

# **Microsoft Windows Server 2012.**

Справочник администратора.

# Оглавление

<b>Введение .....</b>	<b>5</b>
Для кого предназначена эта книга .....	6
Организация книги .....	7

## **ЧАСТЬ I. ОСНОВЫ АДМИНИСТРИРОВАНИЯ WINDOWS SERVER 2012..... 11**

<b>Глава 1. Обзор администрирования Windows Server .....</b>	<b>13</b>
Windows Server 2012 и Windows 8 .....	13
Знакомство с Windows Server 2012 .....	15
Параметры управления питанием .....	18
Сетевые утилиты и протоколы .....	21
Сетевые настройки .....	22
Работа с сетевыми протоколами .....	22
Контроллеры домена, рядовые серверы и службы домена .....	24
Работа с Active Directory .....	24
Контроллеры домена только для чтения .....	26
Перезапускаемые доменные службы Active Directory .....	26
Сервисы разрешения имен .....	27
Система доменных имен .....	28
Службы имен Интернета для Windows .....	29
Протокол LLMNR .....	31
Часто используемые инструменты .....	32
Windows PowerShell 3.0 .....	33
Служба удаленного управления Windows .....	35
Включение и использование WinRM .....	35
Настройка WinRM .....	36
<b>Глава 2. Управление серверами на базе Windows Server 2012.....</b>	<b>39</b>
Роли серверов, службы ролей и компоненты Windows Server 2012 .....	39

Установки сервера: полная, с минимальным графическим интерфейсом и установка основных серверных компонентов .....	47
Обзор установки основных серверных компонентов .....	48
Установка Windows Server 2012 .....	50
Чистая установка .....	51
Обновление существующей системы .....	54
Дополнительные административные задачи во время установки .....	55
Использование командной строки во время установки .....	55
Принудительное удаление раздела диска во время установки .....	59
Загрузка драйверов устройств во время установки .....	59
Создание, форматирование, удаление и расширение разделов диска во время установки .....	60
Изменение типа установки .....	61
Конвертирование полной установки и установки с минимальным графическим интерфейсом .....	62
Конвертирование установки с основными серверными компонентами .....	62
Управление ролями, службами ролей и компонентами .....	63
Начальная настройка .....	63
Основные компоненты диспетчера серверов и двоичные файлы .....	68
Удаленное управление серверами .....	71
Подключение и работа с удаленными серверами .....	73
Добавление и удаление ролей, ролевых служб и компонентов .....	76
Управление свойствами системы .....	79
Вкладка <i>Имя компьютера</i> .....	81
Вкладка <i>Оборудование</i> .....	82
Вкладка <i>Дополнительно</i> .....	82
Настройка быстродействия Windows .....	82
Настройка быстродействия приложений .....	83
Настройка виртуальной памяти .....	83
Настройка предотвращения выполнения данных .....	86
Настройка системных и пользовательских переменных среды .....	87
Настройка загрузки и восстановления системы .....	89
Вкладка <i>Удаленный доступ</i> .....	91
<b>Глава 3. Мониторинг процессов, служб и событий .....</b>	<b>93</b>
Управление приложениями, процессами и производительностью .....	93
Диспетчер задач .....	93
Просмотр и работа с процессами .....	94
Администрирование процессов .....	97
Просмотр системных служб .....	100
Просмотр и управление производительностью системы .....	101
Использование центрального процессора .....	102
Использование памяти .....	103
Использование сети .....	104
Просмотр и управление удаленными сеансами пользователей .....	105
Управление системными службами .....	106
Навигация по службам в диспетчере серверов .....	106
Навигация по службам в консоли <i>Управление компьютером</i> .....	107
Запуск, остановка и приостановка служб .....	109
Настройка запуска службы .....	109
Настройка входа в систему службы .....	110

Настройка восстановления службы.....	112
Отключение ненужных служб .....	113
Просмотр и протоколирования событий .....	113
Доступ к событиям в диспетчере серверов.....	115
Доступ к событиям в средстве <i>Просмотр событий</i> .....	116
Фильтрация журналов событий.....	118
Установка параметров журнала событий .....	120
Очистка журналов событий .....	122
Архивирование журналов событий .....	122
Форматы архивов журналов .....	122
Архивирование журналов.....	123
Просмотр архивов журналов.....	123
Мониторинг производительности и активности сервера .....	124
Почему нужно контролировать сервер? .....	124
Готовимся к мониторингу .....	125
Использование консолей мониторинга.....	125
Выбор счетчиков.....	128
Журналирование производительности .....	130
Группы сборщиков данных: создание и управление .....	131
Сбор данных счетчиков производительности.....	131
Сбор данных трассировки производительности.....	133
Сбор данных сведений о конфигурации системы .....	133
Просмотр отчетов сборщика данных .....	134
Настройка оповещений счетчиков производительности.....	135
Тюнинг производительности системы .....	136
Мониторинг и тюнинг использования памяти .....	136
Мониторинг и тюнинг использования процессора.....	138
Мониторинг и тюнинг дискового ввода-вывода .....	138
Мониторинг и тюнинг пропускной способности сети и возможности соединения.....	139
<b>Глава 4. Автоматизация административных задач, политики и процедуры.....</b>	<b>141</b>
Групповая политика.....	143
Основы групповой политики .....	144
Порядок применения множественных политик .....	145
Когда применяются групповые политики?.....	145
Требования групповой политики и совместимость версий.....	146
Изменение групповой политики .....	146
Управление локальными групповыми политиками .....	149
Локальные объекты групповой политики.....	149
Получение доступа к настройкам локальной политики верхнего уровня.....	150
Настройки локального объекта групповой политики.....	151
Получение доступа к административной и неадминистративной политике и пользовательской политике .....	152
Управление политиками сайта, домена и организационного подразделения.....	152
Политики домена и политики по умолчанию.....	153
Консоль управления групповой политикой.....	154
Знакомство с редактором политик.....	155
Использование административных шаблонов для установки политик.....	157
Создание и связь объекта групповой политики .....	158
Создание и использование исходных объектов групповой политики.....	160
Делегирование полномочий для управления групповой политикой .....	160
Блокирование, переопределение и отключение политик .....	162

Обслуживание, поиск и устранение неисправностей групповой политики .....	165
Обновление групповой политики .....	165
Настройка интервала обновления .....	166
Моделирование групповой политики для планирования .....	168
Копирование, вставка и импорт объектов политики .....	171
Резервное копирование и восстановление объектов политики .....	172
Определение текущих настроек групповой политики и статуса определения .....	173
Отключение неиспользуемой части групповой политики .....	173
Изменение свойств обработки политики .....	174
Настройка обнаружения медленного соединения .....	175
Удаление ссылок и удаление GPO .....	177
Поиск и устранение неисправностей групповой политики .....	178
Исправление объектов групповой политики по умолчанию .....	180
Управление пользователями и компьютерами с помощью групповой политики .....	180
Централизованное управление специальными папками .....	181
Перенаправление специальных папок в единое расположение .....	181
Перенаправление специальных папок на основании членства в группе .....	183
Удаление перенаправления .....	185
Управление сценариями пользователя и компьютера .....	185
Назначения сценариев Computer Startup и Computer Shutdown .....	186
Назначение сценариев входа и выхода пользователя .....	187
Развертывание программного обеспечения через групповую политику .....	189
Знакомство с политикой установки программного обеспечения .....	189
Развертывание программ в организации .....	190
Настройка параметров развертывания программного обеспечения .....	191
Обновление развернутого программного обеспечения .....	193
Обновление развернутого приложения .....	193
Автоматическая регистрация сертификатов компьютера и пользователя .....	194
Управление автоматическими обновлениями с помощью групповой политики .....	195
Настройка автоматических обновлений .....	196
Оптимизация автоматических обновлений .....	196
Использование службы обновлений в интрасети .....	197
<b>Глава 5. Улучшение безопасности компьютера .....</b>	<b>199</b>
Использование шаблонов безопасности .....	199
Использование оснасток <i>Шаблоны безопасности</i> и <i>Анализ и настройка безопасности</i> .....	201
Просмотр и изменение настроек шаблона .....	201
Изменение настроек для политики учетных записей, локальных политик и журнала событий .....	202
Настройка групп с ограниченным доступом .....	203
Включение, отключение и настройка системных служб .....	204
Настройка параметров безопасности для реестра и файловой системы .....	206
Анализ, просмотр и применения шаблонов безопасности .....	209
Развертывание шаблонов безопасности на нескольких компьютерах .....	212
Использование мастера настройки безопасности .....	214
Создание политик безопасности .....	214
Редактирование политик безопасности .....	219
Применение политик безопасности .....	219
Откат последней примененной политики безопасности .....	220
Развертывание политики безопасности на нескольких компьютерах .....	220

