невозможно добиться такого невероятного уровня прогнозирования, и приводит к необходимости оснащения Server 2012 множеством инструментов диагностики, которые помогают находить и исправлять неполадки, отслеживать состояние сервера. И Server 2012 оснащен инструментами, которые помогают узнать, что в системе работает не так, как должно. Он обладает компонентами, которые могут предупредить вас о потенциальных проблемах.

В Server 2012 центральный инструмент управления сервером и решения проблем — это диспетчер серверов. Что касается меня, обновленный диспетчер серверов обладает одним из лучших, если не лучшим, пользовательским интерфейсом среди продуктов, вышедших из Редмонда. Я говорю это с некоторой иронией, так как Microsoft рекомендует использовать вариант установки сервера без графического интерфейса и применять PowerShell для выполнения действий, которые можно выполнить с помощью диспетчера серверов. Рискую навлечь на себя гнев приверженцев PowerShell, я продолжаю утверждать, что многие администраторы решат пользоваться графическим интерфейсом диспетчера серверов. Особенно те из них, кто выполняет множество различных обязанностей в небольших организациях, где ИТ-персонала не очень много, а обязанностей достаточно.

Диспетчер серверов

С первого взгляда можно заметить, что диспетчер серверов теперь оснащен новым интерфейсом, который основан на плитках и вполне соответствует современному внешнему виду Windows 8. Но более глубокие изменения, касающиеся внутренних механизмов, заметить не так просто. Как и диспетчер сервера Windows Server 2008 R2, новый диспетчер серверов позволяет решать различные административные задачи, такие как добавление ролей, запуск анализатора соответствия рекомендациям (Best Practices Analyzer)

и проверка журнала событий (Event Viewer). Диспетчер сервера, который появился в Server 2008, предоставлял возможность единообразного управления серверами, то есть управления множеством серверов и конфигурационных параметров из единой консоли.

Однако теперь у обновленного диспетчера серверов есть новые возможности, которые делают его более совершенным инструментом управления, чем его коллега из Server 2008 R2. Для начинающих хочется отметить, что процесс добавления сервера в новом диспетчере серверов отличается от той же операции в его предыдущей версии.

Добавление сервера

В Server 2008 R2 добавить в диспетчер сервера другой сервер можно было, щелкнув правой кнопкой мыши на имени сервера и выбрав в появившемся меню команду Подключиться к другому компьютеру (Connect to Another Computer) (рис. 10.1).

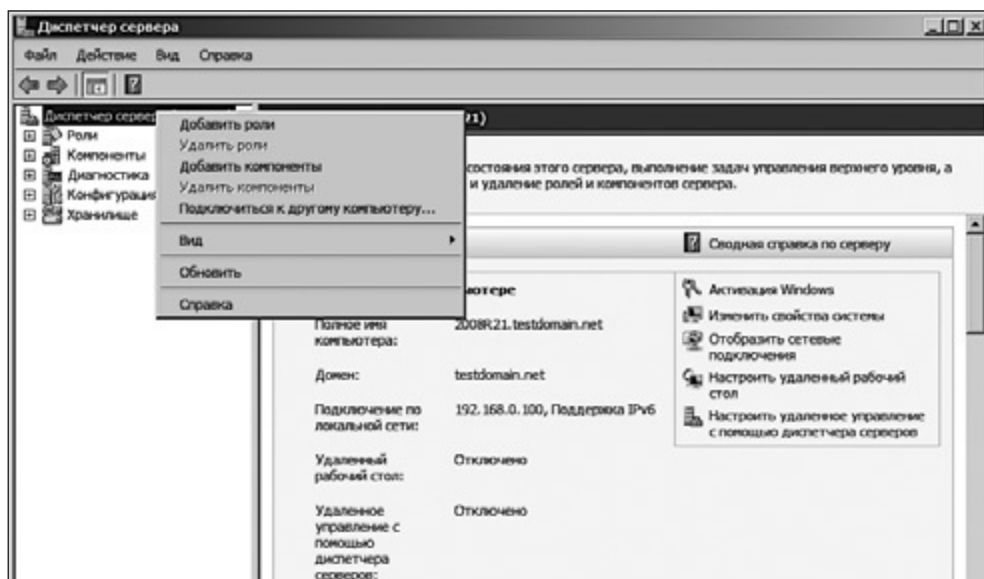


Рис. 10.1. Подключение к удаленным серверам в Server 2008 R2

В диспетчере серверов Server 2012 к другому серверу можно подключиться прямо из панели мониторинга, щелкнув на ссылке **Добавить другие серверы**

для управления (Add other servers to manage) в разделе Настроить этот локальный сервер (Configure this local server) (рис. 10.2).

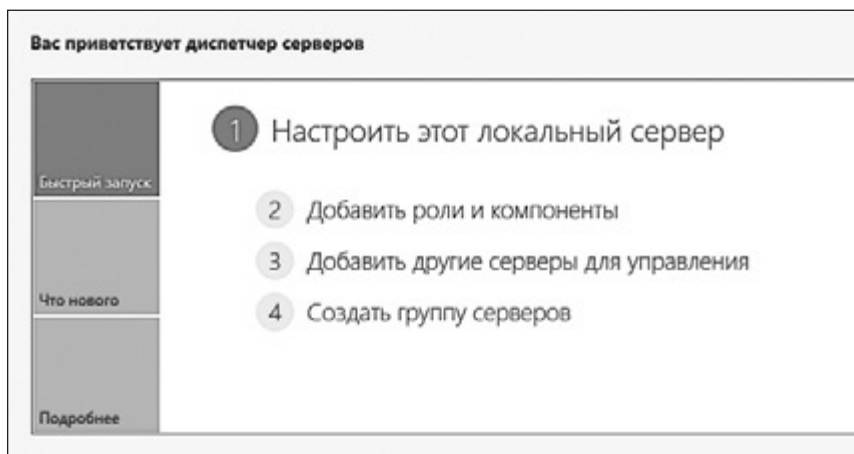


Рис. 10.2. Ссылка добавления серверов для управления в Server 2012

На рис. 10.3 показано, как я добавила в диспетчер серверов развернутый на виртуальной машине сервер, являющийся членом домена и работающий под управлением Server 2008 R2. Щелчок правой кнопкой мыши на строке, соответствующей серверу, открывает контекстное меню, которое позволяет перезапускать сервер, управлять им, подключаться к удаленному Рабочему столу и выполнять другие действия.

Создание групп серверов

Еще одна очень удобная возможность для окружений с большим количеством серверов, которыми нужно управлять, заключается в создании групп серверов. Это хороший способ организации серверов, который позволяет улучшить систему управления ими. Дело в том, что задачи можно выполнять для всей группы, а не для каждого отдельного сервера.

