УНИВЕРСИТЕТ ИТМО

С.М. Платунова

WINDOWS SERVER 2012

УПРАВЛЕНИЕ СЕРВЕРАМИ АВТОМАТИЗАЦИЯ АДМИНИСТРАТИВНЫХ ЗАДАЧ

Учебное пособие

Санкт-Петербург

2016

С.М. Платунова

WINDOWS SERVER 2012

УПРАВЛЕНИЕ СЕРВЕРАМИ АВТОМАТИЗАЦИЯ АДМИНИСТРАТИВНЫХ ЗАДАЧ

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2016

Платунова С.М. Windows Server 2012. Управление серверами. Автоматизация административных задач. Учебное пособие по дисциплине «Администрирование вычислительных сетей». – СПб: НИУ ИТМО, 2016. – 126 с.

В учебном пособии содержатся основные сведения об управлении ролями, службами ролей и компонентов, установке сервера, удаленном управлении серверами, основах групповой политики, управлении пользователями и компьютерами с помощью групповой политики под управлением операционной системы Microsoft Windows Server 2012.

Учебное пособие предназначено для подготовки магистров по направлению «09.04.01 - Информатика и вычислительная техника» по магистерской программе «Системное администрирование аппаратно-программных комплексов и сетей».

Рекомендовано к печати Ученым советом факультета Академии ЛИМТУ, протокол № 8 от 09.11.2015

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

Глава 1. 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:

1. добавление серверов для удаленного управления;
2. инициирование удаленных соединений к серверам;
3. настройка локального сервера;
4. управление установленными ролями и компонентами;
5. управление томами и общими ресурсами;
6. настройка объединения сетевых адаптеров NIC (Network Interface Card);
7. просмотр событий и предупреждений;
8. 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:

1. изменения имени компьютера;
2. настройки производительности приложений, виртуальной памяти и параметров реестра;
3. управления переменными окружения пользователя и системы;
4. 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.

1. 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.
2. 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.

3. 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.
4. 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. 1.1 представлен обзор основных ролей и связанных с ними служб ролей, доступных для размещения на сервере под управлением ОС Windows Server 2012.

Таблица 1.1. Основные роли и связанные ролевые службы для Windows Server 2012

Роль	Описание
Службы сертификатов Active Directory (Active Directory Certificate Services, AD CS)	зыва цифровых сертификатов для пользователей, компьютеров клиентов и серверов. Службы роли: Центр сертификации (Certification Authority), Веб-служба политик регистрации сертификатов (Certificate Enrollment Policy Web Service), Веб-служба регистрации сертификатов (Certificate Enrollment Web Service), Сетевой ответчик (Online Responder),

	Служба регистрации в центре сертификации через Интернет (Certification AuthorityWeb Enrollment Support), Служба регистрации на сетевых устройствах (Network Device Enrollment Service)
Доменные службы ActiveDirectory (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
Службы федерации Active Directory (Active Directory Federation Services, AD FS)	Производят аутентификацию и управление доступом для AD DS путем расширения этих функций на WWW. Сервисы и подсервисы роли: Службы федерации (Federation Service), Поддерживающий утверждение агент AD FS 1.1 (Claims-Aware Agent), Агент Windows на основе токенов (Windows Token-Based Agent), Прокси-агент службы федерации (Federation Service Proxy)
Службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services, AD LDS)	Предоставляют хранилище данных для каталогозависимых приложений, которые не требуют AD DS и размеще-ния на контроллере домена. Не требует дополнительных служб ролей
Службы управления правами Active Directory (Active Directory Rights Management, AD RMS)	Предоставляют контролируемый доступ к защищенным сообщениям e-mail, документам, страницам интрасети и другим типам файлов. Требует наличие служб: Сервер управления правами Active Directory (Active Directory Rights Management Server) и Поддержка федерации удостоверений (Identity Federation Support)

Сервер приложений (Application Server)	Позволяет серверу размещать приложения, построенные с помощью ASP.NET, Enterprise Services и Microsoft .NET Framework 4.5. Требует более 10 служб ролей
DHCP-сервер (DHCP Server)	Предоставляет централизованное управление IP-адресацией. DHCP-серверы динамически назначают IP-адреса и другие TCP/IP-параметры другим компьюте-рам сети. Не требует дополнительных ролевых служб
DNS-сервер (DNS Server)	DNS — система разрешения имен, преобразующая имена компьютеров в IP-адреса. Наличие DNS-серверов обяза- тельно в доменах Active Directory. Не требует дополнительных ролевых служб
Факс-сервер (Fax Server)	Предоставляет централизованный контроль над отправкой и приемом факсов на предприятии. Факс-сервер может работать как шлюз для факсов и позволяет управлять факс-ресурсами: заданиями и отчетами, факс-устройствами на сервере или в сети. Не требует дополнительных служб
Файловые службы и службы хранилища (File And Storage Services)	Предоставляют сервисы для управления файлами и хранилищем. Некоторые роли требуют дополнительные типы файловых служб. Службы роли: BranchCache для сетевых файлов (BranchCache for Network Files), Дедупликация данных (Data Deduplication), Распределенная файловая система (Distributed File System), Пространства имен распределенной файловой системы (DFS Namespaces), Репликация DFS (DFS Replication), Файловый сервер (File Server), Диспетчер ресурсов файлового сервера (File Server Resource Manager), Services for Network File System (NFS), Конечный iSCSI-сервер (iSCSI Target Server),

	Загрузка цели iSCSI (iSCSI Target Storage Provider) и Storage Services
Hyper-V	Предоставляет службы для создания и управления виртуальными машинами и эмулирования физических компьютеров. На виртуальные машины можно установить операционные системы, отличные от операционной системы сервера
Службы политики сети и доступа (NPAS, Network Policy and Access Services)	Предоставляют службы для управления политиками сетевого доступа. Ролевые сервисы: Сервер политики сети (Network Policy Server), Протокол авторизации учетных данных узла (Host Credential Authorization Protocol) и Центр регистрации работоспособности (Health Registration Authority)
Службы печати и документов (Print And Document Services	Предоставляют службы для управления сетевыми принтерами, сетевыми сканерами и соответствующими драйверами. Ролевые сервисы: Сервер печати (Print Server), Печать через Интернет (Internet Printing), Сервер распределенного сканирования (Distributed Scan Server), Служба LPD (LPD Service)
Удаленный доступ (Remote Access)	Обеспечивает сервисы для управления маршрутизацией и удаленным доступом к сетям. Используйте эту роль, если необходимо настроить виртуальную частную сеть (VPN), трансляцию сетевых адресов (NAT) и другие сервисы маршрутизации. Службы: DirectAccess и VPN (RAS) (DirectAccess and VPN (RAS)), Маршрутизация (Routing)
Службы удаленных рабочих столов (Remote Desktop Services)	Предоставляют службы, позволяющие пользователям запускать Windows-приложения, установленные на удаленном сервере.

	При запуске пользователем приложения на терминальном сервере весь процесс выполнения происходит на сервере, по сети передаются только данные от приложения
Volume Activation Services	Предоставляет службы для автоматического управления лицензионными ключами томов и активацией ключей томов
Веб-сервер (IIS) (Web Server (IIS))	Используется для размещения веб-сайтов и веб-приложений. Веб-сайты, размещаемые на веб-сервере, могут иметь статический и/или динамический контент. Некоторые веб-приложения, которые будут размещены на веб-сервере, используют ASP.NET и .NET Framework 4.5. При установке веб-сервера можно управлять конфигурацией сервера с помощью модулей и утилит администратора IIS 8. Содержит около 10 служб ролей
Служба развертывания Windows (Windows Deployment Services, WDS)	Предоставляет сервисы для размещения Windows-компьютеров на предприятии. Службы ролей: Сервер развертывания (Deployment Server), Транспортный сервер (Transport Server)
Службы Windows Server Update Services (WSUS)	Предоставляют сервисы для Microsoft Update, разрешая предоставлять обновления для определенных серверов

В табл. 1.2 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 1.2. Основные компоненты ОС Windows Server 2012

Компонент	Описание

Фоновая интеллектуальная служба передачи (BITS) (Background Intelligent Transfer Service	Обеспечивает фоновую интеллектуальную передачу. После установки этого компонента сервер может действовать как BITS-сервер, который способен принимать загрузки файлов от клиентов. Этот компонент не является необходимым для клиентов, использующих BITS. Дополнительные подкомпоненты: Расширение сервера IIS (BITS IIS Server Extension) и Облегченный сервер загрузки (BITS Compact Server)
Шифрование диска BitLocker (BitLocker Drive Encryption)	Обеспечивает основанную на аппаратных средствах защиту данных с помощью шифрования всего тома. Компьютеры, оснащенные модулем Trusted Platform Module (TPM), могут использовать Шифрование диска BitLocker в режиме Startup Key или TPM-Only
Сетевая разблокировка BitLocker (BitLocker Network Unlock)	Обеспечивает поддержку для основанных на сети ключевых средств защиты, которые автоматически разблокируют BitLocker-защищенные диски операционной системы, когда присоединенный к домену компьютер будет перезапущен
BranchCache	Предоставляет функциональность, необходимую для клиентов и серверов BranchCache. Содержит службы HTTP protocol, Hosted Cache и др.
Клиент для NFS (Client for NFS	Обеспечивает функциональность для доступа к файлам, находящимся на NFS-серверах под управлением UNIX
Мост для центра обработки данных (Data Center Bridging)	Поддерживает набор IEEE-стандартов для улучшения локальных Ethernet-сетей путем обеспечения гарантированной аппаратной пропускной способности
Enhanced Storage	Обеспечивает поддержку устройств Enhanced Storage