<b>ЧАСТЬ II. АДМИНИСТРИРОВАНИЕ СЛУЖБ КАТАЛОГОВ WINDOWS SERVER .....</b>	<b>223</b>
<b>Глава 6. Использование Active Directory .....</b>	<b>225</b>
Введение в Active Directory .....	225
Active Directory и DNS .....	225
Развертывание контроллера домена только для чтения .....	227
Компоненты Active Directory для Windows Server 2008 R2 .....	227
Компоненты Active Directory для Windows Server 2012 .....	229
Работа со структурами домена .....	231
Домены .....	231
Лес и дерево домена .....	232
Организационные подразделения .....	235
Сайты и подсети .....	236
Работа с доменами Active Directory .....	237
Использование компьютеров с Active Directory .....	237
Работа с функциональными уровнями домена .....	238
Использование функционального уровня Windows Server 2003 .....	239
Использование функционального уровня Windows Server 2008 .....	240
Использование функционального уровня Windows Server 2008 R2 .....	241
Использование функционального уровня Windows Server 2012 .....	242
Повышение или понижение функциональности домена и леса .....	242
Структура каталога .....	244
Хранилище данных .....	245
Глобальные каталоги .....	245
Кэширование состава универсальных групп .....	246
Репликация и Active Directory .....	247
Active Directory и LDAP .....	248
Роли FSMO .....	248
Корзина Active Directory .....	250
Подготовка схемы для Корзины .....	250
Восстановление удаленных объектов .....	251
Использование Ldp.exe для базового восстановления .....	252
Использование Windows PowerShell для базового и расширенного восстановления .....	252
Использование расширенной Корзины для восстановления .....	254
<b>Глава 7. Базовое администрирование Active Directory .....</b>	<b>255</b>
Средства управления Active Directory .....	255
Утилиты администрирования Active Directory .....	255
Утилиты Active Directory для командной строки .....	256
Утилиты поддержки Active Directory .....	257
Использование оснастки <i>Active Directory — пользователи и компьютеры</i> .....	258
Центр администрирования Active Directory и Windows PowerShell .....	262
Управление учетными записями компьютера .....	265
Создание учетных записей компьютера на рабочей станции или сервере .....	265
Создание учетной записи компьютера в Центре администрирования Active Directory .....	266
Создание учетной записи компьютера с помощью оснастки <i>Active Directory —     пользователи и компьютеры</i> .....	267
Просмотр и редактирование свойств учетной записи компьютера .....	269
Удаление, отключение и включение учетных записей компьютера .....	269
Сброс заблокированных учетных записей .....	270

Перемещение учетных записей компьютера .....	271
Управление компьютерами .....	272
Присоединение компьютера к домену или рабочей группе .....	272
Использование автономной регистрации в домене .....	274
Управление контроллерами домена, ролями и каталогами .....	276
Установка и понижение роли контроллера домена .....	276
Просмотр и передача ролей домена .....	279
Просмотр и передача роли <i>Владелец доменных имен</i> .....	280
Просмотр и передача роли хозяина схемы .....	281
Передача ролей с использованием командной строки .....	281
Захват ролей с использованием командной строки .....	282
Настройка глобальных каталогов .....	285
Настройка кэширования членства в универсальных группах .....	285
Управление организационными подразделениями .....	286
Создание организационных подразделений .....	286
Просмотр и редактирование свойств организационных подразделений .....	287
Переименование и удаление организационных подразделений .....	287
Перемещение организационных подразделений .....	287
Управление сайтами .....	287
Создание сайтов .....	288
Создание подсетей .....	289
Связь контроллеров домена с сайтом .....	290
Настройка связей сайта .....	290
Создание мостов связей сайта .....	293
Обслуживание Active Directory .....	294
Использование утилиты <i>Редактирование ADSI</i> .....	294
Исследование межсайтовой топологии .....	296
Решение проблем с Active Directory .....	297
<b>Глава 8. Создание учетных записей пользователя и группы .....</b>	<b>301</b>
Модель безопасности Windows Server .....	301
Протоколы аутентификации .....	302
Контроль доступа .....	303
Технология идентификации на основе требований .....	303
Централизованные политики доступа .....	305
Различия между учетными записями пользователя и группы .....	307
Учетные записи пользователей .....	307
Имена входа, пароли и публичные сертификаты .....	307
Идентификаторы безопасности и учетные записи пользователей .....	308
Учетные записи групп .....	308
Типы групп .....	309
Область действия группы .....	309
Идентификаторы безопасности и учетные записи групп .....	310
Когда использовать локальные группы домена, глобальные и универсальные группы .....	311
Учетные записи пользователей и групп по умолчанию .....	312
Встроенные учетные записи пользователей .....	313
Предопределенные учетные записи пользователя .....	313
Учетная запись <i>Администратор</i> .....	313
Учетная запись <i>Гость</i> .....	314

Встроенные и предопределенные группы .....	314
Неявные группы и специальные идентификаторы .....	315
Возможности учетной записи .....	315
Привилегии.....	316
Права входа .....	319
Встроенные возможности для групп в Active Directory .....	320
Использование учетных записей групп по умолчанию.....	322
Группы, используемые администраторами .....	322
Неявные группы и идентификаторы .....	324
Установка и организация учетной записи пользователя .....	325
Политики именования учетных записей .....	325
Правила для отображаемых имен .....	326
Правила для имен входа .....	326
Схемы имен .....	326
Политики паролей и учетных записей .....	327
Использование безопасных паролей.....	327
Установка политик учетных записей.....	327
Настройка политик учетной записи.....	330
Настройка политик паролей.....	330
Ведение журнала паролей.....	330
Максимальный срок действия пароля .....	330
Минимальный срок действия пароля .....	331
Минимальная длина пароля .....	331
Пароль должен отвечать требованиям сложности .....	331
Хранение паролей с использованием обратимого шифрования .....	331
Настройка политик блокировки учетной записи .....	332
Пороговое значение блокировки .....	332
Продолжительность блокировки учетной записи .....	332
Время до сброса счетчика блокировки.....	333
Настройка политик Kerberos.....	333
Принудительное ограничение входа пользователей .....	334
Максимальный срок жизни .....	334
Максимальная погрешность .....	334
Настройка политик прав пользователя .....	335
Настройка глобальных прав пользователей .....	335
Настройка локальных прав пользователей .....	337
Добавление учетной записи пользователя .....	338
Создание учетных записей пользователей домена .....	338
Создание локальных учетных записей .....	342
Добавление учетной записи группы .....	343
Создание глобальной группы .....	343
Создание локальной группы и назначение ее членов .....	345
Обработка членства глобальной группы .....	346
Индивидуальное управление членством в группе.....	347
Множественное управление членством в группе.....	347
Установка основной группы для отдельных пользователей и компьютеров .....	348
Реализация управляемых учетных записей.....	348
Создание и использование управляемых учетных записей служб.....	350
Настройка служб на использование управляемых учетных записей служб.....	351
Удаление управляемых учетных записей служб .....	352



Перемещение управляемых учетных записей служб .....	353
Использование виртуальных учетных записей .....	353
<b>Глава 9. Управление учетными записями пользователя и группы .....</b>	<b>355</b>
Управление контактной информацией пользователя .....	355
Установка контактной информации.....	355
Поиск пользователей и групп в Active Directory .....	358
Настройка параметров среды пользователя .....	359
Системные переменные среды .....	361
Сценарии входа.....	362
Назначение домашних каталогов .....	363
Установка параметров и ограничений учетной записи .....	364
Управление часами входа .....	364
Настройка времени входа.....	364
Принудительное отключение пользователей.....	365
Установка разрешенных для входа рабочих станций.....	366
Установка привилегий входящих звонков и VPN.....	367
Установка параметров безопасности учетной записи .....	369
Управление профилями пользователей.....	370
Локальные, перемещаемые и обязательные профили .....	371
Работа с перемещаемыми и обязательными профилями .....	371
Ограничение перемещаемых профилей .....	372
Создание локальных профилей .....	373
Создание перемещаемых профилей .....	373
Создание обязательных профилей.....	373
Использование утилиты <i>Система</i> для управления локальными профилями.....	374
Создание профиля вручную .....	375
Копирование существующего профиля в новую учетную запись пользователя .....	375
Копирование или восстановление профиля .....	376
Удаление локального профиля и назначение нового .....	376
Изменение типа профиля.....	377
Обновление учетных записей пользователя и группы.....	378
Переименование учетных записей пользователя и группы.....	379
Копирование учетных записей пользователя домена .....	380
Импорт и экспорт учетных записей .....	381
Удаление учетных записей пользователя и группы .....	382
Изменение и сброс паролей .....	382
Включение учетных записей пользователя .....	383
Учетная запись отключена .....	383
Учетная запись заблокирована.....	384
Срок действия учетной записи истек.....	384
Управление несколькими учетными записями.....	384
Установка профилей для нескольких учетных записей.....	386
Установка часов входа для нескольких учетных записей .....	387
Установка разрешенных для входа рабочих станций для множественных учетных записей.....	387
Установка свойств входа, пароля и срока действия для множественных учетных записей.....	387
Решение проблем с входом в систему .....	388
Просмотр и установка разрешений Active Directory.....	389