Создать группу серверов в диспетчере серверов довольно просто. Щелкните на ссылке Создать группу серверов (Create a server group) в панели мониторинга, добавьте серверы для включения в группу (рис. 10.4) и дайте группе имя. Например, можно создать группу для серверов главного офиса и еще одну — для филиала.

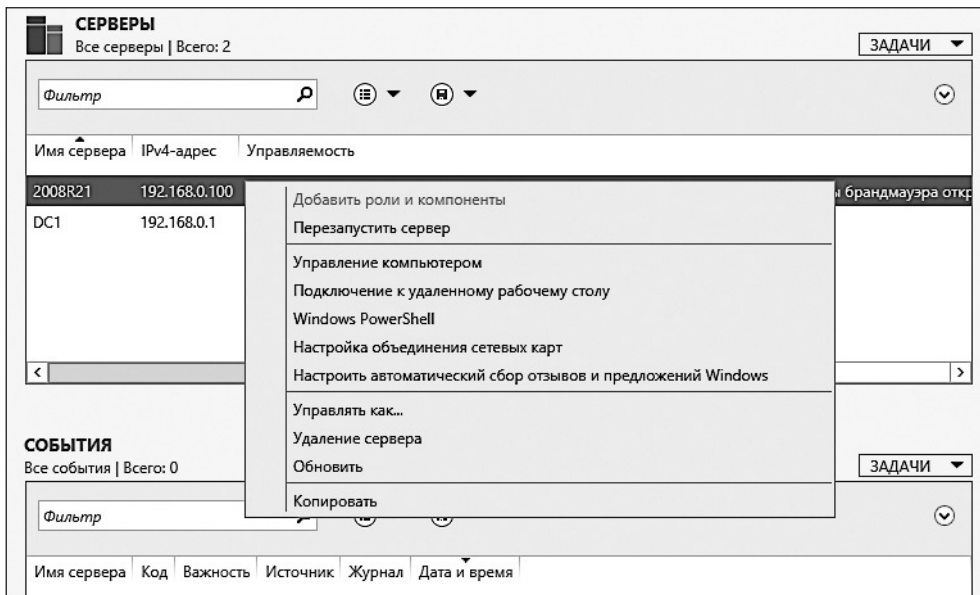


Рис. 10.3. Сервер, работающий под управлением Server 2008 R2, добавленный в диспетчер серверов

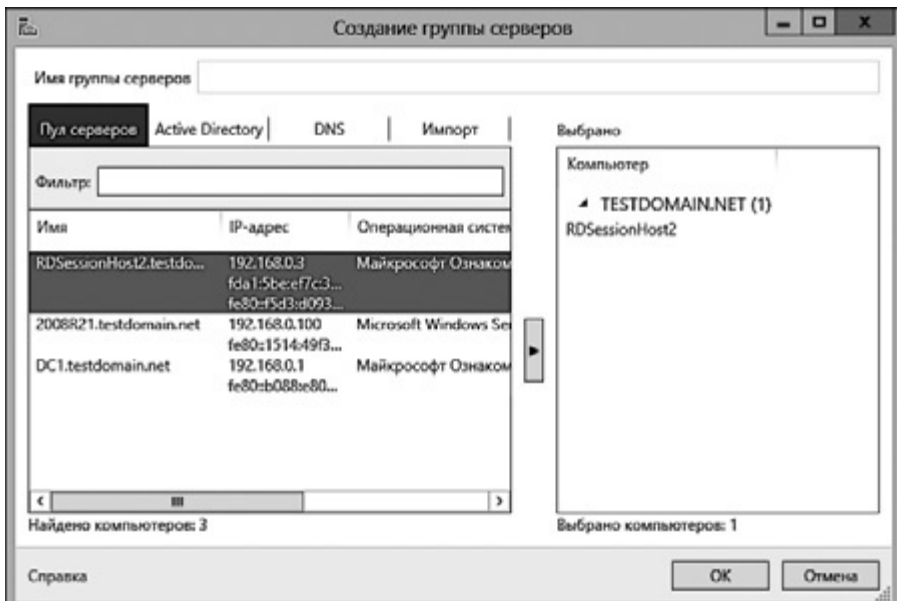


Рис. 10.4. Создание группы серверов

После того как группа создана, щелкните на ней правой кнопкой мыши, для того чтобы открыть контекстное меню, содержащее список операций, которые можно выполнить для серверов, входящих в группу (рис. 10.5).