Отказоустойчивая кластеризация (Failover Clustering)	Позволяет нескольким серверам работать вместе для обеспечения высокого уровня доступности ролей серверов. Можно кластеризировать многие типы серверов, в том числе файловый сервер и сервер печати. Серверы баз данных и сообщений - отличные кандидаты для кластеризации
Управление групповой политикой (Group Policy Management)	Устанавливает консоль управления групповой политикой (Group Policy Management Console (GPMC)) для централизованного администрирования групповой политики
Служба рукописного ввода (Ink and Handwriting Services)	Обеспечивает использование ручки или стилуса, а также распознавания рукописного ввода
Сервер управления IP-адресами (IP Address Management Server)	Централизованно управляет пространством IP-адресов и соответствующими серверами инфраструктуры
Клиент печати через Интернет (Internet Printing Client)	Позволяет клиентам использовать протокол HTTP для печати на принтерах, подключенных к веб-серверам печати
Служба iSNS-сервера (Internet Storage Naming Server (iSNS) Server Service)	Предоставляет управление и функции сервера для iSCSI-устройств. Позволяет серверу обрабатывать запросы регистрации и дерегистрации, также запросы от iSCSI-устройств
Монитор LPR-порта (LPR Port Monitor)	Позволяет выполнять печать на принтерах, подключенных к UNIX-компьютерам
Media Foundation	Обеспечивает необходимую функциональность для Windows Media Foundation
Очередь сообщений (Message Queuing)	Функции управления и сервер-функции для распределенной очереди сообщений. Как правило, доступна группа дополнительных подкомпонентов
Multipath I/O (MPIO)	Обеспечивает функциональность,

	необходимую для использования путей данных к устройствам хранения данных
.NET Framework 4.5	Предоставляет API для разработки приложений. Дополнительные подкомпоненты: .NET Framework 4.5, ASP.NET 4.5 и Windows Communication Foundation (WCF) Activation Components
Балансировка сетевой нагрузки (NLB) (Network Load Balancing)	Распределяет трафик между несколькими серверами по протоколу TCP/IP. Идеальными кандидатами для балансировки нагрузки являются веб-серверы
Протокол однорангового разрешения имен (PNRP) (Peer Name Resolution Protocol)	Предоставляет функциональность Link-Local Multicast Name Resolution (LLMNR), обеспечивая тем самым одноранговое разрешение имен. После добавления этого компонента приложения, установленные на сервере, смогут регистрировать и разрешать имена с помощью LLMNR
QWave (Quality Windows Audio Video Experience)	Сетевая платформа для передачи аудио/видео по домашним сетям
Пакет администрирования диспетчера RAS-подключений (RAS Connection Manager Administration Kit)	Фреймворк для создания профилей соединений к удаленным серверам и сетям
Удаленный помощник (Remote Assistance)	Разрешает удаленному пользователю подключаться к серверу для обеспечения или получения удаленной помощи
Удаленное разностное сжатие (Remote Differential Compression)	Вычисляет и передает различия между двумя объектами данных и минимизирует объем передаваемых данных
Средства удаленного администрирования сервера (RSAT) (Remote Server Administration Tools)	Устанавливает средства управления ролями и компонентами, которые могут использоваться для удаленного администрирования других Windows-серверов. Администратор может выбрать, какие именно средства необходимо установить
RPC через HTTP-прокси (Remote	Устанавливает прокси для передачи

Procedure Call (RPC) over HTTP Proxy)	RPC-сообщений от клиентских приложений к серверам через HTTP-прокси. RPC по HTTP - это альтернатива доступа клиента к серверу через частную сеть
Простые службы TCP/IP (Simple TCP/IP Services)	Устанавливает дополнительные TCP/IP-сервисы, в том числе Character Generator, Daytime, Discard, Echo и Quote of the Day
SMTP-сервер (Simple Mail Transfer Protocol (SMTP) Server	SMTP - сетевой протокол для контроля передачи и маршрутизации сообщений e-mail. После установки этого компонента сервер может работать как базовый SMTP-сервер. Для полноценного решения нужно установить сервер сообщений вроде Microsoft Exchange Server
Служба SNMP (Simple Network Management Protocol (SNMP) Services)	SNMP - протокол, используемый для упрощения управления TCP/IP-сетями. Протокол SNMP используется для централизованного управления сетью, если в сети есть SNMP-совместимые устройства. Также протокол SNMP применяется для мониторинга сети с помощью программного обеспечения мониторинга сетью
Подсистема для UNIX-приложений (Subsystem for UNIX-Based Applications (SUA))	Предоставляет возможность запуска UNIX-приложений. Дополнительные инструменты управления доступны для загрузки с сайта Microsoft (не рекомендуется использовать)
Клиент Telnet (Telnet Client)	Используется для подключения к удаленному Telnetсерверу и запуска приложений на этом сервере
Сервер Telnet (Telnet Server)	Размещает удаленные сессии Telnet-клиентов. При запущенном сервере Telnet пользователи могут использовать клиенты Telnet для удаленного подключения к этому компьютеру
Пользовательские интерфейсы и инфраструктура (User Interfaces And Infrastructure)	Позволяет контролировать параметры пользовательского интерфейса (Графические средства

	управления и инфраструктура, Возможности рабочего стола, Графическая оболочка сервера)
Биометрическая платформа Windows (Windows Biometric Framework)	Поддерживает устройства сканирования отпечатков Пальцев
Внутренняя база данных Windows (Windows Internal Database)	Реляционное хранилище данных, которое может быть использовано только функциями и ролями Windows Server, например, AD RMS, UDDI Services, WSUS, Windows SharePoint Services и WSRM
Windows PowerShell	Разрешает управлять функциями Windows PowerShell-сервера. Windows PowerShell 3.0 и PowerShell ISE устанавливаются по умолчанию
Windows PowerShell Web Access	Превращает сервер в веб-шлюз для удаленного управления серверами с помощью веб-браузера
Служба активации процессов Windows (Windows Process Activation Service)	Обеспечивает поддержку распределенных веб-приложений, которые используют HTTP- и не-HTTP-протоколы
Стандартизированное управление хранилищами Windows (Windows Standards-Based Storage Management	Позволяет обнаруживать запоминающие устройства, управлять ними и контролировать их работу. Предоставляет классы для WMI и Windows PowerShell
Система архивации данных Windows Server (Windows Server Backup)	Позволяет выполнять резервное копирование и восстановление операционной системы, состояния системы и любых данных, хранящихся на сервере
Диспетчер системных ресурсов Windows (WSRM) (Windows System Resource Manager (WSRM))	Позволяет управлять использованием ресурсов (не рекомендуется)
Фильтр Windows TIFF IFilter (Windows TIFF IFilter)	Выполняет распознавания текста в файлах, соответствующих стандарту TIFF 6.0
Расширение IIS WinRM (WinRM IIS Extension)	Позволяет серверу принимать запросы от клиента, используя протокол WS-Management
WINS-сервер (WINS Server)	Сервис разрешения имен, который сопоставляет имена компьютеров их IP-адресам. Установка этого

	компонента превращает компьютер в WINS-сервер
Служба беспроводной локальной сети (Wireless LAN Service)	Позволяет серверу использовать беспроводную сеть
Поддержка WoW64 (WoW64 Support)	Поддержка WoW64, необходимая для полной установки сервера. Удаление этого компонента превращает полную установку сервера в установку основных компонентов
Средство просмотра XPS (XPS Viewer)	Программа для просмотра XPS-документов

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

Администратора могут попросить установить или удалить динамически подключаемые библиотеки (DLL), особенно если он работает в команде ИТ-разработчиков. Для этого используется утилита Regsvr32, которая запускается из командной строки. После открытия окна Командная строка (Command Prompt) для установки или регистрации DLL-библиотеки введите команду regsvr32 имя.dll , например: regsvr32 mylibs.dll

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

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

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

Операционная Windows Server 2012 поддерживает следующие типы установки: полная установка, установка с минимальным графическим интерфейсом и установка основных серверных компонентов (Server Core). Полная установка также называется Сервер с графическим интерфейсом пользователя. Она содержит компоненты Графические средства управления и инфраструктура (Graphical Management Tools And Infrastructure) и Графическая оболочка сервера (Server Graphical Shell), которые входят в состав компонента

Пользовательские интерфейсы и инфраструктура, а также компонент Поддержка WoW64 (WoW64 Support). Установка с минимальным интерфейсом пользователя подобна полной установке, но без компонента Графическая оболочка сервера. Установка основных серверных компонентов (Server Core) обладает ограниченным интерфейсом пользователя и не содержит компонентов Поддержка WoW64 и Пользовательские интерфейсы и инфраструктура (User Interfaces And Infrastructure).