<b>ЧАСТЬ III. АДМИНИСТРИРОВАНИЕ ДАННЫХ WINDOWS SERVER 2012 .....</b>	<b>393</b>
<b>Глава 10. Управление файловыми системами и дисками.....</b>	<b>395</b>
Управление ролью <i>Файловые службы</i> .....	395
Добавление жестких дисков.....	399
Физические диски.....	399
Подготовка физического диска для использования.....	401
Использование оснастки <i>Управление дисками</i> .....	403
Сменные устройства хранения данных.....	406
Установка и проверка нового диска.....	407
Статус диска.....	408
Работа с базовыми, динамическими и виртуальными дисками .....	410
Использование базовых и динамических дисков.....	410
Особенности базовых и динамических дисков .....	411
Изменение типа диска .....	411
Конвертирование базового диска в динамический .....	412
Преобразование динамического диска обратно в базовый.....	413
Повторная активация диска .....	413
Повторная проверка дисков.....	413
Перемещение динамического диска в новую систему .....	413
Управление виртуальными дисками .....	414
Использование базовых дисков и разделов .....	415
Основы управления разделами .....	416
Создание разделов и простых томов.....	416
Форматирование разделов .....	419
Сжатие дисков и данных .....	420
Сжатие дисков.....	421
Сжатие каталогов и файлов .....	421
Декомпрессия сжатых дисков.....	422
Декомпрессия сжатых каталогов и файлов .....	422
Шифрование дисков и данных.....	422
Шифрование и файловая система EFS.....	423
Шифрование каталогов и файлов.....	424
Работа с зашифрованными файлами и папками.....	425
Настройка политики восстановления.....	426
Расшифровка файлов и каталогов .....	427
<b>Глава 11. Настройка томов и RAID-массивов.....</b>	<b>429</b>
Использование томов и массивов томов.....	430
Понимание базовых томов.....	430
Массивы томов .....	431
Создание томов и массивов томов .....	433
Удаление томов и массивов томов.....	436
Управление томами .....	436
Повышение производительности и отказоустойчивости с помощью RAID.....	436
Реализация RAID на Windows Server 2012 .....	437
Реализация RAID 0: чередование диска.....	437
Реализация RAID 1: зеркалирование диска .....	438
Создание зеркального набора в оснастке <i>Управление дисками</i> .....	440
Зеркалирование существующего тома .....	440
Реализация RAID 5: чередование диска с контролем четности.....	440
Создание чередующегося набора с четностью в оснастке <i>Управление дисками</i> .....	441

Управление RAID-массивами и восстановление после сбоя .....	442
Разделение зеркального набора .....	442
Ресинхронизация и восстановление зеркального набора .....	442
Восстановление зеркального системного тома для включения загрузки .....	443
Удаление зеркального набора .....	444
Восстановление чередующегося массива с контролем четности .....	444
Регенерация чередующегося массива с четностью .....	444
Стандартизированное управление хранилищами .....	445
Знакомство со стандартизированным управлением хранилищами .....	445
Работа со стандартизированным хранилищем .....	446
Создание пулов носителей и распределение пространства .....	448
Создание пространства хранилища .....	449
Создание виртуального диска в пространстве хранилища .....	450
Создание стандартного тома .....	452
Управление существующими разделами и дисками .....	453
Назначение буквы диска или путей .....	453
Изменение или удаление метки диска .....	454
Удаление разделов и дисков .....	455
Преобразование тома в NTFS .....	455
Синтаксис утилиты Convert .....	456
Использование утилиты Convert .....	456
Изменение размера раздела и тома .....	457
Автоматическое исправление ошибок диска .....	459
Проверка дисков вручную .....	461
Интерактивный запуск проверки дисков .....	463
Анализ и оптимизация дисков .....	463
<b>Глава 12. Общий доступ к данным, безопасность и аудит .....</b>	<b>467</b>
Использование и включение общего доступа к файлам .....	468
Настройка стандартного общего доступа к файлам .....	471
Просмотр существующих общих ресурсов .....	471
Создание общих папок в оснастке <i>Управление компьютером</i> .....	473
Создание общих папок в диспетчере серверов .....	476
Изменение параметров общей папки .....	479
Управление разрешениями общих ресурсов .....	480
Различные разрешения общего ресурса .....	480
Просмотр и настройка разрешений общего доступа .....	481
Управление существующими общими ресурсами .....	484
Особые общие ресурсы .....	484
Подключение к особым ресурсам .....	485
Просмотр сессий пользователя и компьютера .....	486
Управление сеансами и общими ресурсами .....	487
Завершение отдельных сеансов .....	487
Закрытие всех сеансов .....	488
Управление открытыми ресурсами .....	488
Закрытие открытого файла .....	488
Закрытие всех открытых файлов .....	489
Прекращение общего доступа .....	489
Настройка общих ресурсов NFS .....	489
Использование теневых копий .....	491
Что такое теневые копии .....	492
Создание теневых копий .....	492

Восстановление теневой копии .....	493
Восстановление предыдущего состояния всего тома .....	493
Удаление теневых копий .....	494
Отключение теневых копий .....	494
Подключение к сетевым дискам .....	495
Сопоставление сетевого диска .....	495
Отключение сетевого диска .....	496
Управление объектами, владением и наследованием .....	496
Объекты и диспетчеры объектов .....	496
Владение объектом и передача владения .....	497
Наследование объекта .....	497
Разрешения файла и папки .....	499
Подробности о разрешениях файлов и папок .....	499
Установка базовых разрешений файла и папки .....	503
Установка особых разрешений для файлов и папок .....	504
Установка разрешений на основе требований .....	507
Аудит системных ресурсов .....	509
Установка политик аудита .....	510
Аудит файлов и папок .....	511
Аудит реестра .....	513
Аудит объектов Active Directory .....	514
Использование, настройка и управление дисковых квот файловой системы NTFS .....	515
Понимание дисковых квот файловой системы NTFS или как используются квоты .....	516
Установка политик дисковых квот файловой системы NTFS .....	518
Включение дисковых квот на томах NTFS .....	520
Просмотр записей квот .....	522
Создание записей квоты .....	523
Удаление записей квот .....	524
Экспорт и импорт дисковых квот NTFS .....	525
Отключение дисковых квот NTFS .....	526
Использование, настройка и управление квотами диспетчера ресурсов .....	526
Понимание дисковых квот диспетчера ресурсов .....	526
Управление шаблонами квот .....	527
Создание квот диспетчера ресурсов .....	530
<b>Глава 13. Резервное копирование и восстановление данных .....</b>	<b>531</b>
Создание плана резервного копирования и восстановления .....	531
Нюансы плана резервного копирования .....	531
Основные типы резервного копирования .....	533
Дифференцированное и добавочное резервное копирование .....	534
Выбор устройств и носителей данных для резервного копирования .....	534
Общие решения для резервного копирования .....	535
Покупка и использование носителей резервной копии .....	536
Выбор утилиты для резервного копирования .....	537
Основы резервного копирования данных .....	538
Установка утилит резервного копирования и восстановления Windows .....	538
Введение в <i>Систему архивации данных Windows Server</i> .....	539
Знакомство с утилитами резервного копирования командной строки .....	542
Работа с командами Wbadmin .....	543
Команды общего назначения .....	544
Команды управления резервной копией .....	544
Команды управления восстановлением .....	545