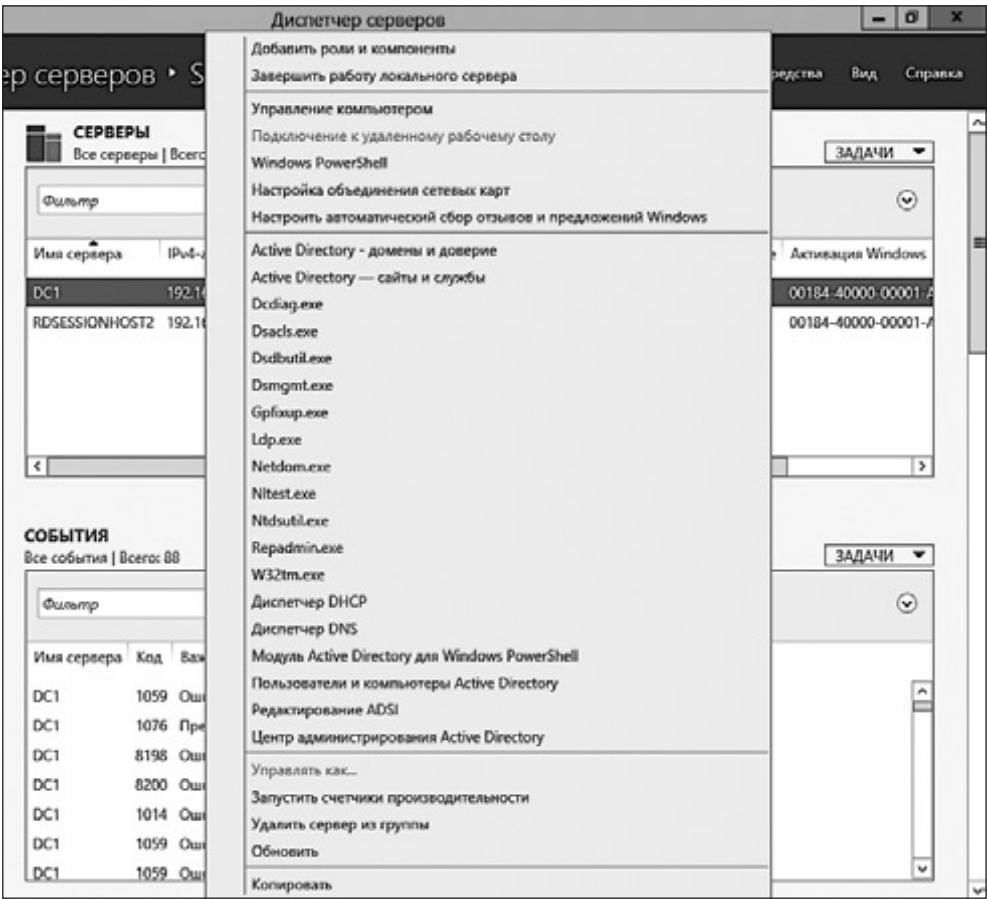


Рис. 10.5. Команды для управления группой серверов

Microsoft утверждает, что с помощью диспетчера серверов можно управлять сотней серверов. Однако если учесть нагрузку на сеть и на аппаратное обеспечение основного сервера, как и то, что роли и компоненты, развернутые на управляемых серверах, тоже потребляют ресурсы, попытка работать примерно с сотней серверов из одной консоли диспетчера серверов приведет к немалым сложностям в плане производительности. Большинству организаций, обладающих подобным количеством серверов, полезно будет обратить внимание

на Microsoft System Center 2012. Этот программный продукт разработан специально для организации управления большим количеством серверов. Некоторые рекомендации по эффективному и правильному использованию диспетчера серверов вы можете найти во врезке далее.

РЕКОМЕНДАЦИИ ПО ЭФФЕКТИВНОМУ ИСПОЛЬЗОВАНИЮ ДИСПЕТЧЕРА СЕРВЕРОВ

Вот несколько важных правил, которые стоит помнить при работе с диспетчером серверов.

- Добавление серверов, расположенных в различных доменах, требует доверительных отношений между доменами.
- С сервера, который обладает графическим интерфейсом, можно управлять ролями и компонентами систем, работающих под управлением ОС Server 2012, которая развернута в режиме установки основных серверных компонентов.
- В диспетчер серверов можно добавить отказоустойчивый кластер, но видны будут не имена отдельных серверов, а имя кластера. Кроме того, с помощью диспетчера серверов нельзя развертывать роли и компоненты в кластере.
- С помощью диспетчера серверов нельзя в удаленном режиме развертывать роли и компоненты на серверах, работающих под управлением ОС Windows Server, отличающихся от Server 2012.
- С помощью диспетчера серверов можно добавлять роли и компоненты на временно недоступные виртуальные жесткие диски, которые установлены на серверах, работающих под управлением Server 2012.

Значок оповещения

Значки оповещений, которые появляются в верхней части окна диспетчера серверов, весьма полезны. Они сигнализируют о выполнении каких-либо задач или о том, что на сервере произошло какое-то событие, требующее внимания администратора. Желтый значок — это предупреждение о событии. Красный флажок (рис. 10.6) сигнализирует об ошибке.

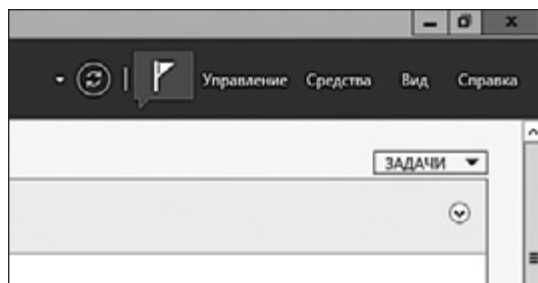


Рис. 10.6. Значок в диспетчере серверов, сигнализирующий об ошибке

Если щелкнуть на значке, будет открыто окно, сообщающее подробности о происходящем. Из сведений, которые там представлены, можно выяснить, что происходит с сервером, и быстро обратить внимание на возникшую проблему.

Конечно, вы можете использовать диспетчер серверов на клиентском компьютере, установив средства удаленного администрирования сервера (Remote Server Administration Tools, RSAT). При установке их на клиентский компьютер, работающий под управлением Windows 8, вы сможете воспользоваться всеми возможностями диспетчера серверов. Средства удаленного администрирования Server 2012 можно установить и на Windows 7-компьютере, но их возможности ограничены: используя их, вы узнаете лишь о том, работает ли в настоящий момент сервер. Поэтому, для того чтобы воспользоваться полными возможностями удаленного управления сервером, работайте с Windows 8-клиентами.

Анализатор соответствия рекомендациям

Хотя анализатор соответствия рекомендациям (Best Practices Analyzer, BPA) — это не новая функция Server 2012, он лучше представлен в интерфейсе диспетчера серверов. Его возможности, как и прежде, весьма полезны для системных администраторов.

С помощью анализатора соответствия рекомендациям можно просканировать любой сервер, добавленный в диспетчер серверов (рис. 10.7).

Анализатор соответствия рекомендациям ценен еще и тем, что он позволяет обнаруживать проблемы в режиме реального времени. Он связан со средством просмотра событий (Event Viewer). Вместо того чтобы независимо запускать

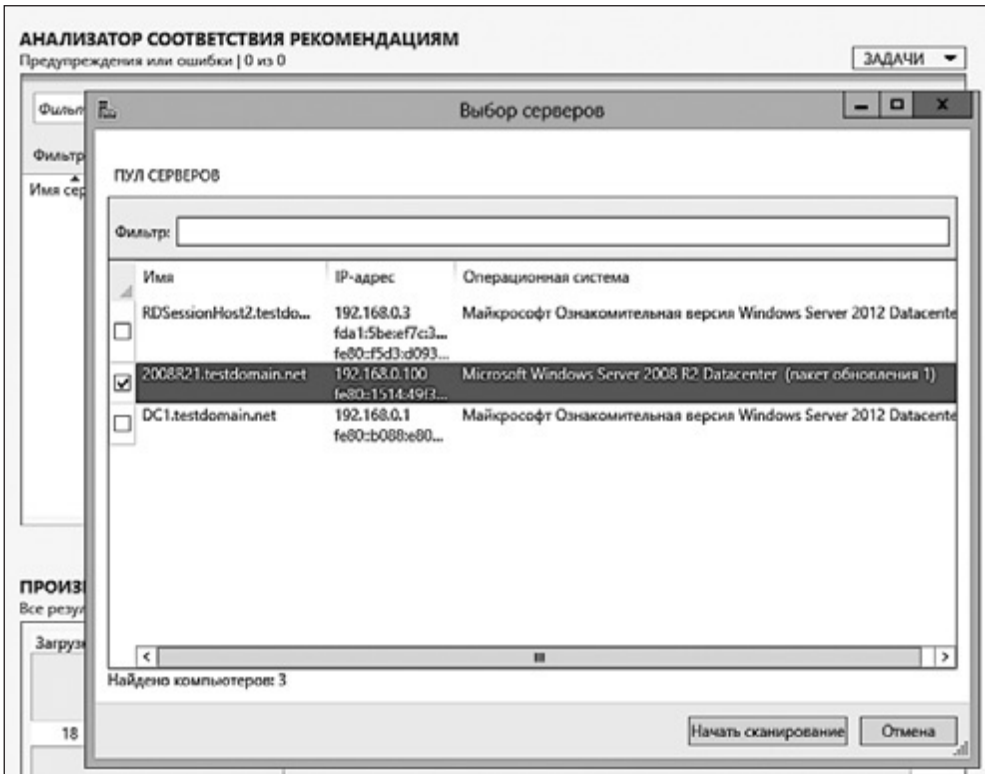


Рис. 10.7. Анализатор соответствия рекомендациям

средство просмотра событий и заниматься поиском ошибок в журнале, вы можете воспользоваться удобным интерфейсом ВРА. Это хороший пример широких возможностей управления инфраструктурой серверов, собранных в едином интерфейсе диспетчера серверов в Server 2012.