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

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

Обзор установки основных серверных компонентов

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

- экран входа в систему, который служит для входа в систему и выхода из нее;
- редактор Блокнот (notepad.exe) для редактирования файлов;
- редактор реестра (regedit.exe) для управления реестром;
- диспетчер задач (taskmgr.exe) для управления задачами и запуска новых задач;
- командную строку (cmd.exe) для администрирования;
- оболочку PowerShell для администрирования;

- утилиту Проверка подписи файла (sigverif.exe) для проверки цифровых подписей системных файлов;
- утилиту Сведения о системе (msinfo32.exe) для получения системной информации;
- Установщик Windows (msiexec.exe);
- панель Дата и время (timedata.cpl) для просмотра/установки даты, времени и часового пояса;
- панель Язык и региональные стандарты (intl.cpl) для просмотра/изменения региональных и языковых опций, в том числе форматов и раскладки клавиатуры;
- утилиту конфигурации сервера (sconfig), предоставляющую текстовое меню для управления настройкой сервера.

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

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

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

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

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. 1.3.

Таблица 1.3. Полезные команды и инструменты для управления установкой с основными серверными компонентами

Команда	Задача
Cscript Scregedit.wsf	Настраивает операционную систему. Используйте параметр /cli для вывода доступных областей настройки
Diskraid.exe	Настраивает программный RAID-массив
ipconfig /all	Выводит информацию о настройке IP-адреса компьютера
Netdom RenameComputer	Устанавливает имя сервера
Netdom Join	Подключает сервер к домену
Netsh	Предоставляет контекст для управления конфигурацией сетевых компонентов. Введите netsh interface ipv4 для настройки параметров IPv4 или netsh interface ipv6 для настройки IPv6
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. Запус-кает Cscript slmgr.vbs –ipk
SystemInfo	Выводит подробности конфигурации системы
Wecutil.exe	Создает и управляет подписками на перенаправляемые события
Wevtutil.exe	Позволяет просматривать системные события
Winrm quickconfig	Настраивает сервер на прием запросов WS-Management от других компьютеров. Запускает Cscript winrm.vbs quickconfig
Wmic datafile where name="FullFilePath" get version	Выводит версию файла
Wmic nicconfig index=9 call enabledhcp	Настраивает компьютер на использование динамического IP-адреса (вместо статического IP)
Wmic nicconfig index=9 callenablestatic("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 настройки 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.

Операционную систему Windows Server 2012 необходимо активировать после установки.

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

5. На странице Выберите операционную систему, которую вы хотите установить (Select The Operating System You Want To Install) доступны опции

Установка основных серверных компонентов (Server Core Installation) и Сервер с графическим интерфейсом пользователя (Server With A GUI). Сделайте соответствующий выбор и нажмите кнопку Далее.

6. Лицензионное соглашение Windows Server 2012 отличается от предыдущих версий Windows. Прочитайте его, отметьте флажок Я принимаю условия лицензии и нажмите кнопку Далее.

7. На странице Выберите тип установки (Which Type Of Installation Do You Want) выберите тип установки, которую необходимо осуществить. Поскольку выполнится чистая установка, для замены существующей инсталляции или для настройки нового компьютера нажмите кнопку Выборочная: только установка Windows (для опытных пользователей) (Custom Install Windows Only (Advanced)). Если компьютер загружен с дистрибутивного диска, кнопка Обновление (Upgrade) будет недоступна. Для обновления системы нужно перезагрузить компьютер, загрузить установленную ОС, войти в систему и запустить установку.

8. На странице Где вы хотите установить Windows? (Where Do You Want To Install Windows?) выберите диск или раздел диска, на который необходимо установить операционную систему. Существуют две версии этой страницы, поэтому нужно иметь в виду следующее.

- Когда у компьютера есть один жесткий диск с одним разделом на весь диск или одной областью нераспределенного пространства, указывают весь диск, и можно нажать кнопку Далее для выбора этого диска в качестве назначения установки. Если диск не размечен, можно создать необходимые разделы перед установкой операционной системы, как будет показано в разд. "Создание, форматирование, удаление и расширение разделов диска во время установки" далее в этой главе.
- Когда у компьютера имеется несколько дисков или один диск с несколькими разделами, нужно либо выбрать существующий раздел для установки операционной системы, либо создать новый раздел. Как можно создать новый раздел, будет показано в разд. "Создание, форматирование, удаление и расширение разделов диска во время установки" далее в этой главе.
- Если диск не инициализирован или BIOS компьютера не поддерживает запуск операционной системы с выбранного диска, нужно инициализировать диск, создав один или более разделов на этом диске. Нельзя выбрать диск, использующий файловую систему FAT/FAT32. Также нельзя отформатировать диск в этой файловой системе.

  Если раздел, на который планируется установить Windows Server, отформатирован как FAT32, нужно конвертировать его в NTFS. При работе с этой страницей программы установки можно получить доступ к командной строке для осуществления необходимых предустановочных задач (см. разд. "Создание, форматирование, удаление и расширение разделов диска во время установки" далее в этой главе).

9. Если выбранный раздел содержит установку предыдущей версии Windows, инсталлятор сообщит вам, что существующие настройки пользователя и

приложений будут перемещены в папку Windows.old и нужно будет скопировать эти параметры в новую установку Windows. Нажмите кнопку OK.
10. Нажмите кнопку Далее. Инсталлятор начнет установку операционной системы. Во время этого процесса инсталлятор скопирует полный образ диска Windows Server 2012 на выбранный вами диск/раздел, а затем развернет его. После этого инсталлятор установит дополнительные компоненты на основании конфигурации вашего компьютера и обнаруженных аппаратных средств. Этот процесс требует нескольких автоматических перезагрузок. После завершения установки будет загружена операционная система и можно осуществить начальную настройку, например, установить пароль администратора и имя сервера.
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, которое 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.
Невозможно осуществить обновление до Windows Server 2012 на компьютере с 32-битной операционной системой, даже если у компьютера 64-битный процессор. Нужно перенести службы, предоставляемые этим компьютером, на другие серверы, а затем осуществить чистую установку. В этом помогут средства переноса данных (Windows Server Migration tools). Эти утилиты доступны на компьютерах с запущенной ОС Windows Server 2012. Осуществить обновление до Windows Server 2012 можно с помощью следующих действий:
1. Включите компьютер, войдите в систему, используя учетную запись администратора. После помещения установочного диска Windows Server 2012 в DVD-ROM автоматически запустится инсталлятор. Если это не произошло, используйте Проводник для доступа к файлу установочного диска и двойным щелчком запустите программу Setup.exe.
2. Поскольку программа установки запускается из текущей операционной системы, инсталлятор не будет просить выбрать пользователя язык, форматы валюты и времени и раскладку клавиатуры. При установке будет доступна только одна раскладка клавиатуры — та, которая используется в установленной операционной системе. Если язык раскладки и язык выпуска Windows Server 2012 не совпадают, при вводе можно увидеть неожиданные символы.
3. Нажмите кнопку Установить для запуска инсталляции. После этого инсталлятор скопирует временные файлы на компьютер и спросит, нужно ли получить обновления во время установки. Выберите переключатель Установить обновления из Интернета сейчас или Нет, спасибо.
4. В случае с корпоративными выпусками Windows Server 2012 не нужно вводить ключ продукта во время установки операционной системы. Если используется OEM-версия, скорее всего, вас попросят ввести ключ продукта. Нажмите кнопку Далее для продолжения. Флажок Автоматически активировать Windows при подключении к Интернету отмечен по умолчанию, чтобы гарантировать активацию операционной системы, как только компьютер подключится к Интернету.
5. На странице Выберите операционную систему, которую вы хотите установить доступны опции Установка основных серверных компонентов и Сервер с графическим интерфейсом пользователя. Сделайте соответствующий выбор и нажмите кнопку Далее.
6. Лицензионное соглашение Windows Server 2012 отличается от предыдущих версий Windows. Прочитайте его, отметьте флажок Я принимаю условия лицензии и нажмите кнопку Далее.
7. На странице Выберите тип установки (Which Type Of Installation Do You Want) выберите тип установки, которую необходимо осуществить. Поскольку осуществляется обновление, нажмите кнопку Обновление (Upgrade). Если установка запущена с загрузочного диска, а не из Windows, кнопка Обновление будет недоступной. Для обновления нужно перезагрузить компьютер, загрузить

установленную версию Windows, войти в систему и запустить программу установки.
8. Затем инсталлятор начнет установку. Поскольку происходит обновление системы, не нужно выбирать место для установки. Во время этого процесса инсталлятор скопирует полный образ диска Windows Server 2012 на системный диск, а затем установит дополнительные компоненты в зависимости от конфигурации компьютера и обнаруженного оборудования. По окончанию установки будет загружена операционная система, и можно осуществить начальную настройку, например, установить пароль администратора и имя сервера.