Резервное копирование сервера.....	545
Настройка запланированных резервных копий.....	547
Изменение или остановка запланированного резервного копирования .....	550
Организация запланированного резервного копирования с помощью Wbadmin .....	551
Создание резервных копий вручную.....	552
Восстановление сервера после сбоя оборудования или процесса запуска .....	554
Восстановление после сбоя запуска.....	556
Запуск сервера в безопасном режиме.....	556
Резервное копирование и восстановление состояния системы .....	558
Восстановление Active Directory .....	559
Восстановление операционной системы и всего сервера .....	560
Восстановление приложений, несистемных томов, файлов и папок .....	562
Управление политикой восстановления шифрования .....	564
Сертификаты шифрования и политики восстановления .....	564
Настройка политики восстановления EFS .....	565
Резервное копирование и восстановление зашифрованных данных и сертификатов.....	566
Архивирование сертификата шифрования .....	567
Восстановление сертификата шифрования .....	567

## **ЧАСТЬ IV. АДМИНИСТРИРОВАНИЕ СЕТИ В WINDOWS SERVER 2012.....569**

<b>Глава 14. Управление TCP/IP-сетью .....</b>	<b>571</b>
Навигация по сетям в Windows Server 2012 .....	571
Управление сетью в Windows 8 и Windows Server 2012 .....	574
Установка сети TCP/IP .....	577
Настройка TCP/IP-сети.....	578
Настройка статического IP-адреса .....	578
Использование команды <i>ping</i> для проверки IP-адреса.....	579
Настройка статического IPv4- или IPv6-адреса .....	579
Настройка динамических и альтернативных IP-адресов.....	580
Настройка нескольких шлюзов.....	581
Настройка сети для Nupur-V .....	582
Управление сетевыми подключениями.....	583
Проверка состояния, скорости и активности сетевого подключения .....	583
Включение или отключение сетевых подключений.....	584
Переименование сетевых подключений .....	584
<b>Глава 15. Запуск DHCP-клиентов и серверов.....</b>	<b>585</b>
Обзор DHCP .....	585
Динамическая IPv4-адресация .....	585
Динамическая IPv6-адресация .....	587
Проверка назначения IP-адреса .....	589
Области адресов.....	589
Установка DHCP-сервера.....	590
Установка компонентов DHCP.....	591
Запуск и использование консоли DHCP .....	593
Подключение к удаленным DHCP-серверам .....	594
Запуск и остановка DHCP-сервера.....	594
Авторизация DHCP-сервера в Active Directory .....	595
Настройка DHCP-серверов.....	595
Настройка привязок сервера.....	595
Обновление DHCP-статистики .....	595

Аудит и устранение неисправностей DHCP .....	596
Интеграция DHCP и DNS.....	597
Интеграция DHCP и NAP.....	598
Как избежать конфликтов IP-адресов .....	601
Сохранение и восстановление конфигурации DHCP.....	602
Управление областями DHCP .....	602
Суперобласти: создание и управление .....	602
Создание суперобластей .....	603
Добавление областей в суперобласть .....	603
Удаление областей из суперобласти .....	603
Включение и отключение суперобласти .....	603
Удаление суперобласти .....	603
Создание областей и управление ими .....	604
Создание обычной области для IPv4-адресов .....	604
Создание обычной области для IPv6-адресов .....	606
Создание многоадресных областей .....	609
Установка параметров области .....	610
Изменение областей .....	612
Активация и деактивация областей .....	612
Включение протокола BOOTP .....	612
Удаление области .....	613
Настройка нескольких областей в сети .....	613
Создание и управление отказоустойчивыми областями.....	613
Создание отказоустойчивой области.....	613
Модификация или удаление отказоустойчивых областей .....	615
Управление пулом адресов, арендами и резервированием .....	616
Просмотр статистики области .....	616
Включение и настройка фильтрации MAC-адресов .....	616
Установка нового диапазона исключений .....	618
Резервирование DHCP-адресов .....	619
Освобождение адресов и аренды .....	620
Изменение свойств резервирования .....	620
Удаление аренды и резервирования .....	620
Резервное копирование и восстановление базы данных DHCP .....	621
Резервное копирование базы данных DHCP .....	621
Восстановление базы данных DHCP из резервной копии.....	621
Архивация и восстановление для перемещения базы данных DHCP на новый сервер.....	622
Принудительное регенерирование базы данных DHCP .....	622
Согласование аренд и резервирования .....	623
<b>Глава 16. Оптимизация DNS .....</b>	<b>625</b>
Общие сведения о DNS .....	625
Интеграция Active Directory и DNS.....	625
Включение DNS в сети.....	627
Настройка разрешения имен на DNS-клиентах.....	629
Установка DNS-серверов .....	631
Установка и настройка службы <i>DNS-сервер</i> .....	631
Настройка основного DNS-сервера.....	634
Настройка дополнительного DNS-сервера.....	636
Настройка зон обратного просмотра .....	637
Настройка глобальных имен.....	639

Управление DNS-серверами .....	640
Добавление и удаление серверов для управления.....	640
Запуск и остановка DNS-сервера.....	641
Использование DNSSEC и подпись зон.....	641
Создание дочерних доменов в зонах.....	643
Создание дочерних доменов в отдельных зонах.....	644
Удаление домена или подсети .....	645
Управление записями DNS .....	645
Добавление записей адреса и указателя.....	646
Добавление записи указателя позже .....	647
Добавление DNS-псевдонимов с помощью CNAME .....	647
Добавление почтовых серверов.....	647
Добавление серверов имен.....	648
Просмотр и обновление DNS-записей .....	649
Обновление свойств зоны и записи SOA .....	649
Изменение записи SOA .....	650
Разрешение и запрещение передачи зоны .....	651
Уведомление дополнительных серверов об изменениях.....	653
Установка типа зоны .....	654
Включение и выключение динамических обновлений.....	654
Управление конфигурацией DNS-сервера и безопасностью.....	654
Включение и отключение IP-адресов для DNS-сервера.....	655
Управление доступом к внешним DNS-серверам .....	655
Создание серверов без пересылки и кэширующих серверов.....	656
Создание серверов пересылки.....	656
Настройка сервера условной пересылки .....	656
Включение и отключение протоколирования событий.....	657
Использование журнала отладки для отслеживания активности DNS .....	657
Мониторинг DNS-сервера.....	658
<b>Предметный указатель.....</b>	<b>661</b>

# Введение

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

Хорошая новость заключается в том, что операционная система Windows Server 2012 построена на той же базе, что и Microsoft Windows 8. Это означает, что можно применить большую часть знаний о Windows 8 к Windows Server 2012, в том числе и то, как Windows работает с сенсорным пользовательским интерфейсом. Вряд ли Windows Server 2012 будет устанавливаться на компьютеры с сенсорным интерфейсом, но можно управлять Windows Server 2012 с такого компьютера. Понимание принципов работы с сенсорным интерфейсом является залогом вашего успеха. Но в этой книге также рассмотрена и работа традиционным способом — с помощью мыши и клавиатуры.

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

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



◆ **Растяжение.** Коснитесь элемента двумя пальцами, а затем разведите пальцы. Этот жест увеличивает масштаб элемента.

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

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

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

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

## Для кого предназначена эта книга

Книга охватывает все редакции Windows Server 2012 и предназначена для:

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

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

Я также предполагаю, что читатель знаком с командами и процедурами Windows, а также с интерфейсом пользователя этой ОС. Если есть необходимость в изучении основ Windows, нужно обратиться к другим ресурсам.

## Организация книги

Рим строился не за один день, и эта книга не рассчитана на то, что она будет прочитана за один день, за одну неделю и даже за один месяц. В идеале, эту книгу нужно читать в собственном темпе, каждый день понемногу, в процессе работы с Windows Server 2012. Эта книга состоит из 16 глав. Главы выстроены в логической последовательности, начиная от задач планирования и развертывания до задач обслуживания и настройки.

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

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

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

# **часть I**

## **Основы администрирования Windows Server 2012**

- Глава 1.** Обзор администрирования Windows Server
- Глава 2.** Управление серверами на базе Windows Server 2012
- Глава 3.** Мониторинг процессов, служб и событий
- Глава 4.** Автоматизация административных задач, политики и процедуры
- Глава 5.** Улучшение безопасности компьютера

# ГЛАВА 1

## Обзор администрирования Windows Server

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

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

## Windows Server 2012 и Windows 8

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

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

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

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

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

### **Дополнительная информация**

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

Подобно Windows 8, Windows Server 2012 обладает следующими возможностями.

