Операционные системы Windows Server 2008 R2 и Windows 7 официально пришли на смену паре Windows 2008 и Windows Vista. Новые системы построены на том же коде, и в общем архитектура осталась неизменной, поэтому большая часть материала будет актуальна и для более ранних версий, тем не менее в них сделаны действительно полезные усовершенствования, которые позволят администратору получить легко управляемую, гибкую в настройках и безопасную систему.

Новое в Windows 7 и Windows Server 2008 R2

Операционные системы Windows Server 2008 R2 и Windows 7 принадлежат к семейству NT 6.x, получившему при разработке кодовое имя «Longhorn». Поэтому, чтобы понять их возможности, необходимо начать с изучения родоначальников семейства.

ПРИМЕЧАНИЕ

В дальнейшем при изложении материала будем ориентироваться на серверные версии операционных систем, так как именно они несут большую функциональность. Поэтому для краткости клиентские операционные системы Windows Vista и Windows 7 будут опускаться, а там, где это необходимо, будет делаться соответствующее замечание.

Разработка «Longhorn» (NT 6.x) продолжалась несколько лет. Первая тестовая (Beta 1) версия была представлена еще в 2005 году. Окончательный релиз новых систем состоялся: Windows Vista — в январе 2007 года, серверной Windows Server 2008 — в конце февраля 2008 года. Эти операционные системы призваны заменить Windows 2003 и Windows XP, срок прекращения поддержки которых датирован июлем 2010 и апрелем 2012 года соответственно. Почти через два года (22 октября 2009 года) были представлены Windows Server 2008 R2 и Windows 7.

ПРИМЕЧАНИЕ

Операционную систему Microsoft Windows XP считают одной из самых удачных систем, разработанных этой корпорацией, в первую очередь благодаря стабильности в работе, нетребовательности к ресурсам. Количество проданных копий данной ОС превысило 500 млн. В итоге пользователи выступили с протестом об окончании ее поддержки. Поэтому было объявлено, что поддержка Windows XP с пакетом обновления SP2 (SP3) будет продлена до 2014 года, затем появилась информация о возможности увеличения срока до 2020 года.

Начнем с того, что ядро операционной системы (ntoskrnl.exe) изначально поддерживает многопроцессорные системы, причем Windows Server 2008 — это последняя 32-разрядная операционная система. Вышедшая ей на замену Windows Server 2008 R2 представлена только в 64-битной версии, что вполне логично, так как последние версии процессоров исключительно 64-битные.

ПРИМЕЧАНИЕ

Поддержка 32-битных приложений в R2 осталась и реализована при помощи слоя эмуляции WOW64 (Windows on Windows64).

Претерпел существенные усовершенствования диспетчер памяти, в результате чего повысилась производительность операционной системы. Новая система избавилась от ограничения в 64 Кбит на объем операций ввода-вывода, доставшегося ей в наследство еще от первой NT, и при упреждающем чтении диспетчер кэша считывает вдвое больший объем данных. Это позволило ускорить работу с файлами большого объема. Также оптимизирован алгоритм работы с файлом подкачки.

ПРИМЕЧАНИЕ

Изначально для Windows Server 2008 R2 предусматривалось более громкое название — Windows Server 7, но на конференции PDC 2008 было объявлено, что новинка будет называться именно Windows Server 2008 R2 и ее следует рассматривать не как основной, а как промежуточный релиз. Теперь основные (major) релизы серверных версий системы будут выходить раз в пять лет, промежуточный релиз — через два года после основного.

Одна из главных новинок — появление версии сервера без графической оболочки (Server Core). Присутствие графической среды в серверной версии операционной системы давно уже вызывало критику у администраторов. Ведь наличие лишних приложений и служб на сервере, выполняющем критические задачи, увеличивало количество потенциальных уязвимостей и упрощало задачу взломщику, не говоря уже о том, что графика требовала дополнительных системных ресурсов.

ПРИМЕЧАНИЕ

Подробную информацию о Windows Server 2008 R2 и Windows 7 можно получить на различных ресурсах сайта корпорации Microsoft (http://www.microsoft.com/windowsserver2008/ru/ru/default.aspx, http://www.microsoft.com/rus/windows/enterprise/) или в библиотеке TechNet (http://technet.microsoft.com/ru-ru/).