Дополнительные административные задачи во время установки

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

Использование командной строки во время установки

При получении доступа к командной строке из программы установки администратор будет работать с окружением MINWINPC (mini Windows PC), которое используется инсталлятором операционной системы. Получить доступ к командной строке можно с помощью комбинации клавиш <Shift>+<F10>, нажатой на странице Где вы хотите установить Windows? Окружение mini Windows PC предоставляет большинство утилит, доступных в командной строке Windows Server 2012 (табл. 1.4).

Таблица 1.4. 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
CHOICE	Создает список, из которого пользователи могут выбрать один из нескольких вариантов (используется в пакетном сценарии)
CLS	Очищает окно консоли
CMD	Запускает новый экземпляр окна командной строки Windows
COLOR	Устанавливает цвет окна командной оболочки Windows
CONVERT	Конвертирует FAT-тома в NTFS
COPY	Копирует или комбинирует файлы
DATE	Отображает/устанавливает системную дату
DEL	Удаляет один или больше файлов
DIR	Отображает список файлов и подкаталогов заданного каталога
DISKPART	Вызывает командный интерпретатор, позволяющий управлять дисками, разделами и томами, используя отдельную командную строку и внутренние команды DISKPART
DISM	Управляет образами Windows
DOSKEY	Используется для создания макросов, состоящих из команд Windows
ECHO	Отображает сообщения, а также переключает режим отображения команд на экране
ENDLOCAL	Завершение локализации окружения в пакетном файле
ERASE	Стирает один или более файлов
EXIT	Выход из командного интерпретатора
EXPAND	Разархивирует файлы
FIND	Производит поиск текстовой строки в файлах
FOR	Запускает указанную команду для каждого файла из набора файлов
FORMAT	Форматирует дискету или жесткий диск
FTP	Передает файлы
FTYPE	Отображает/изменяет типы файлов, используемые в ассоциации расширений

GOTO	Передает управление содержащей метку строке командного файла
HOSTNAME	Выводит имя компьютера
IF	Осуществляет проверку условия в пакетных программах
IPCONFIG	Отображает конфигурацию TCP/IP
LABEL	Создает, изменяет или удаляет информацию о томе диска
MD/MKDIR	Создает каталог или подкаталог
MORE	Поэкранно выводит данные
MOUNTVOL	Управляет точкой монтирования тома
MOVE	Перемещает файлы из одного каталога в другой на одном и том же диске
NBTSTAT	Отображает статус NetBIOS
NET ACCOUNTS	Управляет учетной записью пользователя и политиками паролей
NET COMPUTER	Добавляет/удаляет компьютер в домен или из домена
NET CONFIG SERVER	Отображает/модифицирует конфигурацию службы Сервер
NET CONFIG WORKSTATION	Отображает/модифицирует конфигурацию службы Рабочая станция
NET CONTINUE	Возобновляет работу приостановленной службы
NET FILE	Отображает открытые файлы на сервере или управляет ими
NET GROUP	Показывает глобальные группы или управляет ими
NET LOCALGROUP	Показывает локальные группы или управляет ими
NET NAME	Отображает/модифицирует получателей для службы сообщений
NET PRINT	Отображает/модифицирует задания печати и управляет очередью печати
NET SEND	Отправляет сообщение с использованием службы сообщений
NET SESSION	Показывает или завершает установленные сеансы
NET SHARE	Показывает общие принтеры и каталоги или управляет ими
NET START	Запускает сетевые сервисы или отображает запущенные сервисы

NET STATISTICS	Отображает статистику рабочей станции и сервера
NET STOP	Останавливает сервисы
NET TIME	Отображает/синхронизирует сетевое время
NET USE	Отображает удаленные соединения или управляет ими
NET USER	Управляет локальными учетными записями пользователей
NET VIEW	Отображает сетевые ресурсы или компьютеры
NETSH	Открывает отдельную командную оболочку, позволяющую управлять конфигурацией разных сетевых сервисов на локальном и удаленном компьютерах
NETSTAT	Отображает статус сетевых соединений
PATH	Отображает или устанавливает путь поиска исполняемых файлов в текущем командном окне
PATHPING	Трассирует маршрут и предоставляет информацию о потере пакетов
PAUSE	Приостанавливает обработку сценария и ждет ввод с клавиатуры
PING	Определяет, установлено ли сетевое соединение
POPD	Переходит в каталог, сохраненный командой PUSHD
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
SETLOCAL	Начинает локализацию окружения в пакетном файле
SFC	Сканирует и проверяет защищенные системой файлы

Принудительное удаление раздела диска во время установки

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

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

Загрузка драйверов устройств во время установки

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

Для загрузки драйвера диска выполните следующие действия:

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

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

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

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

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

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

Создание раздела диска во время установки

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

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

После создания раздела его нужно отформатировать для продолжения установки.

Форматирование раздела диска во время установки

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

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

Удаление раздела диска во время установки

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

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

Расширение раздела диска во время установки

Операционная система Windows Server 2012 требует как минимум 10 Гбайт дискового пространства для установки (рекомендуется 32 Гбайт). Если существующий раздел слишком мал, его нельзя использовать для установки

ОС. Чтобы установить ОС, нужно расширить раздел для увеличения его размера за счет использования нераспределенного пространства текущего диска. Расширить раздел можно, только если он отформатирован под файловую систему NTFS 5.2 (или более позднюю версию NTFS). Новые разделы, созданные в инсталляторе, также могут быть расширены, если на диске есть нераспределенное дисковое пространство.

Для расширения раздела выполните следующие действия:

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

Изменение типа установки

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

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

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

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

Конвертирование полной установки и установки с минимальным графическим интерфейсом

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

uninstall-windowsfeature server-gui-shell -restart
Эта команда предписывает Windows Server удалить компонент Графическая оболочка сервера, а затем перезапустить сервер. Если компонент Возможности рабочего стола установлен, его нужно также удалить.
Перед вводом команды, у которой могут быть далеко идущие последствия, лучше всего выполнить ее с параметром -Whatif. Этот параметр заставляет PowerShell сообщать, что произойдет при запуске команды.
Чтобы конвертировать установку с минимальным интерфейсом в полную установку, нужно добавить компонент Графическая оболочка сервера. Можно использовать мастер добавления ролей и компонентов (Add Roles And Features Wizard) или выполнить следующую PowerShell-команду:
install-windowsfeature server-gui-shell -restart
Эта команда устанавливает компонент Графическая оболочка сервера и перезапускает сервер для завершения установки. Если также нужно добавить компонент Возможности рабочего стола, используйте эту команду вместо предыдущей:
install-windowsfeature server-gui-shell, desktop-experience -restart

Конвертирование установки с основными серверными компонентами

Для преобразования полной установки или установки с минимальным графическим интерфейсом в установку с основными серверными компонентами (Server Core) необходимо удалить компоненты Графические средства управления и инфраструктура и Поддержка WoW64. Сервер будет сконфигурирован под установку Server Core. Хотя для удаления пользовательского интерфейса обычно используется мастер удаления ролей и компонентов, можно обойтись командой, введенной в приглашении PowerShell:
uninstall-windowsfeature server-gui-mgmt-infra -restart
Эта команда указывает Windows Server удалить пользовательский интерфейс для компонента Графические средства управления и инфраструктура и перезагрузить сервер для завершения удаления. Поскольку многие зависимые роли, ролевые службы и компоненты могут быть удалены, введите команду с параметром -Whatif , чтобы увидеть, что было удалено.
Если сервер установлен с пользовательским интерфейсом, а потом установка конвертирована в Server Core, вернуться к полной установке можно командой:
install-windowsfeature server-gui-mgmt-infra -restart
Поскольку бинарные файлы для этого компонента и зависимых компонентов не были удалены, команда должна выполниться успешно. Если бинарные файлы были удалены или установлена оригинальная инсталляция Server Core, тогда нужно указать источник для требуемых бинарных файлов.
Чтобы восстановить бинарные файлы из точки монтирования Windows Imaging (WIM), нужно указать параметр -Source . Например, если в вашей компании есть смонтированный образ Windows Server 2012, доступный в сети по адресу \\ImServer18\WinS12EE, команда будет такой:
install-windowsfeature server-gui-mgmt-infra -source \\imserver18\wins12ee

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

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

Управление ролями, службами ролей и компонентами

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

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

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

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).

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 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.

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

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

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

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

принимать участие в Программе улучшения качества программного обеспечения (Customer Experience Improvement Program, CEIP). Щелкните по соответствующей ссылке для изменения этой настройки.

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

- Ethernet - показывает конфигурацию TCP/IP для проводных Ethernet-соединений. Щелкните по соответствующей ссылке, чтобы открыть консоль Сетевые подключения (Network Connections). Для настройки соединения дважды щелкните на нем, а затем нажмите Свойства (Properties) для открытия одноименного окна. По умолчанию серверы настраиваются для использования динамической адресации для IPv4 и IPv6. Консоль Сетевые подключения можно также вызвать из Центра управления сетями и общим доступом, выбрав задачу Изменение параметров адаптера (Change Adapter Settings).
- Конфигурация усиленной безопасности Internet Explorer (IE Enhanced Security Configuration) - показывает статус расширенной безопасности Internet Explorer (IE ESC). Щелкните по соответствующей ссылке для включения или отключения IE ESC.