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

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

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

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

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

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

## Знакомство с Windows Server 2012

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

Windows Server 2012 — строго 64-разрядная операционная система. В этой книге 64-битными системами называются системы, разработанные для архитектуры x64. Поскольку раз-

---

<sup>1</sup> Уильям Р. Станек. Microsoft® Windows 8. Справочник администратора. — СПб.: Microsoft Press, БХВ-Петербург, 2013.

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

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

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

#### ПРИМЕЧАНИЕ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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



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

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

#### **ПРИМЕЧАНИЕ**

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

## Параметры управления питанием

Для управления питанием важно сфокусироваться на следующем:

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

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

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

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

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

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

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

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

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

### **Дополнительная информация**

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

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

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

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

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

**Рис. 1.1.** Понимание состояний процессоров

### **ПРАКТИЧЕСКИЙ СОВЕТ**

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

---

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

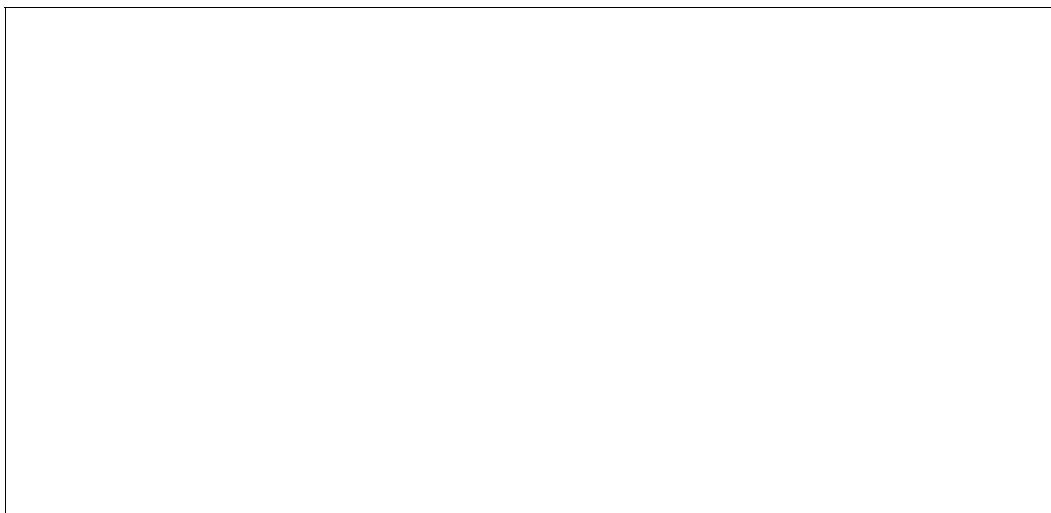
в зависимости от состояния сна, а потребление энергии меньше, чем в состоянии G0. Состояние G2 (также называется состоянием сна S5) — "мягкое" выключение, когда операционная система не выполняется, задержка длинная, а потребляемая энергия близка к нулю. Состояние G3, состояние механического выключения,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

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

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

## Сетевые утилиты и протоколы

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



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

## Сетевые настройки

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

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

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

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

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

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

## Работа с сетевыми протоколами

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

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

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

#### ПРИМЕЧАНИЕ

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

#### ПРАКТИЧЕСКИЙ СОВЕТ

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

32-битные IPv4-адреса обычно представлены четырьмя отдельными десятичными значениями, например 127.0.0.1 или 192.168.10.52. Четыре десятичных значения также называются *октетами*, поскольку каждое представляет 8 бит в 32-битном числе. В IPv4-адресации часть IP-адреса представляет идентификатор сети, а другая часть — идентификатор компьютера. IPv4-адрес узла и внутренний адрес машины (MAC-адрес) сетевого адаптера никак не связаны друг с другом.

При IPv6-адресации используются 128-битные адреса, которые делятся на восемь 16-битных блоков, разделенных двоеточиями. Каждый 16-битный блок представлен в шестнадцатеричной форме, например, `FEC0:0:0:02BC:FF:FE0B:FE4F:961D`. В обычной одноадресной IPv6-адресации первые 64 бита представляют идентификатор сети, а последние 64 бита — сетевой интерфейс. Поскольку многие блоки в IPv6-адресах равны 0, последовательность нулевых блоков может быть заменена символами `::` — так называемым двойным двоеточием. С помощью двойного двоеточия нулевые блоки в предыдущем адресе можно сжать так: `FEC0::02BC:FF:FE0B:FE4F:961D`. Три и более нуля сжимаются так же, например, `FFE8:0:0:0:0:0:1` превратится в `FFE8::1`.

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

## Контроллеры домена, рядовые серверы и службы домена

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

## Работа с Active Directory

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

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

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

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

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

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

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



## Контроллеры домена только для чтения

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

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

### **СОВЕТ**

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

## Перезапускаемые доменные службы Active Directory

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

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

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

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

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

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

## Сервисы разрешения имен

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

Современные операционные системы Windows поддерживают три системы разрешения имен:

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

В следующих разделах мы рассмотрим все эти три системы.

## Система доменных имен

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

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

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

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

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

Важно понимать разницу между полной и частичной интеграцией.

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

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

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

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

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

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

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

## Службы имен Интернета для Windows

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

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

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

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

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

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

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

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

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

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

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

## Протокол LLMNR

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

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

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

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

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

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

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

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

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

### **ПРАКТИЧЕСКИЙ СОВЕТ**

По умолчанию LLMNR включен на компьютерах, работающих под управлением Windows 7 и более поздних версий. Отключить LLMNR можно с помощью реестра. Для этого установите следующий параметр реестра в 0: HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\EnableMulticast.

Для отключения LLMNR для определенного сетевого интерфейса создайте и установите в 0 следующий параметр реестра: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\AdapterGUID\EnableMulticast.

Здесь AdapterGUID — глобальный уникальный идентификатор сетевого адаптера, для которого нужно отключить LLMNR. Чтобы включить LLMNR снова, установите это значение в 1. Также можно управлять LLMNR с помощью групповой политики.

## **Часто используемые инструменты**

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

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

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

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

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

## Windows PowerShell 3.0

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

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

### ПРАКТИЧЕСКИЙ СОВЕТ

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

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

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



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

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

```
powershell
```

### ПРИМЕЧАНИЕ

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

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

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

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

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

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

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

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

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

### ПРАКТИЧЕСКИЙ СОВЕТ

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

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

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

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

## Служба удаленного управления Windows

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

### Включение и использование WinRM

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

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

```
get-service winrm
```

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

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

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

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

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

```
Enable-PSRemoting -force
```

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

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

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

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

Здесь *RemoteComputer* — имя удаленного компьютера, например:

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

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

```
winrm quickconfig
```

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

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

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

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

## Настройка WinRM

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

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

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

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

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

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

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

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

#### Листинг 1.1. Пример конфигурации слушателей

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

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

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

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

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

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

или

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

Следующие команды включают и отключают базовую аутентификацию клиента:

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

или

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

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

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

или

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

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

## ГЛАВА 2

# Управление серверами на базе Windows Server 2012

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

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

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

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

## Роли серверов, службы ролей и компоненты Windows Server 2012

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

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

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

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

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

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

Таблица 2.1 (продолжение)

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



Таблица 2.1 (окончание)

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

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

Таблица 2.2. Основные компоненты ОС Windows Server 2012

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

Таблица 2.2 (продолжение)

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

Таблица 2.2 (продолжение)

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

Таблица 2.2 (окончание)

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

**ПРИМЕЧАНИЕ**

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

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

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

```
regsvr32 mylibs.dll
```

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

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

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

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

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

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

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

## Обзор установки основных серверных компонентов

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

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

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

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

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

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

---

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

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

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

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

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

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

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



Таблица 2.3 (окончание)

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

## Установка Windows Server 2012

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

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

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

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

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

## Чистая установка

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

Для осуществления чистой установки Windows Server 2012 выполните следующие действия:

1. Запустите программу установки, используя один из методов.