Windows PowerShell 3.0

В этой книге мы не вдавались в подробности работы с PowerShell, так как эта тема слишком обширна и, по сути, требует отдельной книги. Как я уже говорила, множество администраторов в компаниях небольшого и среднего размера, скорее всего, воспользуются средствами управления сервером, имеющими графический интерфейс. Однако всем администраторам нелишне будет познакомиться и с PowerShell, в частности, из-за его новых возможностей.

В Server 2012 включен PowerShell v3.0. Новичкам удобно начинать знакомство с PowerShell с использования встроенной в него системы IntelliSense. Этот механизм помогает изучать и создавать команды PowerShell. Как только вы начинаете вводить команду PowerShell, появляется список автозавершения, содержащий возможные варианты ввода команды.

Например, вы решили установить с помощью PowerShell какой-нибудь компонент, но не знаете точно, каков синтаксис команды, или не уверены в имени компонента. Компоненты можно установить с помощью команды PowerShell, имеющей вид `Install-компонент_windows -имя`. Если вы войдете в Windows Power Shell ISE (integrated scripting engine, интегрированная среда сценариев) и начнете вводить `Install-`, то увидите выпадающее меню, которое содержит список всех команд, которые можно использовать с `Install-` (рис. 10.8).

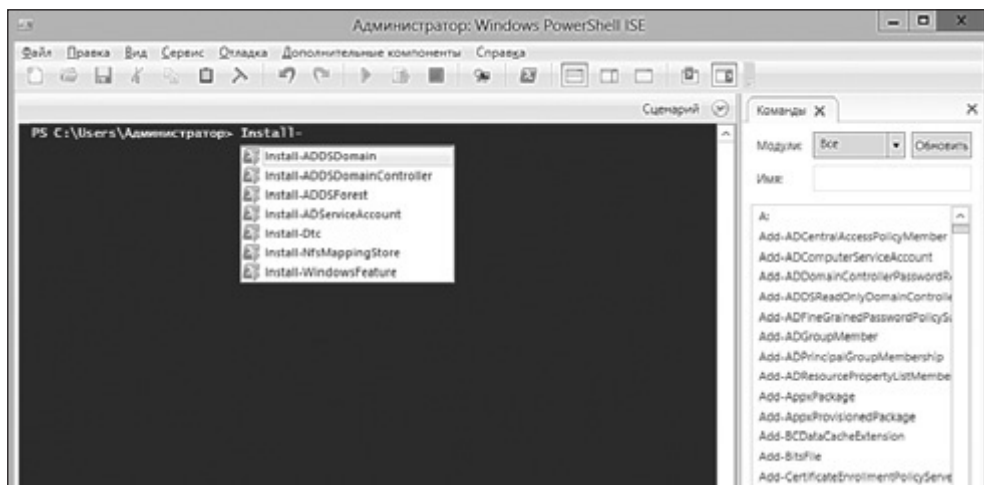


Рис. 10.8. Работа системы IntelliSense в PowerShell

Обратите внимание на правую часть рис. 10.8. Здесь вы видите список модулей, в котором можно искать командлеты PowerShell. В Server 2012 PowerShell позволяет управлять системой, используя командную строку, а благодаря наличию IntelliSense вы можете во время работы изучить правила написания команд PowerShell.

PowerShell обладает множеством новых возможностей, в том числе в этой системе имеется один особенный новый компонент, с которым многие из вас наверняка захотят познакомиться. Это веб-доступ к Windows PowerShell

(Windows Power Shell Web Access). Он позволяет управлять удаленным компьютером, используя PowerShell, через веб-браузер.

Для настройки этого компонента выполните следующее:

1. В панели мониторинга диспетчера серверов щелкните на ссылке **Добавить роли и компоненты** (Add roles and features). Щелкните на кнопке **Далее** (Next) и выберите **Установка ролей или компонентов** (Role-based or feature-based installation). Щелкните на кнопке **Далее** (Next). Выберите сервер, на котором хотите произвести установку. Снова щелкните на кнопке **Далее** (Next). Когда доберетесь до окна **Выбор ролей сервера** (Select server roles), щелкните на пункте **Компоненты** (Features) в левом меню. Найдите в списке компонентов группу **Windows PowerShell (установлено)** (Windows PowerShell (Installed)). Разверните группу, в ней будет присутствовать строка **Windows PowerShell Web Access** (Веб-доступ к Windows PowerShell) (рис. 10.9).