Данная функция может быть включена/выключена для пользователей, администраторов либо для тех и других одновременно. IE ESC - средство защиты, которое уменьшает восприимчивость сервера к потенциальным атакам, повышая стандартные уровни безопасности в зонах безопасности Internet Explorer и изменяя настройки этого браузера по умолчанию. По умолчанию функциональность IE ESC включена для администраторов и для пользователей. В большинстве случаев у вас должна быть включена функциональность IE ESC и для администраторов, и для пользователей. Однако включение IE ESC ограничивает функциональность Internet Explorer. Когда расширенная безопасность Internet Explorer включена, зоны безопасности настраиваются так: для зоны Интернет (Internet) устанавливается высокий уровень безопасности, для зоны Надежные сайты (Trusted Sites) - средний, для зоны Местная интрасеть (Local Intranet) — ниже среднего, для зоны Опасные сайты (Restricted) - высокий. Также устанавливаются следующие параметры: включается параметр Включить защищенный режим (Enhanced Security Configuration), сторонние расширения и звуки страниц отключаются, анимация на веб-страницах отключается, включается проверка подписи для загружаемых программ, зашифрованные страницы не сохраняются, временные файлы Интернета удаляются при закрытии окна браузера, включаются предупреждения для защищенных и незащищенных режимов, включается защита памяти.

- Объединение сетевых карт (NIC Teaming) - показывает статус и конфигурацию объединения сетевых карт. Щелчок по

соответствующей ссылке позволит добавить/удалить объединенные сетевые интерфейсы и изменить их настройки.

- Код продукта (Product ID) - показывает идентификатор продукта Windows Server. Щелкните по соответствующей ссылке для ввода кода продукта и активации операционной системы через Интернет.
- Удаленный рабочий стол (Remote Desktop) - щелкните по соответствующей ссылке, чтобы отобразить окно Свойства системы с активной вкладкой Удаленный доступ (Remote). Для настройки удаленного рабочего стола установите необходимые параметры и нажмите кнопку OK. По умолчанию удаленные соединения к серверу запрещены. Вызвать диалоговое окно Свойства системы можно с помощью утилиты Система (System) Панели управления, на левой панели которой нужно выбрать Настройка удаленного доступа (Remote Settings).
- Удаленное администрирование (Remote Management) - показывает, включено ли для этого сервера удаленное администрирование. Щелкните по соответствующей ссылке для включения или выключения удаленного администрирования.
- Часовой пояс (Time Zone) - показывает текущий часовой пояс для сервера. Щелкните по соответствующей ссылке для отображения окна Дата и время (Date And Time). Далее нажмите кнопку Изменить часовой пояс (Change Time Zone), выберите нужный часовой пояс и дважды нажмите кнопку OK. Также можно вызвать окно Дата и время, щелкнув правой кнопкой мыши на панели задач и выбрав команду Настройка даты и времени (Adjust Date/Time). Хотя все серверы настроены для автоматической синхронизации времени с интернет-сервером времени, процесс синхронизации времени не изменяет часовой пояс компьютера.
- Отчеты об ошибках Windows (Windows Error Reporting) - показывает статус средства Отчеты об ошибках Windows (Windows Error Reporting, WER). Щелкните по соответствующей ссылке для изменения настроек данного средства. В большинстве случаев нужно оставить средство включенным как минимум на протяжении 60 дней с момента установки операционной системы. С включенным средством WER ваш сервер будет отправлять описания проблем в Microsoft, а Windows - уведомлять вас о возможных решениях этих проблем. Просмотреть отчеты о проблеме и возможные решения можно с помощью Центра поддержки (Action Center). Чтобы открыть Центр поддержки, щелкните правой кнопкой мыши на значке Центра поддержки в области уведомлений панели задач и выберите команду Открыть Центр поддержки (Open Action Center).
- Брандмауэр Windows (Windows Firewall) - показывает статус брандмауэра Windows. Если брандмауэр активен, это свойство отображает имя активного профиля и статус брандмауэра. Щелкните

по соответствующей ссылке для отображения окна утилиты Брандмауэр Windows (Windows Firewall). По умолчанию брандмауэр Windows включен. Эту же утилиту можно вызвать через Панель управления, переключив ее в режим Крупные значки (или Мелкие значки) и дважды щелкнув на ссылке Брандмауэр Windows.

- Центр обновления Windows (Windows Update) - показывает текущий статус Центра обновления Windows. Щелчок (или нажатие) по соответствующей ссылке позволяет вызвать утилиту Центр обновления Windows, которую можно использовать для автоматического обновления (если обновление отключено) или проверить наличие обновлений (если обновление включено). Аналогично, данную утилиту можно вызвать через Панель управления.

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 installwindowsfeature 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 путь используется только для полезных данных, не найденных в папке Windows Side-By-Side (WinSXS) сервера. На многих крупных предприятиях в сети доступен образ Windows Server 2012, но можно смонтировать дистрибутивный диск и использовать папку Windows\WinSXS этого диска в качестве источника. Чтобы сделать это, выполните следующие действия:

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

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

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

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

Удаленное управление серверами

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

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

Средства удаленного администрирования сервера для Windows 8 можно получить через центр загрузок Microsoft - Download Center

(download.microsoft.com). Обратите внимание, что есть разные версии для систем 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 OK.
После этого диспетчер серверов выполнит несколько фоновых задач для отключения службы Удаленное управление Windows (WinRM) и удаленного доступа Windows PowerShell для управления локальным сервером. Одна из этих задач - выключение соответствующего исключения, которое позволяет приложениям взаимодействовать через Брандмауэр Windows, используя удаленное управление Windows. Исключения для компонентов Инструментарий управления Windows (Windows Management Instrumentation) и Удаленное управление Windows в режиме совместимости (Windows Remote Management (Compatibility)) не будут затронуты.
Для управления компьютером с помощью диспетчера серверов пользователь должен быть членом группы Администраторы (Administrators). Для удаленных соединений в конфигурациях "рабочая группа - рабочая группа" или "рабочая группа - домен" вам нужно войти в систему с использованием встроенной учетной записи Администратор (Administrator) или настроить ключ реестра LocalAccountTokenFilterPolicy для разрешения удаленного доступа с вашего компьютера. Для установки этого ключа используется следующая команда, которую нужно ввести в командной строке с привилегиями администратора:
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
Для включения удаленного управления воспользуйтесь следующей командой, которую нужно ввести в командной строке с правами администратора: configure-SMRemoting.exe –enableЕсли нужно удаленно управлять компьютером, работающим на базе Windows 8, введите команду winrm quickconfig (управление производится с использованием протокола WS-Management). На все задаваемые вопросы нужно ответить Y. В результате будет запущена служба Удаленное управление Windows (WinRM) и настроена на прием запросов WS-Management с любого IP-адреса, созданы исключения брандмауэра для удаленного управления Windows, а также настроен ключ LocalAccountTokenFilterPolicy для предоставления соответствующих административных прав для удаленного управления.
Множество иных типов удаленного управления зависит от других исключений брандмауэра Windows.

- Удаленный рабочий стол (Remote Desktop) - может быть включен/отключен отдельно от удаленного администрирования. Чтобы разрешить другим пользователям подключаться к локальному серверу с использованием удаленного рабочего стола, нужно разрешить соответствующие соединения к компьютеру и настроить доступ к нему (см. главу 4).
- Удаленное управление службами (Remote Service Management) - используется для удаленного управления службами компьютера, должно быть создано соответствующее правило Брандмауэра Windows. В дополнительных параметрах брандмауэра есть несколько правил, разрешающих управление, например, Удаленное управление

службой (RPC) и Удаленное управление службой (именованные каналы, NP).

- Удаленное управление журналом событий - должно быть настроено как разрешенное приложение Брандмауэра Windows для удаленного управления журналом событий компьютера. В дополнительных параметрах брандмауэра есть несколько соответствующих правил, разрешающих управление с помощью технологий NP (Named Pipes) и RPC (Remote Procedure Call).
- Удаленное управление томами - должно быть настроено как разрешенное управление Брандмауэром Windows для удаленного управления томами. В дополнительных параметрах брандмауэра есть несколько соответствующих правил: Управление удаленными томами - служба виртуальных дисков, Управление удаленными томами - загрузчик службы виртуальных дисков.
- Удаленное управление назначенными задачами - должно быть настроено как разрешенное приложение Брандмауэра Windows, чтобы удаленно управлять назначенными задачами компьютера. В дополнительных настройках брандмауэра есть несколько соответствующих правил, которые разрешают управление назначенными задачами через RPC.

По умолчанию включено лишь исключение Удаленное управление службами.