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

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

#### **ПРИМЕЧАНИЕ**

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

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

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

- Когда у компьютера имеется несколько дисков или один диск с несколькими разделами, нужно либо выбрать существующий раздел для установки операционной системы, либо создать новый раздел. Как можно создать новый раздел, будет показано в *разд. "Создание, форматирование, удаление и расширение разделов диска во время установки"* далее в этой главе.
  - Если диск не инициализирован или BIOS компьютера не поддерживает запуск операционной системы с выбранного диска, нужно инициализировать диск, создав один или более разделов на этом диске. Нельзя выбрать диск, использующий файловую систему FAT/FAT32. Также нельзя отформатировать диск в этой файловой системе. Если раздел, на который планируется установить Windows Server, отформатирован как FAT32, нужно конвертировать его в NTFS. При работе с этой страницей программы установки можно получить доступ к командной строке для осуществления необходимых предустановочных задач (см. *разд. "Создание, форматирование, удаление и расширение разделов диска во время установки"* далее в этой главе).
9. Если выбранный раздел содержит установку предыдущей версии Windows, инсталлятор сообщит вам, что существующие настройки пользователя и приложений будут перемещены в папку Windows.old и нужно будет скопировать эти параметры в новую установку Windows. Нажмите кнопку **ОК**.
10. Нажмите кнопку **Далее**. Инсталлятор начнет установку операционной системы. Во время этого процесса инсталлятор скопирует полный образ диска Windows Server 2012 на выбранный вами диск/раздел, а затем развернет его. После этого инсталлятор установит дополнительные компоненты на основании конфигурации вашего компьютера и обнаруженных аппаратных средств. Этот процесс требует нескольких автоматических перезагрузок. После завершения установки будет загружена операционная система и можно осуществить начальную настройку, например, установить пароль администратора и имя сервера.

### **ПРАКТИЧЕСКИЙ СОВЕТ**

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

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

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

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

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

## Обновление существующей системы

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

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

### ПРИМЕЧАНИЕ

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

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

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

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

## Дополнительные административные задачи во время установки

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

### Использование командной строки во время установки

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

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

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

Таблица 2.4 (продолжение)

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

Таблица 2.4 (продолжение)

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



Таблица 2.4 (окончание)

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

## Принудительное удаление раздела диска во время установки

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

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

## Загрузка драйверов устройств во время установки

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

Для загрузки драйвера диска выполните следующие действия:

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

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

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

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

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

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

### Создание раздела диска во время установки

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

Для создания нового раздела выполните следующие действия:

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

После создания раздела его нужно отформатировать для продолжения установки.

### Форматирование раздела диска во время установки

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

Для форматирования раздела выполните следующие действия:

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

### Удаление раздела диска во время установки

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

Для удаления раздела выполните следующие действия:

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

### Расширение раздела диска во время установки

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

Для расширения раздела выполните следующие действия:

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

## Изменение типа установки

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

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

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

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

## Конвертирование полной установки и установки с минимальным графическим интерфейсом

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

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

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

### СОВЕТ

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

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

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

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

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

## Конвертирование установки с основными серверными компонентами

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

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

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

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

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

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

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

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

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

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

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

## Управление ролями, службами ролей и компонентами

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

### Начальная настройка

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

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

#### ПРИМЕЧАНИЕ

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

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

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

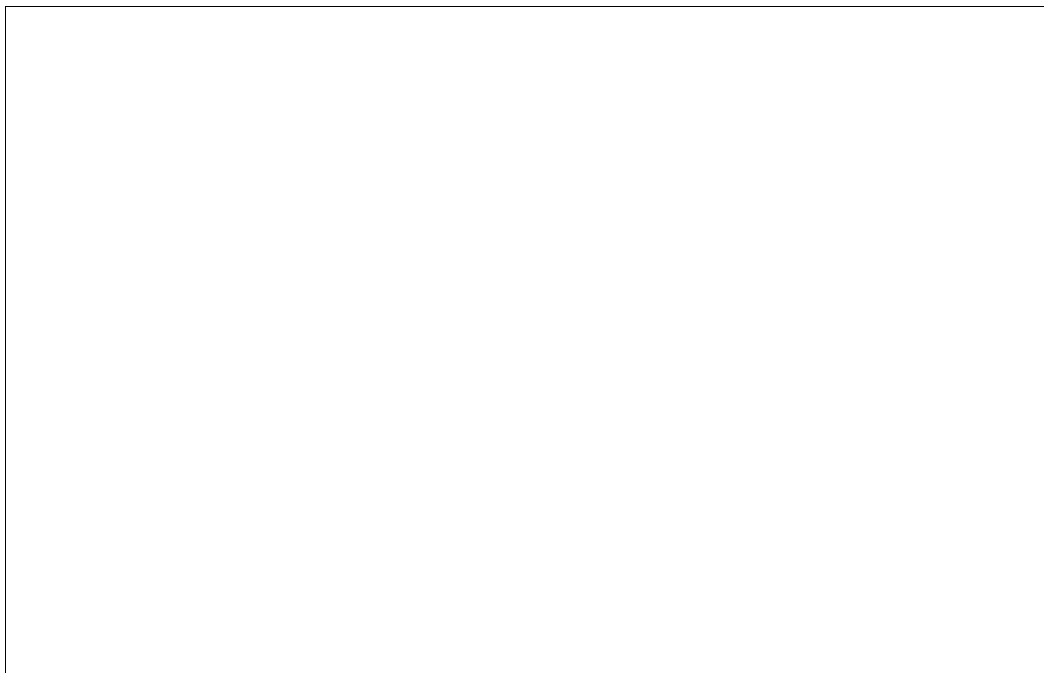


Рис. 2.1. Используйте Панель мониторинга для общего администрирования

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

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

### **СОВЕТ**

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

### **ПРАКТИЧЕСКИЙ СОВЕТ**

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

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

Информация о локальном сервере распределена по нескольким панелям.

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



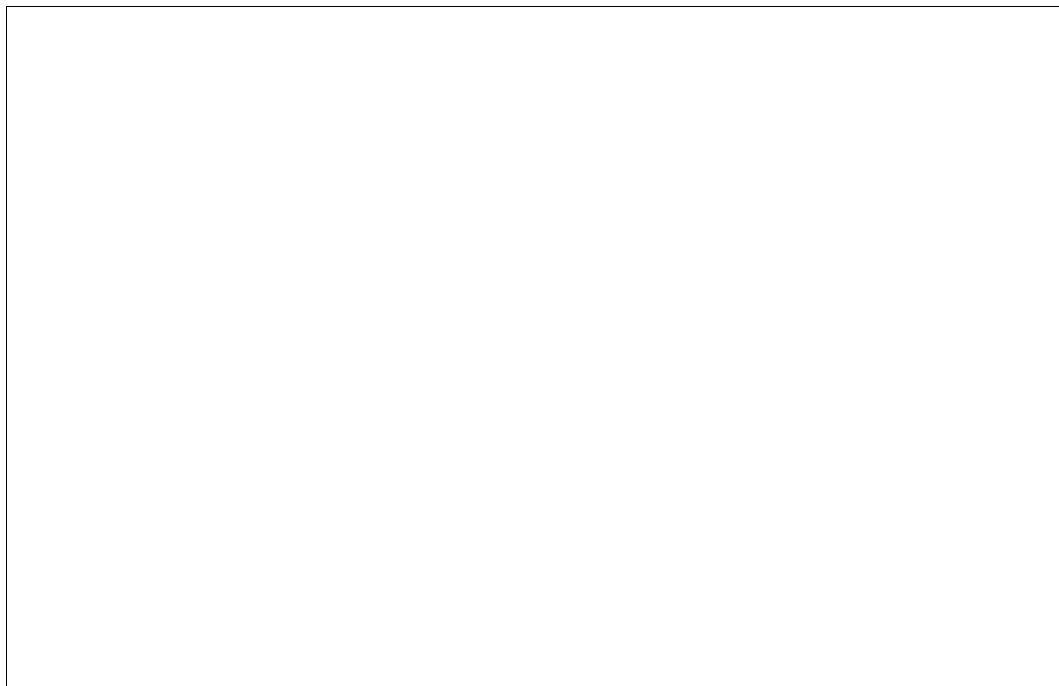


Рис. 2.2. Управление свойствами локального сервера

- ◆ **РОЛИ И КОМПОНЕНТЫ (ROLES AND FEATURES)** — выводит список ролей и компонентов в порядке их установки на сервер. Для удаления роли или компонента щелкните правой кнопкой мыши (или нажмите и удерживайте палец) и выберите команду **Удалить роль или компонент (Remove role or feature)**.
  - ◆ **СЛУЖБЫ (SERVICES)** — выводит список служб, запущенных на сервере (по имени, статусу и типу запуска). Для изменения статуса службы используйте контекстное меню.
- Панель **СВОЙСТВА (PROPERTIES)** позволяет произвести начальную настройку сервера. Для быстрой настройки доступны следующие свойства.
- ◆ **Имя компьютера/Рабочая группа (Computer Name/Domain)** — отображает имя компьютера и домена. Щелкните по соответствующей ссылке, чтобы отобразить окно **Свойства системы (System Properties)** с активной вкладкой **Имя компьютера (Computer Name)**. Затем можно изменить имя компьютера и имя домена, нажав кнопку **Изменить (Change)**. После чего введите имя компьютера и домена и нажмите кнопку **ОК**. По умолчанию серверам назначаются случайным образом сгенерированные имена, и они настраиваются как часть рабочей группы WORKGROUP. Вызвать окно **Свойства системы** можно с помощью Панели управления. Для этого запустите утилиту **Система (System)**, когда выбрано представление **Крупные значки (Large Icons)** или **Мелкие значки (Small Icons)**. Затем щелкните по ссылке **Изменить параметры (Change Settings)** напротив параметра **Компьютер (Computer Name)**. Откроется окно **Свойства системы** с активной вкладкой **Имя компьютера**.
  - ◆ **Программа улучшения качества программного обеспечения (Customer Experience Improvement Program)** — определяет, будет ли сервер принимать участие в Программе улучшения качества программного обеспечения (Customer Experience Improvement