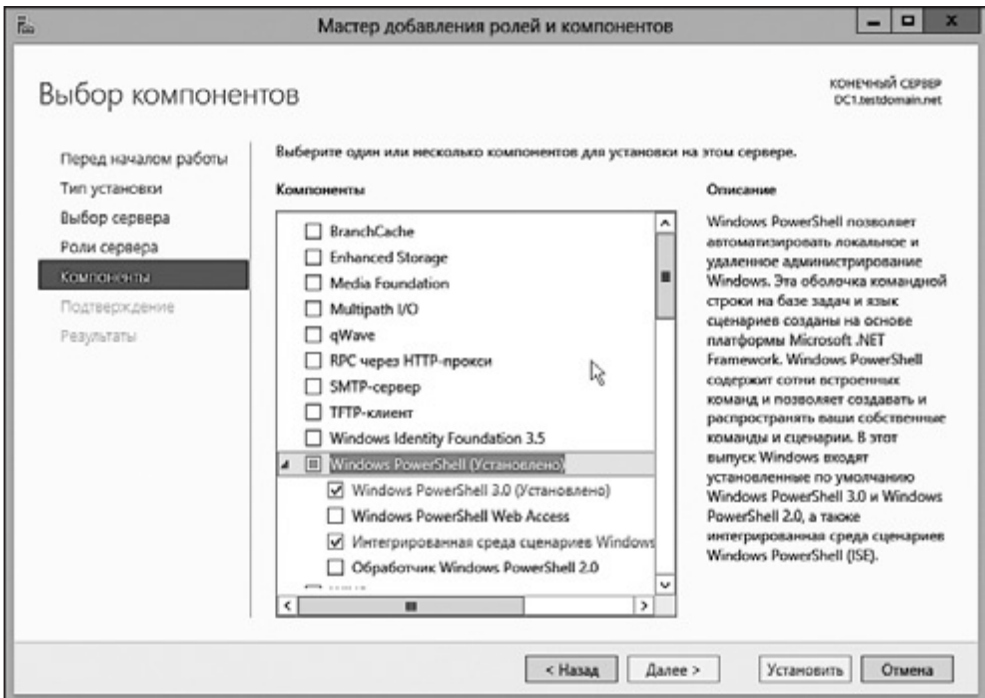


Рис. 10.9. Установка компонента веб-доступа к Windows PowerShell

2. Установите флажок **Windows PowerShell Web Access** (Веб-доступ к Windows PowerShell) и нажмите в появившемся окне кнопку **Добавить компоненты** (Add Features). Три раза щелкните на кнопке **Далее** (Next) и затем на кнопке **Установка** (Install).
3. Для того чтобы автоматически настроить веб-доступ к Windows PowerShell на использование параметров по умолчанию, выполните в PowerShell, запущенном от имени администратора, команду **Install-Pswa-WebApplication**. На рис. 10.10 показаны результаты выполнения этой команды.

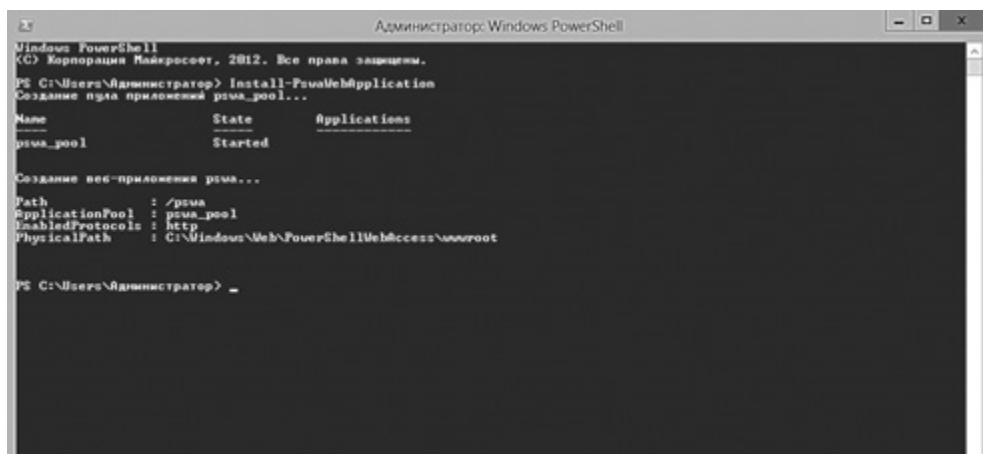


Рис. 10.10. Настройка веб-доступа к Windows PowerShell

После установки вы увидите в панели мониторинга диспетчера серверов службу IIS (Веб-сервер). Следующий этап настройки веб-доступа к PowerShell заключается в конфигурировании IIS. В данном примере мы настроим веб-доступ к PowerShell в виде подпапки IIS.

4. В диспетчере серверов выполните команду **Средства ► Диспетчер служб IIS (Tools ► IIS Manager)**. Теперь нужно создать пул приложений. Это можно сделать, развернув группу с именем IIS-сервера, щелкнув правой кнопкой на объекте Пулы приложений (Application Pools) и выбрав в появившемся меню команду **Добавить пул приложений** (Add Application Pools).
5. Дайте имя пулу приложения веб-доступа к PowerShell и нажмите ОК (рис. 10.11).

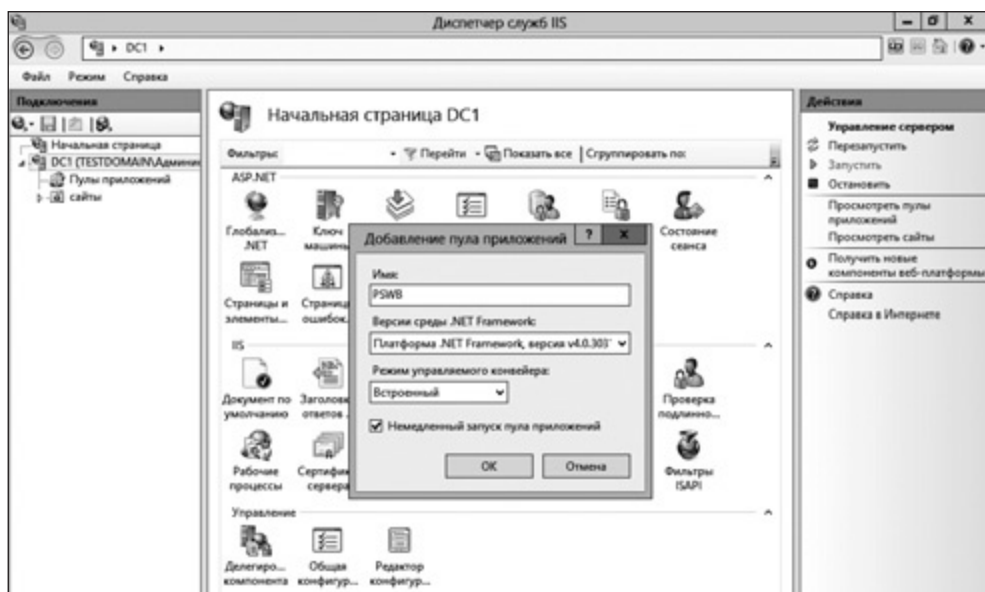


Рис. 10.11. Добавление пула приложений

6. Щелкните правой кнопкой мыши на объекте Default Web Site (Веб-сайт по умолчанию), который расположен в папке *Сайты (Sites)*, и в появившемся меню выберите команду **Добавить приложение (Add Application)**.
7. Введите псевдоним приложения и выберите пул приложений, созданный для веб-доступа к PowerShell. Кроме того, введите путь к системе веб-доступа к PowerShell — *C:\Windows\Web\PowerShellWebAccess\wwwroot*. Настройте и проверьте авторизацию, используя кнопки **Connect as** и **Test settings**. Нажмите **OK**.

Теперь вы можете пользоваться PowerShell удаленно, через браузер, введя в строку адреса URL, включающий в себя имя компьютера, на котором установлен веб-доступ к PowerShell, и имя приложения веб-доступа к PowerShell. В нашем примере имя компьютера — DC1, а имя приложения веб-доступа к PowerShell — PSWA. Введя в адресную строку браузера URL вида *http://DC1/PSWA*, мы увидим страницу подключения (рис. 10.12).