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

Подключение и работа с удаленными серверами

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

1. Откройте диспетчер серверов. В левой панели выберите пункт Все серверы для просмотра всех добавленных для управления серверов. Если необходимого сервера нет в списке, в меню Управление (Manage) выберите команду Добавление серверов (Add Servers). Откроется одноименное диалоговое окно.
2. В окне Добавление серверов есть две панели:
    - Active Directory (выбрана по умолчанию) - позволяет ввести короткое или полное имя удаленного сервера, работающего под управлением Windows Server. Введите имя сервера и нажмите кнопку Найти (Find Now);
    - DNS — позволяет добавить серверы по имени или IP-адресу. Введите имя или IP-адрес и нажмите кнопку Поиск (Search).
3. Дважды щелкните на найденном сервере для помещения его в список Выбрано (Selected).
4. Повторите действия 2-3 для добавления других серверов. Нажмите кнопку OK. Для добавления сразу нескольких серверов в диспетчер серверов применяется процесс импорта:

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

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

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

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

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

1. Откройте диспетчер серверов. В меню Управление выберите команду Создание группы серверов (Create Server Group) для отображения одноименного окна.
2. Введите имя группы. Используйте панели и параметры, предназначенные для добавления серверов в группы. Помните о следующем.

- Панель Пул серверов (Server Pool) выбирается по умолчанию, выводит серверы, уже добавленные для управления. Если сервер, который нужно добавить в группу, есть в этом списке, добавьте его в группу с помощью двойного нажатия или двойного щелчка.
- Панель Active Directory позволяет ввести полное или сокращенное имя удаленного сервера, работающего под

управлением Windows Server. После того как введете имя, нажмите кнопку Найти (Find Now). В списке имен выберите сервер и с помощью двойного нажатия или двойного щелчка добавьте его в список Выбрано (Selected).

- Панель DNS позволяет добавить серверы по имени компьютера или IP-адресу. Введите IP-адрес или имя и нажмите кнопку Поиск (Search). В списке серверов дважды щелкните по серверу для его добавления в список Выбрано.
- Панель Импорт (Import) позволяет импортировать список серверов. Нажмите кнопку выбора файла справа от поля Файл (File), затем используйте окно открытия, чтобы открыть список серверов. В списке Компьютер (Computer) дважды щелкните по серверу, чтобы добавить его в список Выбрано.

3. Нажмите кнопку OK для создания группы сервера.

При щелчке правой кнопкой мыши по имени сервера на панели Серверы (в группе серверов или в представлении Все серверы) будет отображен расширенный список команд управления. Все эти команды позволяют выполнить соответствующее действие или открыть соответствующую утилиту управления для выбранного сервера. Например, если щелкнуть правой кнопкой мыши по серверу CorpServer172, а затем выбрать команду Управление компьютером (Computer Management), оснастка Управление компьютером подключится к CorpServer172 и откроет его.

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

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

enter-pssession server85 –credential williams

Добавление и удаление ролей, ролевых служб и компонентов

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

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

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

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

Для управления службой щелкните правой кнопкой мыши по службе и выберите одну из команд: Остановить службы (Stop Service), Запустить службы (Start Service), Приостановить службы (Pause Service), Перезапустить службы (Restart Service), Возобновить работу служб (Resume Service). Во многих случаях, если служба не работает, можно использовать команду Перезапустить службы (Restart Service): служба будет сначала остановлена, а потом запущена.

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.
4. В списке серверов (шаг 3) будут только серверы под управлением Windows Server 2012 и те, которые администратор добавил в диспетчере серверов.
5. 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.
6. 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.
7. Нажмите кнопку Добавить компоненты для закрытия этого окна и установки требуемых компонентов на сервер. По окончанию выбора компонентов нажмите кнопку Далее.
5. 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).
6. На странице Подтверждение установки компонентов (Confirm) щелкните по ссылке Экспорт параметров конфигурации (Export Configuration Settings) для создания отчета установки, который можно просмотреть в Internet Explorer.
7. Если сервер, на котором необходимо установить роли или компоненты не обладает всеми необходимыми двоичными файлами, сервер получит их через Центр обновления Windows (по умолчанию) или из

местоположения, указанного групповой политикой. Можно также указать альтернативный источник для файлов. Для этого щелкните по ссылке Указать альтернативный исходный путь (Specify An Alternate Source Path), в появившемся окне укажите альтернативный путь и нажмите кнопку OK. Например, образ Windows смонтирован и сделан доступным на локальном сервере, как было показано в разд. "Основные компоненты диспетчера серверов и двоичные файлы" ранее в этой главе, можно ввести альтернативный путь в виде c:\mountdir\windows\winsxs.

8. 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\WinServer212\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.

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

1. (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, 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.

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.

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

Из консоли Система можно открыть окно Свойства системы, которое используется для управления различными свойствами системы. Для этого щелкните по ссылке Изменить параметры в области Имя компьютера, имя домена и параметры рабочей группы.

В следующих разделах мы рассмотрим ключевые области операционной системы, которые можно настроить с помощью окна Свойства системы.

Вкладка *Имя компьютера*

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

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

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

1. Для изменения имени компьютера выполните следующие действия:

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

Вкладка *Оборудование*

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

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

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

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

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

Вкладка *Дополнительно*

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

Настройка быстродействия Windows

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

1. Активизируйте вкладку Дополнительно (Advanced), а затем нажмите кнопку Параметры (Settings) в группе Быстродействие (Performance).
2. По умолчанию будет выбрана вкладка Визуальные эффекты (Visual Effects) окна Параметры быстродействия. Для контроля визуальных эффектов доступны следующие опции.

- Пусть Windows выберет, что лучше для моего компьютера (Let Windows Choose What’s Best For My Computer) - операционная система выберет оптимальные настройки быстродействия на основании вашей аппаратной конфигурации. Для новых компьютеров эта опция, возможно, будет идентична выбору Обеспечить наилучший вид (Adjust For Best Appearance). Разница заключается в том, что эта опция бу-дет выбрана операционной системой на основании соответствующих требований к аппаратным возможностям компьютера.

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

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

Настройка быстродействия приложений

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

1. Активизируйте вкладку Дополнительно окна Свойства системы, затем откройте окно Параметры быстродействия (Performance Options), нажав кнопку Параметры в группе Быстродействие.
2. В окне Параметры быстродействия (Performance Options) переключитесь на вкладку Дополнительно (Advanced).
3. На панели Распределение времени процессора (Processor Scheduling) находятся две опции:

- программ (Programs) - используется, чтобы предоставить активным приложениям наилучшее время отклика и большую часть доступных ресурсов. Этот вариант подойдет для серверов разработки или при использовании Windows Server 2012 как настольной операционной системы;
- служб, работающих в фоновом режиме (Background Services) - используйте эту опцию, чтобы предоставить фоновым приложениям лучшее время отклика, чем у активных приложений. Это оптимальная опция для сервера.

4. Нажмите кнопку OK.

Настройка виртуальной памяти

С помощью виртуальной памяти дисковое пространство может использоваться для расширения объема памяти, доступной в системе путем использования жесткого диска как части системной памяти. Эта функция записывает содержимое ОЗУ на диски, используя процесс, называемый подкачкой.

Подкачка записывает определенный объем ОЗУ, скажем 8192 Мбайт, на диск в файл подкачки. Файл подкачки используется, когда нужно место в физическом ОЗУ.
Начальный файл подкачки создается автоматически для диска, содержащего операционную систему. По умолчанию на других дисках нет файлов подкачки, но при необходимости их можно создать. При создании файла подкачки устанавливается его максимальный размер. Файлы подкачки хранятся в корневом каталоге тома и называются Pagefile.sys.
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). 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.

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

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

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

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

При обновлении параметров используемого в данный момент файла подкачки будет выведено сообщение о необходимости перезагрузки сервера (чтобы изменения вступили в силу). Нажмите кнопку OK. После закрытия окна Свойства системы будет предложено перезагрузить систему. На

производственном сервере нужно запланировать эту перезагрузку вне рабочего времени.

Настройка предотвращения выполнения данных

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

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

Использование и настройка DEP

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

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

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

1. Активизируйте вкладку Дополнительно окна Свойства системы, затем откройте окно Параметры быстродействия, нажав кнопку Параметры в группе Быстродействие.

2. В окне Параметры быстродействия перейдите на вкладку Предотвращение выполнения данных. 3. Чтобы добавить программу как исключение, нажмите кнопку Добавить. Появится окно

3. Открыть (Open), выберите исполняемый файл программ и нажмите кнопку Открыть.

4. Для временного удаления программы из списка исключений (например, для решения проблем) отметьте флажок возле имени программы.

5. Для удаления программы из списка исключений щелкните на программе и нажмите кнопку Удалить (Remove).

6. Нажмите кнопку OK для сохранения изменений. DEP-совместимость

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

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

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

Настройка системных и пользовательских переменных среды

Windows использует переменные среды для отслеживания важных строк, например, пути поиска файлов или имени узла контроллера домена. Переменные среды, предназначенные для использования самой системой Windows, называются системными переменными среды.

Они одинаковы для всех, вне зависимости от того, кто вошел в систему на определенном компьютере. Переменные среды, определенные для применения пользователями или программами, называются пользовательскими переменными среды. Они различны для каждого пользователя конкретного компьютера. Настроить системные и пользовательские переменные среды можно с помощью окна Переменные среды (Environment Variables). 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 Новая пользовательская переменная (New User Variable) или Новая системная переменная (New System Variable) соответственно.
2. В поле Имя переменной (Variable Name) введите имя переменной, а в поле Значение переменной (Variable Value) - ее значение.
3. Нажмите кнопку OK.