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

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

#### **ПРАКТИЧЕСКИЙ СОВЕТ**

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

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

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

#### **ПРИМЕЧАНИЕ**

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

## **Основные компоненты диспетчера серверов и двоичные файлы**

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

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

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

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

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

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

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

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

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

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

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

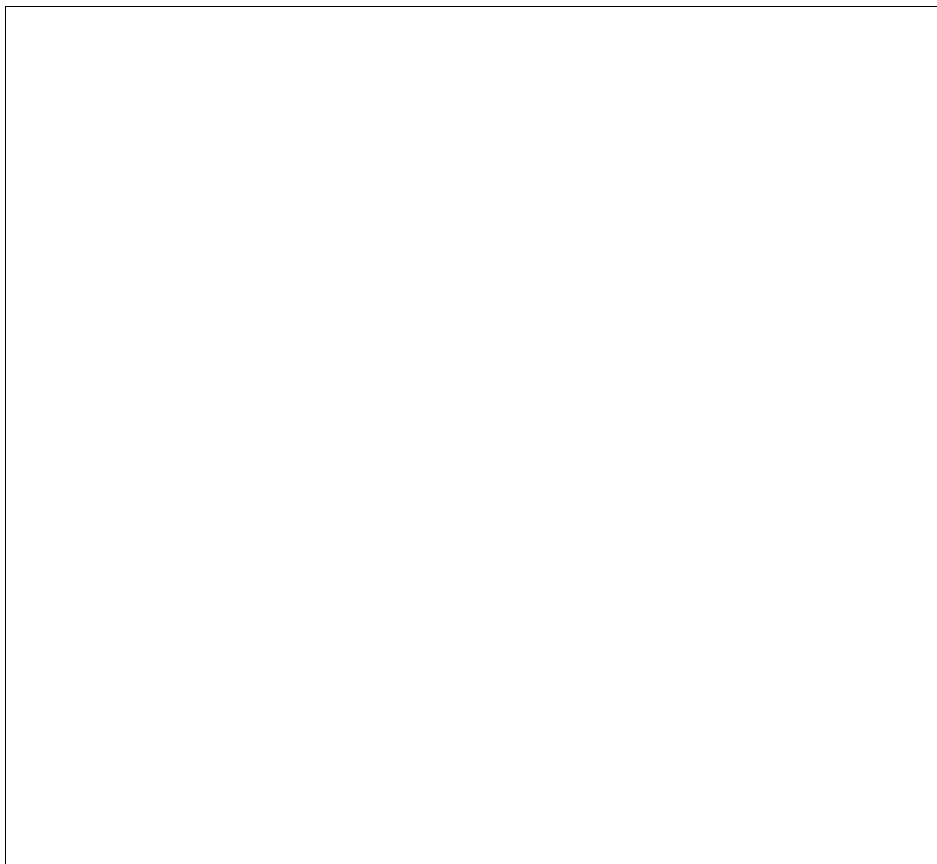
Помните, что указанный вами путь используется только для полезных данных, не найденных в папке Windows Side-By-Side (WinSxS) сервера. На многих крупных предприятиях в сети доступен образ Windows Server 2012, но можно смонтировать дистрибутивный диск

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

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

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

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



**Рис. 2.3.** Контролируйте установку компонентов с помощью групповой политики

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

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

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

## Удаленное управление серверами

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

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

Средства удаленного администрирования сервера для Windows 8 можно получить через центр загрузок Microsoft — Download Center ([download.microsoft.com](http://download.microsoft.com)). Обратите внимание, что есть разные версии для систем x86 и x64.

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

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

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

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

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

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

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

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

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

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

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

#### **ПРИМЕЧАНИЕ**

Для включения удаленного управления воспользуйтесь следующей командой, которую нужно ввести в командной строке с правами администратора:

```
configure-SMRemoting.exe -enable
```

**ПРИМЕЧАНИЕ**

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

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

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

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

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

## Подключение и работа с удаленными серверами

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

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



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

2. В окне **Добавление серверов** есть две панели:

- **Active Directory** (выбрана по умолчанию) — позволяет ввести короткое или полное имя удаленного сервера, работающего под управлением Windows Server. Введите имя сервера и нажмите кнопку **Найти** (Find Now);
- **DNS** — позволяет добавить серверы по имени или IP-адресу. Введите имя или IP-адрес и нажмите кнопку **Поиск** (Search).

3. Дважды щелкните на найденном сервере для помещения его в список **Выбрано** (Selected).

4. Повторите действия 2—3 для добавления других серверов. Нажмите кнопку **ОК**.

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

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

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

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

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

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

Чтобы создать группу серверов, выполните следующие действия:

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



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

2. Введите имя группы. Используйте панели и параметры, предназначенные для добавления серверов в группы. Помните о следующем.

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

3. Нажмите кнопку **ОК** для создания группы сервера.

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

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

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

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

```
enter-psession server85 -credential williams
```

## Добавление и удаление ролей, ролевых служб и компонентов

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

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

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

### СОВЕТ

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

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

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

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

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

1. В консоли **Диспетчер серверов** в меню **Управление** выберите команду **Добавить роли и компоненты** (Add Roles And Features). Будет запущен мастер добавления ролей и компонентов. Если мастер отобразит страницу **Перед началом работы** (Before You Begin), прочитайте вступительный текст и затем нажмите кнопку **Далее**. Можно отказаться от просмотра этой страницы при каждом запуске мастера, установив флажок **Пропускать эту страницу по умолчанию** (Skip This Page By Default) перед нажатием кнопки **Далее**.
2. На странице **Выбор типа установки** (Installation Type) по умолчанию отмечен переключатель **Установка ролей или компонентов** (Role-Based Or Feature-Based Installation). Нажмите кнопку **Далее**.
3. На странице **Выбор целевого сервера** (Server Selection) можно указать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите сервер из пула серверов либо сервер, на котором можно смонтировать виртуальный жесткий диск (VHD). При добавлении ролей и компонентов на VHD нажмите кнопку **Обзор** (Browse), а затем используйте окно **Обзор виртуальных жестких дисков** (Browse For Virtual Hard Disks) для выбора вашего VHD. Когда будете готовы продолжить, нажмите кнопку **Далее**.

#### **ПРИМЕЧАНИЕ**

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

4. На странице **Выбор ролей сервера** (Server Roles) выберите одну или несколько ролей для установки. Если для установки роли требуются дополнительные компоненты, будет отображено дополнительное диалоговое окно. Нажмите кнопку **Добавить компоненты** (Add Features) для добавления необходимых компонентов в инсталляцию сервера. Нажмите кнопку **Далее** для продолжения.
5. На странице **Выбор компонентов** (Features) выберите один или несколько компонентов для установки. Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, будет отображено соответствующее диалоговое окно. Нажмите кнопку **Добавить компоненты** для закрытия этого окна и установки требуемых компонентов на сервер. По окончании выбора компонентов нажмите кнопку **Далее**.
6. В случае с некоторыми ролями будут показаны дополнительные страницы мастера, на которых нужно будет предоставить дополнительную информацию относительно использования и настройки роли. Также можно установить дополнительные ролевые службы