8. Для того чтобы приступить к работе с PowerShell, войдите в систему, используя настроенные учетные данные.



Рис. 10.12. Страница подключения к приложению для веб-доступа к PowerShell

Безопасность

Обеспечить безопасность в любой технологии всегда непросто. Постоянно появляются новые угрозы безопасности, и эти угрозы постоянно развиваются. Microsoft улучшила некоторые функции безопасности Server 2012, взяв за основу механизмы, которые использовались в Server 2008 R2. Множество улучшений системы безопасности, такие как динамический контроль доступа (Dynamic Access Control), рассмотренный в главе 5, созданы для работы с Windows 8-клиентами и доменами Windows.

Что касается безопасности доменов, в Server 2012 появились пять новых параметров групповой политики, которые можно использовать для усиления системы безопасности.

- *Учетные записи: блокировать учетные записи Майкрософт (Accounts: Block Microsoft accounts).* Этот параметр не позволяет пользователям добавлять на компьютер новые учетные записи Microsoft. В редакторе

управления групповыми политиками настроить этот параметр можно, пройдя по пути Конфигурация Windows ► Параметры безопасности ► Локальные политики ► Параметры безопасности (Windows Settings ► Security Settings ► Local Policies ► Security Options).

- *Интерактивный вход в систему: пороговое число неудачных попыток входа (Interactive logon: Machine account threshold)*. Этот параметр позволяет задать политику блокировки компьютеров, на которых для защиты томов используется шифрование BitLocker. Задайте данному параметру значение от 1 до 999, для того чтобы указать количество неудачных попыток входа в систему, после которых компьютер будет заблокирован. Данный параметр также можно найти по адресу: Конфигурация Windows ► Параметры безопасности ► Локальные политики ► Параметры безопасности (Windows Settings ► Security Settings ► Local Policies ► Security Options).
- *Интерактивный вход в систему: предел простоя компьютера (Interactive logon: Machine inactivity limit)*. Этот параметр позволяет заблокировать сеанс после того, как длительность простоя компьютера превысит отрезок времени, который задается в секундах. Найти данный параметр можно, пройдя по пути Конфигурация Windows ► Параметры безопасности ► Локальные политики ► Параметры безопасности (Windows Settings ► Security Settings ► Local Policies ► Security Options).
- *Сетевой сервер (Майкрософт): попытка S4U2Self получить информацию об утверждении (Microsoft network server: Attempt Service for user to self (S4U2Self) to obtain claim information)*. Включение этого параметра позволяет Windows-клиентам с ОС, выпущенными до Windows 8, получать доступ к файловым ресурсам, расположенным на файловом сервере, который работает под управлением Server 2012 и требует использования заявок пользователя. Это часть системы динамического контроля доступа (Dynamic Access Control). Данный параметр также расположен по адресу: Конфигурация Windows ► Параметры безопасности ► Локальные политики ► Параметры безопасности (Windows Settings ► Security Settings ► Local Policies ► Security Options).
- *Правила упакованных приложений (Package app rules)*. Этот параметр применяет правила AppLocker к пакетам приложений, которые имеют общие атрибуты, такие как имя или версия пакета приложения. Технология AppLocker впервые появилась в Windows Server 2008 R2. Она позволяет задавать разрешения на использование приложений пользователями и группами пользователей. Этот параметр можно найти, пройдя по пути Конфигурация Windows ► Параметры безопасности ► Политики

управления приложениями ▶ AppLocker (Windows Settings ▶ Security Settings ▶ Application Control Policies ▶ AppLocker).

BitLocker

В Server 2012 технология BitLocker, впервые появившаяся в Windows 7 и Windows Server 2008 R2, также улучшена. Теперь ее можно использовать с Windows 8-клиентами. Применение BitLocker позволяет шифровать тома дисков, используя стойкий к взлому стандарт шифрования AES (advanced encryption standard, усовершенствованный стандарт шифрования).

В Server 2012 вы можете установить компонент Шифрование диска BitLocker (BitLocker Drive Encryption) с помощью диспетчера серверов. После установки шифрованием BitLocker можно управлять в панели управления (Control panel) сервера (рис. 10.13).



Рис. 10.13. Шифрование диска BitLocker в Server 2012

Для того чтобы разблокировать зашифрованный том, можно использовать либо имя и пароль пользователя, либо смарт-карту. При включении данной возможности вы должны решить, какой должна быть резервная копия ключа восстановления доступа к диску. Ее можно либо сохранить на USB-носитель, либо сохранить в виде файла, либо распечатать на принтере.

При работе с мастером настройки BitLocker (BitLocker Manager wizard) вы обнаружите на одном из его экранов новые параметры. Ранее можно было зашифровать лишь весь том. Теперь вы можете выбрать шифрование только занятого места на диске, что позволяет ускорить процесс шифрования (рис. 10.14).

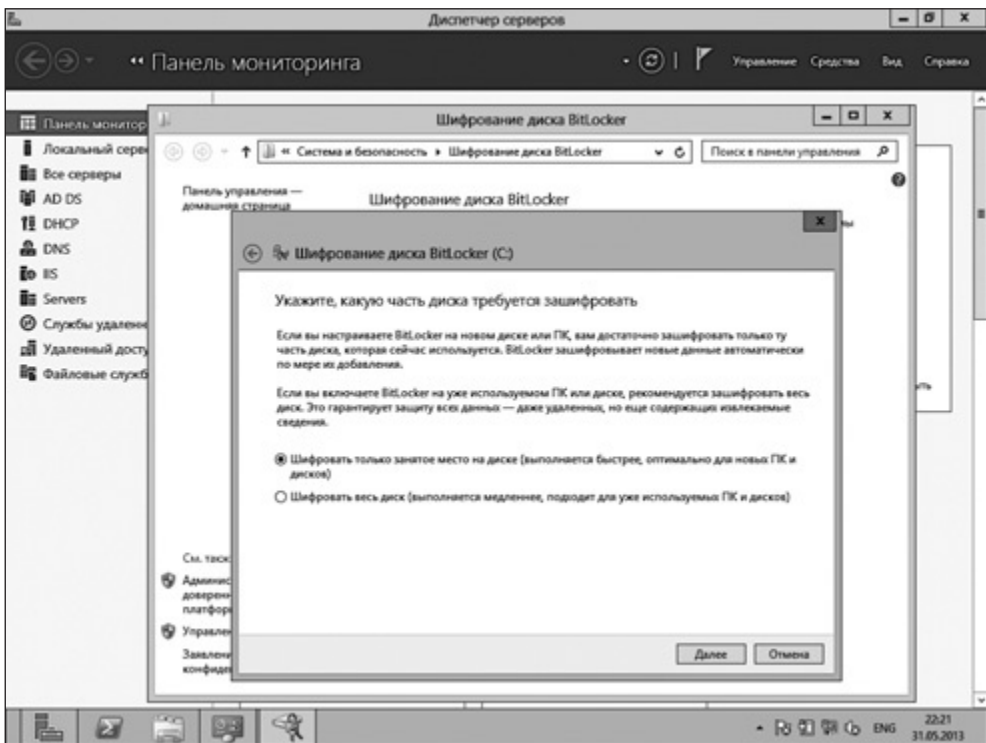


Рис. 10.14. Выбор параметра, который позволяет шифровать только занятое место на диске

Еще одно новшество BitLocker заключается в том, что теперь пользователям можно дать разрешение на изменение их ПИН-кодов и паролей BitLocker. Это поможет сократить количество обращений пользователей в службу поддержки.