Редактирование переменной среды

Для редактирования значения переменной среды выполните такие действия:

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

Удаление переменной среды

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

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

Настройка загрузки и восстановления системы

Настроить параметры загрузки и восстановления системы можно в окне Загрузка и восстановление (Startup And Recovery) (рис. 2.8). Чтобы открыть это

окно, откройте окно Свойства системы и перейдите на вкладку Дополнительно, а затем нажмите кнопку Параметры в группе Загрузка и восстановление (Startup And Recovery).

Установка параметров загрузки

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

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

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

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

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

Определение параметров восстановления

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

- Записать событие в системный журнал (Write An Event To The System Log) - протоколирует ошибку в системный журнал, позволяя администраторам просмотреть последнюю ошибку с помощью утилиты Просмотр событий (Event Viewer);

- Выполнить автоматическую перезагрузку (Automatically Restart) - выберите эту опцию, чтобы перезагрузить систему в случае возникновения фатальной ошибки.

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.

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 свободного 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.

Глава 2. Автоматизация административных задач, политики и процедуры

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

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

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

4. Удаленный помощник (Remote Assistance) предоставляет компонент, позволяющий администратору отправлять приглашение удаленного помощника более старшему администратору. Старший администратор может принять приглашение просмотреть рабочий стол пользователя и получить временный контроль над компьютером для решения проблемы. После установки этого компонента на сервер с помощью Мастера добавления ролей и компонентов управлять им можно с помощью вкладки Удаленный доступ (Remote) окна свойств системы. В Панели управления перейдите в категорию Система и безопасность и щелкните по ссылке Настройка удаленного доступа (Allow Remote Access) в заголовке Система (System) для просмотра соответствующих параметров.
5. Удаленный рабочий стол (Remote Desktop) предоставляет функцию удаленной связи, позволяющую подключаться и управлять сервером с другого компьютера. По умолчанию удаленный рабочий стол установлен, но не включен на серверах под управлением Windows Server 2012. Управлять конфигурацией удаленного рабочего стола можно на вкладке Удаленный доступ окна свойств системы. Чтобы просмотреть относящиеся к компоненту параметры, перейдите в категорию Система и безопасность Панели управления и щелкните по ссылке Настройка удаленного доступа. Установить удаленные соединения можно с помощью утилиты Подключение к удаленному рабочему столу (Remote Desktop Connection).
6. Планировщик заданий (Task Scheduler) разрешает запланированное выполнение одноразовых и повторяющихся задач, например, задач по рутинному обслуживанию. ОС Windows Server 2012 предполагает широкое применение средств запланированных заданий. С запланированными заданиями можно работать в оснастке Управление компьютером. Разверните узел Служебные программы (System Tools), затем — Планировщик заданий | Библиотека планировщика заданий (Task Scheduler | Task Scheduler Library) для просмотра настроенных заданий.
7. Возможности рабочего стола (Desktop Experience) — это подкомпонент компонента Пользовательские интерфейсы и инфраструктура (User Interfaces And Infrastructure), позволяющий установить функциональность рабочего стола Windows на сервере. Этот компонент можно установить, если Windows Server 2012 используется в качестве настольной операционной системы. После добавления этого компонента с помощью Мастера добавления ролей и компонентов функциональность рабочего стола сервера будет расширена, а также будут установлены следующие программы: Проигрыватель Windows Media (Windows Media Player), темы оформления рабочего стола, Видео для Windows (поддержка AVI) (Video for Windows), Защитник Windows (Windows Defender), Очистка

диска (Disk Cleanup), Звукозапись (Sound Recorder), Таблица символов (Character Map), Ножницы (Snipping Tool).

8. Брандмауэр Windows (Windows Firewall) помогает защитить компьютер от атаки неавторизированными пользователями. В состав Windows Server входит базовый брандмауэр, называемый Брандмауэр Windows (Windows Firewall), и расширенный брандмауэр, который называется Брандмауэр Windows в режиме повышенной безопасности (Windows Firewall With Advanced Security). По умолчанию брандмауэры не включены на серверных инсталляциях. Чтобы получить доступ к базовому брандмауэру, запустите утилиту Брандмауэр Windows из Панели управления. Для получения доступа к расширенному брандмауэру выберите команду Брандмауэр Windows в режиме повышенной безопасности в меню Средства (Tools) диспетчера серверов.
9. Служба времени Windows (Windows Time) синхронизирует системное время с мировым временем, чтобы убедиться в точности системного времени. Можно настроить компьютеры на синхронизацию времени с определенным сервером времени. Способ работы службы времени Windows зависит от того, является ли компьютер членом домена или рабочей группы. В домене для синхронизации времени используются контроллеры домена, и можно управлять этой функцией с помощью групповой политики. В рабочей группе для синхронизации времени применяются серверы времени Интернета, и можно управлять этой функцией через утилиту Дата и время (Date And Time).

Много других компонентов предоставляют службы поддержки. Однако нужны эти дополнительные службы только в определенных сценариях. Например, нужно использовать IPAM-серверы (IP Address Management) для управления пространством IP-адресов и отслеживания тенденции использования IP-адресов. Службы удаленного рабочего стола используются, когда нужно позволить пользователям запускать приложения на удаленном сервере.

Службы развертывания Windows (Windows Deployment Services) нужны, когда требуется автоматизированное развертывание операционных систем на базе Windows. Однако есть одна служба, которую нужно освоить при работе с Windows Server 2012, — это групповая политика.

Панель параметров экрана Пуск содержит опцию Поиск, с помощью которой можно найти приложения, параметры и файлы. При нажатии клавиши <Windows> и вводе текста, он вводится в поле Поиск. Поскольку по умолчанию производится поиск приложений, это позволит быстро найти программу, установленную на сервере.

Во время ввода текста в поле поиска, соответствующие результаты будут выведены на экран. При нажатии клавиши <Enter> Windows выполнит выбранный в настоящий момент результат. Можно использовать поиск приложений, чтобы выполнять программу с определенными параметрами — просто введите команду вместе с ее параметрами и опциями, как будто вы работаете в командной строке.

Если нужно запустить команды Windows PowerShell из окна поиска приложений, то просто введите powershell, а затем введите команду.

Групповая политика

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

- контролировать доступ к Windows-компонентам, системным ресурсам, сетевым ресурсам, утилитам Панели управления, рабочему столу и экрану Пуск (см. разд. "Использование административных шаблонов для установки политик" далее в этой главе);
- создать централизованно-управляемые каталоги для специальных папок, например, для пользовательской папки Документы (см. разд. "Централизованное управление специальными папками" далее в этой главе);
- определить сценарии пользователя и сценарии компьютера, которые будут запускаться в конкретное время (см. разд. "Управление сценариями пользователя и компьютера");
- настроить политики для блокировки учетных записей, параметры паролей, аудита, назначения прав пользователей и безопасности. Большая часть этих тем раскрыта в главе 8. Далее объясняется, как можно применять групповые политики.

Основы групповой политики

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

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

Групповые политики применяются только к системам, работающим под управлением ОС Windows 2000 и более поздних версий Windows. Настройки

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

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

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

Наследование можно переопределить. Для этого можно присвоить настройку политики дочернему контейнеру, которая отличается от настройки политики для родительского контейнера. Пока переопределение разрешено (т. е. пока оно не заблокировано), будет применяться установка политики дочернего контейнера. Дополнительную информацию о переопределении и блокировании GPO см. в разд. "Блокирование, переопределение и отключение политик" далее в этой главе.

Порядок применения множественных политик

Когда существуют множественные политики, они применяются в следующем порядке:

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

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

Когда применяются групповые политики?

Настройки групповой политики разделены на две категории:

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

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

1. Запускается сеть, и Windows Server применяет политики компьютера. По умолчанию политики компьютера применяются по одной в указанном ранее порядке. При обработке политик компьютера на экран не выводятся какие-либо сообщения, свидетельствующие об этом.
2. Windows Server выполняет загрузочные сценарии. По умолчанию загрузочные сценарии выполняются по одному: следующий сценарий запускается с небольшим тайм-аутом после завершения работы предыдущего сценария. О выполнении сценариев также ничего не сообщается пользователю, если не определено обратное.
3. Пользователь входит в систему. После проверки пользователя Windows Server загружает его профиль.
4. Windows Server применяет политики пользователя. По умолчанию пользовательские политики применены по одной в указанном ранее порядке. При обработке пользовательских политик интерфейс пользователя выводит соответствующие сообщения.
5. Windows Server выполняет сценарии входа в систему. По умолчанию сценарии входа в систему для групповой политики выполняются одновременно. О выполнении сценариев входа в систему пользователю ничего не сообщается, если не определено обратное. Сценарии из ресурса Netlogon выполняются последними в окне командного процессора.
6. Windows Server выводит на экран интерфейс оболочки, настроенный в групповой политике.
7. По умолчанию групповая политика обновляется, когда пользователь выходит из системы, во время перезапуска компьютера и автоматически каждые 90—120 минут. Можно изменить это поведение, устанавливая интервал обновления групповой политики (см. разд. "Обновление групповой политики" далее в этой главе). Чтобы сделать это, откройте окно командной строки и введите команду gpupdate .