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

7. На странице **Подтверждение установки компонентов** (Confirm) щелкните по ссылке **Экспорт параметров конфигурации** (Export Configuration Settings) для создания отчета установки, который можно просмотреть в Internet Explorer.
8. Если сервер, на котором необходимо установить роли или компоненты не обладает всеми необходимыми двоичными файлами, сервер получит их через Центр обновления Windows (по умолчанию) или из местоположения, указанного групповой политикой. Можно также указать альтернативный источник для файлов. Для этого щелкните по ссылке **Указать альтернативный исходный путь** (Specify An Alternate Source Path), в появившемся окне укажите альтернативный путь и нажмите кнопку **ОК**. Например, образ Windows смонтирован и сделан доступным на локальном сервере, как было показано в разд. "Основные компоненты диспетчера серверов и двоичные файлы" ранее в этой главе, можно ввести альтернативный путь в виде c:\mountdir\windows\winsxs. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer20120\ . Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2-12\install.wim:4.
9. После просмотра параметров установки и их сохранения нажмите кнопку **Установить** (Install) для начала процесса установки. Страница **Ход установки** (Installation Progress) позволяет отслеживать процесс инсталляции. Если мастер бы закрыт, нажмите значок **Уведомления** (Notifications) в диспетчере серверов, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.
10. О завершении установки выбранных ролей и компонентов сообщит страница **Ход установки**. Просмотрите подробности установки и убедитесь, что все фазы инсталляции завершены успешно. Обратите внимание на любые действия, которые могут потребоваться для завершения установки, например, перезагрузка сервера или осуществление дополнительных инсталляционных задач. Если какая-либо часть установки не увенчалась успехом, запомните причину сбоя. Просмотрите записи диспетчера сервера, чтобы понять суть проблемы, и примите соответствующие корректирующие действия.

#### **ПРИМЕЧАНИЕ**

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

Для удаления роли сервера или компонента выполните следующие действия:

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

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

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

## Управление свойствами системы

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

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

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

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

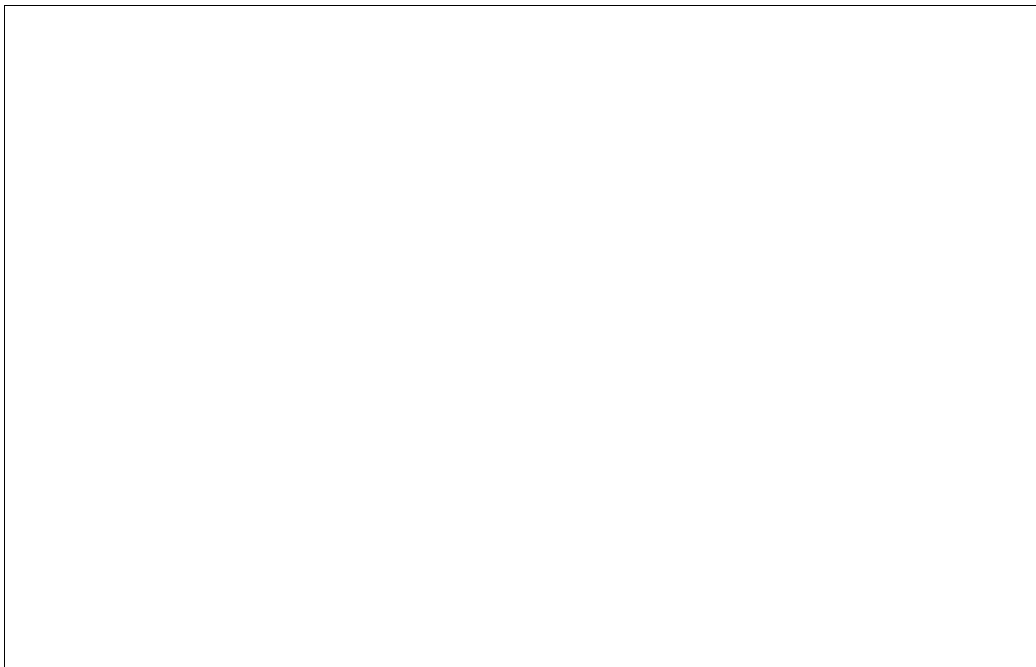


Рис. 2.5. Используйте консоль **Система** для просмотра и управления свойствами системы

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

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

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

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

**ПРИМЕЧАНИЕ**

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

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

## Вкладка **Имя компьютера**

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

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

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

Для изменения имени компьютера выполните следующие действия:

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



## Вкладка Оборудование

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

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

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

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

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

## Вкладка Дополнительно

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

### Настройка быстродействия Windows

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

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

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

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

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

## Настройка быстродействия приложений

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

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

## Настройка виртуальной памяти

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

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

### **ПРАКТИЧЕСКИЙ СОВЕТ**

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

Настроить виртуальную память можно так:

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



Рис. 2.6. Виртуальная память расширяет объем ОЗУ системы

#### ПРИМЕЧАНИЕ

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

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

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

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

**ПРИМЕЧАНИЕ**

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

## Настройка предотвращения выполнения данных

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

**ПРИМЕЧАНИЕ**

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

### Использование и настройка DEP

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

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

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

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

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

## DEP-совместимость

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

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

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

## Настройка системных и пользовательских переменных среды

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

### Создание переменной среды

Для создания переменной среды выполните следующие действия:

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

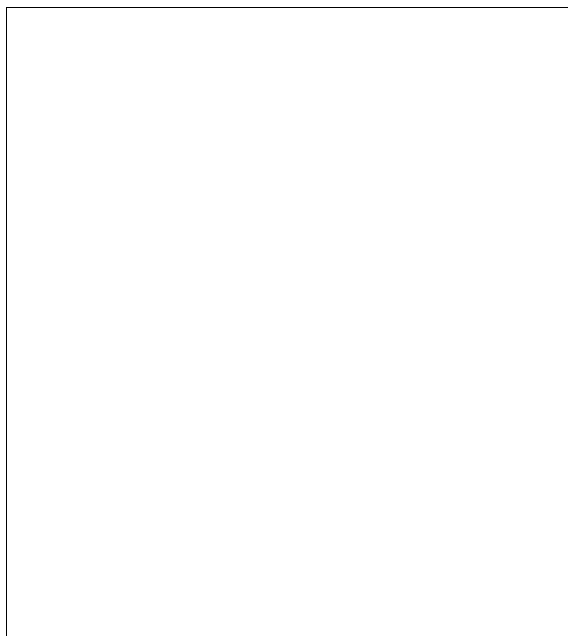


Рис. 2.7. Пользовательские и системные переменные среды в окне **Переменные среды**

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

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

### Редактирование переменной среды

Для редактирования значения переменной среды выполните такие действия:

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

### Удаление переменной среды

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

#### **ПРИМЕЧАНИЕ**

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

## Настройка загрузки и восстановления системы

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

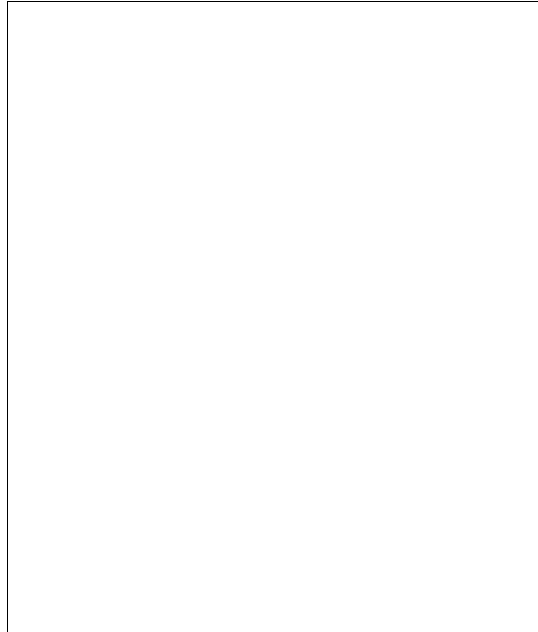


Рис. 2.8. Параметры загрузки и восстановления системы в окне **Загрузка и восстановление**

### Установка параметров загрузки

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

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

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

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



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

### Определение параметров восстановления

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

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

#### ПРИМЕЧАНИЕ

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

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

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

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

#### РЕКОМЕНДАЦИИ

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

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

## **Вкладка *Удаленный доступ***

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

## ГЛАВА 3

# Мониторинг процессов, служб и событий

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

## Управление приложениями, процессами и производительностью

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

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

## Диспетчер задач

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

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

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

#### ПРИМЕЧАНИЕ

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

В следующих разделах описано, как работать с диспетчером задач.

## Просмотр и работа с процессами

У диспетчера задач есть два представления:

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

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

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

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

#### ПРИМЕЧАНИЕ

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

#### ПРАКТИЧЕСКИЙ СОВЕТ

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