Вторым нововведением в Windows Server 2008 стал контроллер доменов только для чтения (Read-Only Domain Controller — RODC). Данный контроллер предназначен в первую очередь для использования в филиалах, где крайне сложно обеспечить физическую безопасность контроллера домена. Для этого RODC содержит незаписываемую и доступную только для чтения копию базы данных Active Directory со всеми объектами и атрибутами.

Полностью переписан стек межсетевых протоколов TCP/IP, в который также внедрен протокол IPv6. Поддержка SMB 2.0 означает ускоренное копирование файлов по сети за счет пакетной отправки данных, то есть подтверждение дается на группу, а не на каждый пакет, как это было в старой версии протокола SMB 1.0. Изменения в стеке протоколов TCP/IP позволяют устанавливать динамический

размер буфера, тогда как в SMB 1.0 размер буфера был фиксированным (64 Кбайт), что замедляло передачу больших потоков данных. В результате средняя скорость копирования файлов увеличилась приблизительно в три раза. Также SMB 2.0 различает символические ссылки NTFS и позволяет использовать их в названиях сетевых ресурсов.

ПРИМЕЧАНИЕ

SMB (сокр. от англ. Server Message Block) — сетевой протокол прикладного уровня, используемый для удаленного доступа к сетевым ресурсам локальной сети (файлам, принтерам). Реализован в компоненте Microsoft Windows Network (Сети Microsoft Windows) и File and Printer Sharing (Совместное использование файлов и принтеров).

При обмене данными с операционными системами нового поколения (не ниже Vista) протокол SMB 2.0 устанавливается автоматически, иначе используется устаревшая версия (1.0).

Не менее интересное нововведение — появление службы сетевой политики и доступа (Network Policy and Access Service), пришедшей на смену IAS (Internet Authentication Server). Одним из ее основных компонентов является защита доступа к сети (Network Access Protection — NAP), применение которого позволяет гарантировать, что узел, подключающийся к сети, удовлетворяет требованиям безопасности и установленным политикам — независимо от того, работает ли антивирусное и антишпионское программное обеспечение, обновлены ли их базы, установлены ли последние заплатки, включен ли межсетевой экран и т. д. На основании этих сведений компьютер получает полный или ограниченный доступ в сеть.

Переработаны входящие в состав операционной системы утилиты, например DCPROMO и Просмотр событий, появились новые инструменты управления в Диспетчере сервера (рис. 1.1), обновились инструменты развертывания Windows AIK (Windows Automated Installation Kit — пакет автоматической установки Windows).

Нужная функциональность сервера наращивается за счет установки ролей и компонентов. При выборе большинства пунктов запускается простой мастер, который за несколько шагов поможет быстро развернуть нужную функциональность. В комплекте поставляется 16 ролей, то есть задач, на которые ориентирован конкретный сервер (Active Directory, Network Policy Server, файловый сервер и т. д.).

Все, что не является обязательным, отнесено к компонентам. Сюда относятся: шифрование диска BitLocker (кстати, тоже новинка), балансировка сетевой нагрузки (Network Load Balancing), оболочка PowerShell, сервера и клиенты Telnet, SMTP, SNMP, управление групповой политикой, диспетчер съемных носителей и др. Выбор ролей и компонентов вместо полной установки позволяет увеличить безопасность и повысить стабильность.