Для того чтобы включить эту возможность, нужно открыть редактор управления групповыми политиками и пройти по пути Конфигурация компьютера ► Политики ► Административные шаблоны ► Компоненты Windows ► Этот параметр позволяет выбрать шифрование диска BitLocker ► Диски операционной системы (Computer Configuration ► Administrative Templates ► Windows Components ► BitLocker Drive Encryption ► Operating System Drives). Настройте параметр политики, позволяющий запретить обычным пользователям изменять ПИН-код или пароль.

В Windows Server 2012 имеется новый компонент: Сетевая разблокировка BitLocker (Network Unlock). Он позволяет автоматически разблокировать системные тома при перезагрузке, если компьютер подключен к корпоративной сети. Этот компонент можно установить с помощью команды Добавить роли и компоненты (Add roles and features) в диспетчере серверов.

Другие улучшения систем безопасности

Знайте, что в Server 2012 имеются улучшения систем безопасности, которые незаметны с первого взгляда. Они относятся к протоколу проверки подлинности Kerberos и поддержке дополнительных устройств сторонних производителей, таких как смарт-карты и биометрические датчики. Если ваша организация нуждается в подобных возможностях, подробности о них вы можете найти на веб-сайте Microsoft TechNet.

Кроме того, Microsoft предлагает некоторые дополнительные инструменты, которыми можно воспользоваться при построении безопасной сетевой инфраструктуры. Вот некоторые из них:

- Microsoft Security Assessment Tool 4.0 (<http://www.microsoft.com/ru-ru/download/details.aspx?id=12273>).
- Microsoft Baseline Security Analyzer 2.2 (<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=7558>).
- Microsoft Security Compliance Manager (<http://www.microsoft.com/en-us/download/details.aspx?displayLang=en&id=16776>).

Выводы

Server 2012 разработан в расчете на значительное расширение обычной клиент-серверной модели инфраструктуры, которая применялась в центрах обработки данных много лет. Эта операционная система поддерживает новейшие тенденции в области информационных технологий, такие как облачные вычисления, использование мобильных устройств в корпоративных сетях, виртуализация. Поэтому организация мониторинга и обеспечение безопасности сетевой инфраструктуры жизненно важны для создания устойчиво функционирующей рабочей среды.

Консоль нового диспетчера серверов является универсальным инструментом для управления физическими серверами, развернутыми на предприятии, и не только ими. Среди других объектов, которыми можно управлять с ее помощью, — виртуальные машины и кластеры серверов. Интеграция диспетчера серверов и средства просмотра событий, возможности показа оповещений дают администратору инструменты для эффективного мониторинга состояния инфраструктуры, позволяют быстро выявлять и решать проблемы.

Помимо новых возможностей в области безопасности, которые легко обнаружить в редакторе групповых политик и средстве настройки BitLocker, платформа Server 2012 обладает и другими усовершенствованиями в данной сфере. Среди них улучшенные механизмы проверки подлинности, управление пользователями и файлами с помощью системы динамического контроля доступа (Dynamic Access Control) и поддержка дополнительных устройств, помогающих обеспечить повышенный уровень безопасности, таких как смарт-карты и сканеры отпечатков пальцев.

Об авторе

Самара Линн более 15 лет работает в IT-индустрии. В частности, она занимала должность IT-директора в крупном медицинском учреждении Нью-Йорка. Она — ведущий сетевой и бизнес-аналитик Rsmag.com. У нее есть несколько сертификатов в области информационных технологий и степень бакалавра, полученная в Бруклинском колледже. Кроме того, она работала редактором отдела технологий в Центре тестирования CRN.

Самара Линн
Администрирование Microsoft Windows Server 2012
Перевел с английского А. Заика

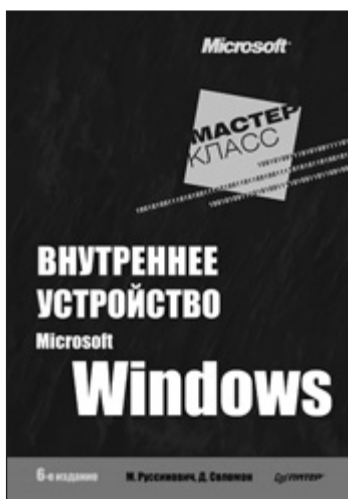
Заведующий редакцией
Руководитель проекта
Ведущий редактор
Литературный редактор
Художественный редактор
Корректор
Верстка

А. Кривцов
А. Юрченко
Ю. Сергиенко
Н. Рощина
Л. Адуевская
В. Листова
Е. Волощина

ООО «Питер Пресс», 192102, Санкт-Петербург, ул. Андреевская (д. Волкова), д. 3, литер А, пом. 7Н.
Налоговая льгота — общероссийский классификатор продукции ОК 005-93, том 2; 95 3005 — литература учебная.
Подписано в печать 19.07.13. Формат 70х100/16. Усл. п. л. 24,510. Тираж 1500. Заказ
Отпечатано в полном соответствии с качеством предоставленных издательством материалов
в ГППО «Псковская областная типография». 180004, Псков, ул. Ротная, 34.

Внутреннее устройство Microsoft Windows. 6-е изд.

М. Руссинович, Д. Соломон



ISBN: 978-5-496-00434-3

Объем: 800 с.

Шестое издание этой легендарной книги посвящено внутреннему устройству и алгоритмам работы основных компонентов операционной системы Microsoft Windows 7, а также Windows Server 2008 R2. Определяются ключевые понятия и термины Windows, дается представление об инструментальных средствах, используемых для исследования внутреннего устройства системы, рассматривается общая архитектура и компоненты ОС. Также в книге дается представление о ключевых основополагающих системных и управляющих механизмах Windows, охватываются основные компоненты операционной системы: процессы, потоки и задания; безопасность и работа в сети.

Книга предназначена для системных администраторов, разработчиков сложных приложений и всех, кто хочет понять, как устроена операционная система Windows.