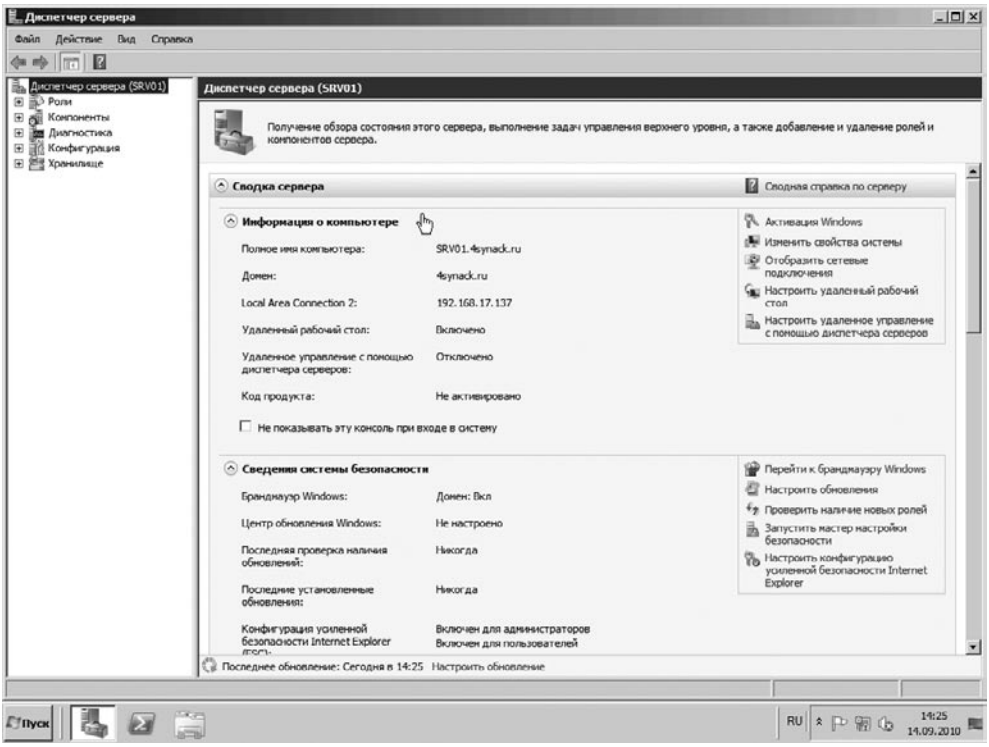

Рис. 1.1. Новые инструменты Диспетчера сервера сделали управление более удобным

Веб-сервер IIS 7.x (Internet Information Services) получил модульную архитектуру. По умолчанию в его состав входит 40 модулей, которые разбиты на восемь категорий, администратор самостоятельно включает только то, что действительно необходимо.

В Windows Server 2008 R2 и Windows 7 добавились и другие усовершенствования. Так, в Vista применен механизм защиты, получивший название UAC (Управление учетными записями пользователя). Он позволял администратору выполнять большинство операций с правами обычного пользователя, а в тех случаях, когда для выполнения некоторой операции или настройки действительно нужны привилегии, выдавался соответствующий запрос. Механизм довольно простой и эффективный, но уж очень неудобный и надоедливый. В Windows 7 UAC сделали более удобным: пользователь может выбрать один из четырех уровней работы, который будет соответствовать требуемому уровню комфорта и безопасности (рис. 1.2).

ПРИМЕЧАНИЕ

Интересный факт: после публикации Windows 7 Beta корпорация Microsoft получила более полумиллиона рационализаторских предложений от пользователей-тестеров со всего мира.

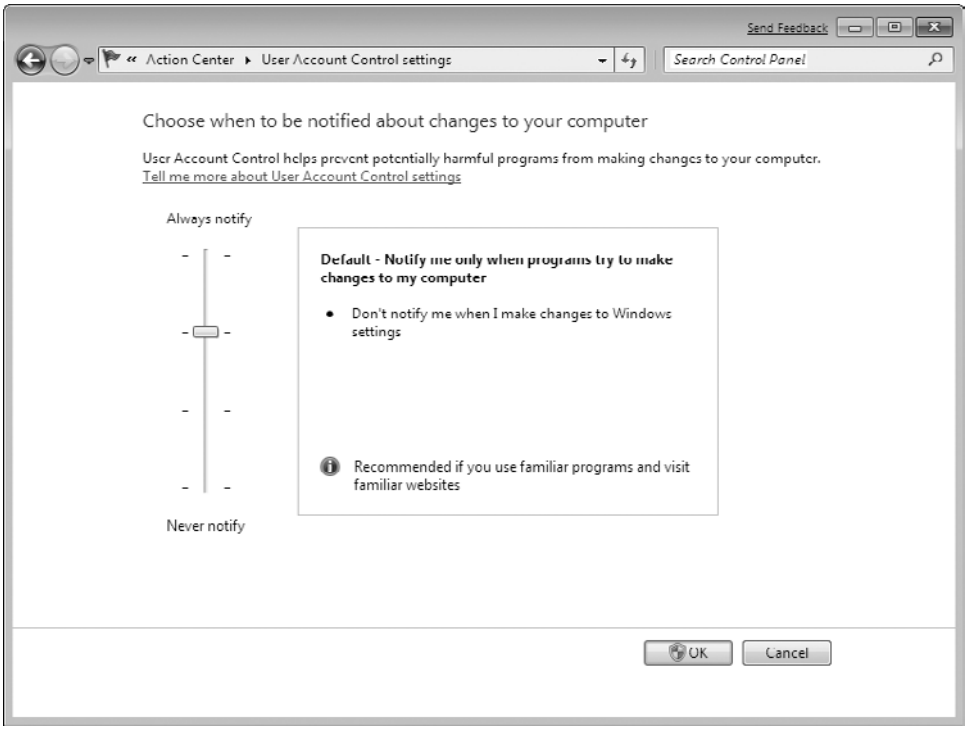

Рис. 1.2. Настройки UAC в Windows 7

Благодаря поддержке седьмой версии протокола RDP (англ. Remote Desktop Protocol — удаленный рабочий стол) клиент удаленного Рабочего стола также получил новые возможности. Среди них — поддержка технологий Aero Glass, Direct2D и Direct3D 10.1, DirectShow, Media Foundation. Увеличена производительность, уменьшены задержки при воспроизведении звука, реализован просмотр видео в высоком качестве и многое другое.

В Windows Server 2008 R2 также появилось несколько новинок. Среди основных нововведений — обновленная система виртуализации Hyper-V 2.0, поддерживающая технологию Live Migration, которая позволяет «на лету» переносить виртуальные машины с одного физического сервера на другой. Динамическое хранилище виртуальных машин дает возможность горячего подключения и отключения хранилищ. Физические и виртуальные системы можно легко развернуть при помощи файлов VHD (Virtual Hard Disk). И в отличие от Windows Server 2008, теперь Hyper-V является неотъемлемой частью системы, то есть больше нет разделения на обычные версии и «with Hyper-V».

На основе R2 можно создавать полноценные решения виртуальных Рабочих столов — Virtual Desktop Infrastructure (VDI). Обеспечивается запуск на центральном

сервере под Hyper-V клиентских систем от Windows XP до Windows 7. Пользователи дистанционно подключаются к своему Рабочему столу с любой точки. Служба Terminal Services получила новое имя — Remote Desktop Services (RDS), что больше отражает ее назначение — работа в структуре VDI.

Технология BranchCache позволяет уменьшить нагрузку на внешний канал за счет кэширования данных. Технология VPN (Virtual Private Network — виртуальная частная сеть), которая используется для доступа компьютеров к ресурсам внутренней (корпоративной) сети и подключения к Интернету, дополнена технологией DirectAccess, также позволяющей устанавливать защищенное соединение, но главным отличием DirectAccess от VPN является работа полностью в фоновом режиме без участия пользователя. В случае обрыва соединение восстанавливается автоматически. В итоге DirectAccess делает работу прозрачной, максимально простой и удобной.

В Windows Server 2008 был представлен новый брандмауэр (Windows Firewall, рис. 1.3), в котором наконец появилась возможность фильтрации исходящего трафика и способность выявлять некоторые типы сетевых атак.