12+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ВАМ НРАВЯТСЯ НАШИ КНИГИ? ЗАРАБАТЫВАЙТЕ ВМЕСТЕ С НАМИ!

У Вас есть свой сайт?

Вы ведете блог?

Регулярно общаетесь на форумах? Интересуетесь литературой, любите рекомендовать хорошие книги и хотели бы стать нашим партнером?

ЭТО ВПОЛНЕ РЕАЛЬНО!

СТАНЬТЕ УЧАСТНИКОМ ПАРТНЕРСКОЙ ПРОГРАММЫ ИЗДАТЕЛЬСТВА «ПИТЕР»!



Зарегистрируйтесь на нашем сайте в качестве партнера по адресу www.piter.com/ePartners



Получите свой персональный уникальный номер партнера



Выбирайте книги на сайте www.piter.com, размещайте информацию о них на своем сайте, в блоге или на форуме и добавляйте в текст ссылки на эти книги (на сайт www.piter.com)

ВНИМАНИЕ! В каждую ссылку необходимо добавить свой персональный уникальный номер партнера.

С этого момента получайте 10% от стоимости каждой покупки, которую совершит клиент, придя в интернет-магазин «Питер» по ссылке с Вашим партнерским номером. А если покупатель приобрел не только эту книгу, но и другие издания, Вы получаете дополнительно по 5% от стоимости каждой книги.

Деньги с виртуального счета Вы можете потратить на покупку книг в интернет-магазине издательства «Питер», а также, если сумма будет больше 500 рублей, перевести их на кошелек в системе Яндекс.Деньги или Web.Money.

Пример партнерской ссылки:

<http://www.piter.com/book.phtml?978538800282> – обычная ссылка

<http://www.piter.com/book.phtml?978538800282&refer=0000> – партнерская ссылка, где 0000 – это ваш уникальный партнерский номер

**Подробнее о Партнерской программе
ИД «Питер» читайте на сайте
WWW.PITER.COM**







КНИГА-ПОЧТОЙ



ЗАКАЗАТЬ КНИГИ ИЗДАТЕЛЬСКОГО ДОМА «ПИТЕР» МОЖНО ЛЮБЫМ УДОБНЫМ ДЛЯ ВАС СПОСОБОМ:

- на нашем сайте: **www.piter.com**
- по электронной почте: **postbook@piter.com**
- по телефону: **(812) 703-73-74**
- по почте: **197198, Санкт-Петербург, а/я 127, ООО «Питер Мейл»**
- по ICQ: **413763617**

ВЫ МОЖЕТЕ ВЫБРАТЬ ЛЮБОЙ УДОБНЫЙ ДЛЯ ВАС СПОСОБ ОПЛАТЫ:

-  Наложенным платежом с оплатой при получении в ближайшем почтовом отделении.
-  С помощью банковской карты. Во время заказа Вы будете перенаправлены на защищенный сервер нашего оператора, где сможете ввести свои данные для оплаты.
-  Электронными деньгами. Мы принимаем к оплате все виды электронных денег: от традиционных Яндекс.Деньги и Web-money до USD E-Gold, MoneyMail, INOCard, RBK Money (RuPay), USD Bets, Mobile Wallet и др.
-  В любом банке, распечатав квитанцию, которая формируется автоматически после совершения Вами заказа.

Все посылки отправляются через «Почту России». Отработанная система позволяет нам организовывать доставку Ваших покупок максимально быстро. Дату отправления Вашей покупки и предполагаемую дату доставки Вам сообщат по e-mail.

ПРИ ОФОРМЛЕНИИ ЗАКАЗА УКАЖИТЕ:

- фамилию, имя, отчество, телефон, факс, e-mail;
- почтовый индекс, регион, район, населенный пункт, улицу, дом, корпус, квартиру;
- название книги, автора, количество заказываемых экземпляров.



Нет времени ходить по магазинам?



наберите:



www.piter.com



Здесь вы найдете:

Все книги издательства сразу
Новые книги — в момент выхода из типографии
Информацию о книге — отзывы, рецензии, отрывки
Старые книги — в библиотеке и на CD



**И наконец, вы нигде не купите
наши книги дешевле!**

ПРЕДСТАВИТЕЛЬСТВА ИЗДАТЕЛЬСКОГО ДОМА «ПИТЕР»
предлагают профессиональную и популярную литературу по различным
направлениям: история и публицистика, экономика и финансы, менеджмент
и маркетинг, компьютерные технологии, медицина и психология.

РОССИЯ

Санкт-Петербург: м. «Выборгская», Б. Сампсониевский пр., д. 29а
тел./факс: (812) 703-73-73, 703-73-72; e-mail: sales@piter.com

Москва: м. «Электrozаводская», Семеновская наб., д. 2/1, стр. 1
тел./факс: (495) 234-38-15; e-mail: sales@msk.piter.com

Воронеж: тел.: 8 951 861-72-70; e-mail: voronej@piter.com

Екатеринбург: ул. Бебеля, д. 11а
тел./факс: (343) 378-98-41, 378-98-42; e-mail: office@ekat.piter.com

Нижний Новгород: тел.: 8 960 187-85-50; e-mail: nnovgorod@piter.com

Новосибирск: Комбинатский пер., д. 3
тел./факс: (383) 279-73-92; e-mail: sib@nsk.piter.com

Ростов-на-Дону: ул. Ульяновская, д. 26
тел./факс: (863) 269-91-22, 269-91-30; e-mail: piter-ug@rostov.piter.com

Самара: ул. Молодогвардейская, д. 33а, офис 223
тел./факс: (846) 277-89-79, 229-68-09; e-mail: samara@piter.com


УКРАИНА


Киев: Московский пр., д. 6, корп. 1, офис 33
тел./факс: (044) 490-35-69, 490-35-68; e-mail: office@kiev.piter.com


Харьков: ул. Суздальские ряды, д. 12, офис 10
тел./факс: (057) 7584145, +38 067 545-55-64; e-mail: piter@kharkov.piter.com

БЕЛАРУСЬ

Минск: ул. Розы Люксембург, д. 163
тел./факс: (517) 208-80-01, 208-81-25; e-mail: minsk@piter.com

 Издательский дом «Питер» приглашает к сотрудничеству зарубежных торговых
партнеров или посредников, имеющих выход на зарубежный рынок
тел./факс: (812) 703-73-73; e-mail: spb@piter.com

 Издательский дом «Питер» приглашает к сотрудничеству авторов
тел./факс издательства: (812) 703-73-72, (495) 974-34-50

 Заказ книг для вузов и библиотек
тел./факс: (812) 703-73-73, доб. 6250; e-mail: uchebnik@piter.com

 Заказ книг по почте: на сайте www.piter.com; по тел.: (812) 703-73-74, доб. 6225