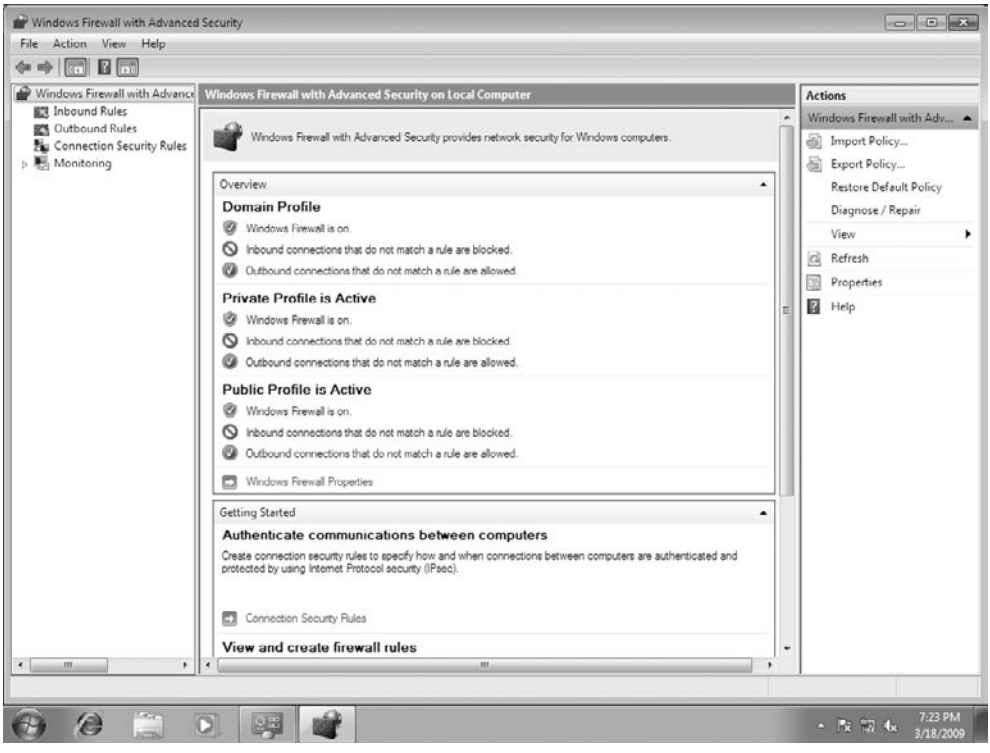

Рис. 1.3. В обновленном Windows Firewall можно активизировать несколько профилей

Кроме этого, он обеспечивает контроль доступа программ в сеть, поддерживает протоколы IPv6 и IPsec, настройку параметров через объекты групповой политики Group Policy Object (GPO). В R2 и Windows 7 в Windows Firewall можно одновременно активизировать несколько профилей (Private, Public или Domain), что не вызывает проблем при подключении к нескольким сетям, добавлена поддержка HTTP ссылок в QoS, реализованы новые функции VPN Reconnect и DHCP Failover.

ПРИМЕЧАНИЕ

В Windows Vista, если компьютер подключен к нескольким сетям, применялся наиболее ограничивающий профиль, что часто вызывало проблемы с подключением.

Например, функция VPN Reconnect, являющаяся частью RRAS (Routing and Remote Access Service — служба маршрутизации и дистанционного доступа), позволяет VPN-клиенту автоматически восстанавливать VPN-подключение в ситуации, когда связь с VPN-сервером временно оборвалась (ранее это нужно было делать вручную или выждать некоторое время).

ПРИМЕЧАНИЕ

Служба QoS (Quality of Service — качество обслуживания) позволяет приоритезировать трафик при доступе к определенным ресурсам.

В Windows Server 2008 R2 и Windows 7 представлена расширенная версия политик ограниченного использования программ — AppLocker. К технологии шифрования разделов жесткого диска BitLocker добавилась технология шифрования съемных носителей BitLocker To Go.

В стандартную поставку системы включен скриптовый язык PowerShell 2.0, являющийся одновременно и средством управления системой, и средством автоматизации многих операций.

Как видите, в новых версиях операционных систем очень много интересных новинок. Осталось научиться применять их на практике. Практически все указанные выше технологии по ходу книги будут рассмотрены более подробно, поэтому не расстраивайтесь, если вы сейчас чего-то не поняли.

Версии и системные требования

Операционные системы Windows 7 и Windows Server 2008 R2 доступны для свободной загрузки на сайте Microsoft. Предлагается несколько редакций как серверной, так и клиентской системы, которые ориентированы на определенное окружение или задачу.