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

перезагружен. Для этого можно ввести в командной строке или в поле поиска команду gpupdate /boot.

Требования групповой политики и совместимость версий

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

Вообще говоря, большинство политик прямо совместимо. Это означает, что, как правило, политики, представленные в Windows Server 2003, могут использоваться на Windows 7 и более поздних версиях, а также на Windows Server 2008 и более поздних версиях. Это также означает, что политики для Windows 8 и Windows Server 2012 обычно не применимы к более ранним версиям Windows. Если политика не применима к определенной версии операционной системы Windows, нельзя применить ее на компьютерах, работающих под этими версиями Windows. Как узнать, поддерживается ли политика на определенной версии Windows? Очень просто. Для каждой настройки политики в окне ее свойств есть поле Поддерживается (Supported On). В нем и описаны разные версии Windows, на которых эта политика будет работать.

Окно свойств не нужно открывать, если в редакторе политики выбрана вкладка Расширенный (Extended) (а не вкладка Стандартный (Standard)). Слева от списка политик выводится запись Требования (Requirements), которая содержит сведения совместимости. Также можно установить новые политики при добавлении пакета обновлений (Service Pack), установке приложений и компонентов Windows. Это означает, что будет виден широкий диапазон записей совместимости.

Изменение групповой политики

Чтобы оптимизировать управление групповой политикой, Microsoft удалила функции управления из инструментов Active Directory и переместила их в основную консоль — Управление групповой политикой (Group Policy Management Console, GPMC), которая впервые появилась в Windows Vista и Windows Server 2008. GPMC — это компонент, который можно добавить в любую установку Windows Server 2008 (или более позднюю версию) с помощью мастера добавления ролей и компонентов. Консоль GPMC будет доступна в Windows Vista (и более поздних версиях), если установить Remote Server Administration Tools (RSAT). Как только консоль GPMC будет установлена, ее команда будет доступна в меню Средства в диспетчере серверов. Если нужно отредактировать объект групповой политики в GPMC, консоль GPMC открывает редактор Управление групповой политикой (Group Policy Management Editor), который используется для управления настройками политики. Если бы Microsoft остановилась на этих двух инструментах, у нас

была бы замечательная и простая в использовании среда управления политикой. К сожалению, существуют почти идентичные редакторы.

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

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

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

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

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

ADMX-файлы делятся на две группы: с расширением admx (не зависят от языка) и с расширением adml (зависят от языка). Не связанный с языком файл

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

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

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

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

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

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

Компьютеры под управлением Windows Vista (или более поздних версий) не используют функциональность журналирования трассировки в Userenv.dll и вместо этого записывают сообщения о событиях групповой политики в журнал Система (System). Далее, вместо журнала Userenv используется операционный

журнал групповой политики. В оснастке Просмотр событий можно получить доступ к операционному журналу так: Журналы приложений и служб\Microsoft\Windows\GroupPolicy (Applications And Services Logs\ Microsoft\Windows\GroupPolicy).
Компьютеры под управлением Windows Vista (и более поздних версий) используют службу NLA (Network Location Awareness) вместо протокола ICMP (Internet Control Message Protocol, ping). Благодаря NLA, компьютер знает тип сети, к которой он подключен, и может быстро реагировать на изменения состояния системы или конфигурации сети. Используя NLA, клиент групповой политики может определить состояние компьютера, состояние сети и доступность пропускной способности сети для определения медленного соединения.

Управление локальными групповыми политиками

Компьютеры под управлением Windows Vista и более поздних версий позволяют использовать несколько локальных GPO на одном компьютере (пока компьютер не является контроллером домена). Ранее у компьютеров был только один локальный GPO. Windows позволяет присваивать отдельный локальный GPO каждому локальному пользователю или типу пользователей. Это дает возможность сделать применение политики более гибким и поддерживает более широкий диапазон сценариев реализации.

Локальные объекты групповой политики

Когда компьютеры используются в автономной конфигурации, а не в конфигурации домена, можно обнаружить, что множественный локальный GPO полезен, поскольку больше не нужно явно отключать или удалять настройки, которые вмешиваются в управление компьютером перед выполнением административных задач. Вместо этого можно реализовать один локальный GPO для администраторов и другой локальный GPO для обычных пользователей. В конфигурации домена, однако, нельзя использовать множественный GPO. В доменах большинство компьютеров и пользователей уже имеют множественные GPO, примененные к ним, а добавление множественных локальных GPO сделает управление групповой политикой слишком запутанным.
Компьютеры под управлением Windows Vista и более поздних выпусков имеют три уровня локальных объектов групповой политики.

- Локальная групповая политика (Local Group Policy). Это только локальный GPO, позволяющий конфигурациям компьютера и пользователя применяться ко всем пользователям компьютера.
- Административная и неадминистративная локальная групповая политика (Administrators and Non-Administrators local Group Policy). Содержит только настройки конфигурации пользователя и применяется на основании того, является ли учетная запись членом локальной группы Администраторы.

– Пользовательская локальная групповая политика (User-specific local Group Policy). Содержит только конфигурацию пользователя и применяется к отдельным пользователям и группам.

Эти уровни локальных GPO обрабатываются в следующем порядке: локальная групповая политика, административная и неадминистративная локальная групповая политика и пользовательская групповая политика.

Поскольку доступные настройки пользовательской конфигурации одинаковы для всех локальных GPO, настройки в одном GPO могут конфликтовать с настройками в другом GPO.

ОС Windows разрешает конфликты в настройках, перезаписывая любые предыдущие настройки настройками, считанными последними. Windows использует последнее установленное значение. Когда Windows разрешает конфликты, имеет значение только включенное/выключенное состояние настроек. Значение Не задано (Not Configured) не оказывает никакого эффекта на состояние настройки из предыдущего приложения политики. Чтобы упростить администрирование домена, можно отключить обработку локальных GPO на компьютерах под управлением Windows Vista и более поздних версий, включив политику Выключение обработки локальных объектов групповой политики (Turn Off Local Group Policy Objects Processing) в GPO домена. Эта настройка находится в узле Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\ Administrative Templates\System\Group Policy) групповой политики.

Получение доступа к настройкам локальной политики верхнего уровня

На всех компьютерах под управлением текущих выпусков Windows есть локальный GPO, доступный для редактирования. Хотя на контроллере домена тоже есть локальный GPO, его настройки редактировать не нужно.

Самый быстрый способ получить доступ к локальному GPO компьютера — это ввести следующую команду в командной строке или поле поиска приложений:
gpedit.msc /gpcomputer: "%ComputerName%"

Поскольку команде передаются дополнительные аргументы, команду в таком виде нельзя использовать в оболочке PowerShell. Чтобы выполнить ее в оболочке PowerShell, нужно заключить ее аргументы в одинарные кавычки и в таком виде передать команду, например: gpedit.msc '/gpcomputer: "%ComputerName%"'.

Эта команда запускает GPOE в консоли управления Microsoft (MMC), а в качестве цели выступает локальный компьютер. Здесь "%ComputerName%" - переменная окружения, содержащая имя локального компьютера. Она должна быть заключена в двойные кавычки, как показано выше. Для получения доступа к локальному GPO верхнего уровня удаленного компьютера введите следующую команду в командной строке или поле поиска приложений:
gpedit.msc /gpcomputer: "RemoteComputer"

Здесь RemoteComputer — имя или полное имя (FQDN) удаленного компьютера. Снова необходимо использовать двойные кавычки, как показано в следующем примере:

gpedit.msc /gpcomputer: "corpsvr82"
Также можно управлять локальным GPO верхнего уровня с помощью следующих действий:

1. В командной строке или поле поиска приложений введите mmc .
2. В консоли управления Microsoft (MMC) выберите команду Файл | Добавить или удалить оснастку (File | Add/Remove Snap-In).
3. В диалоговом окне Добавление или удаление оснасток (Add Or Remove Snap-Ins) выберите оснастку Редактор объектов групповой политики (Group Policy Object Editor) и нажмите кнопку Добавить (Add).
4. В окне Выбор объекта групповой политики (Select Group Policy Object) нажмите кнопку Готово, поскольку по умолчанию будет использоваться объект локального компьютера. Нажмите кнопку OK.

Теперь можно управлять локальными настройками политики. Можно использовать одну и ту же оснастку MMC для управления более чем одним локальным GPO. В диалоговом окне Добавление или удаление оснасток просто добавьте по одному экземпляру оснастки Редактор объектов групповой политики (Group Policy Object Editor) для каждого объекта, с которым нужно работать.

Настройки локального объекта групповой политики

Локальные групповые политики хранятся в папке %SystemRoot%\System32\GroupPolicy на каждом компьютере с Windows Server. В этой папке находятся следующие подпапки:

- Machine — содержит сценарии компьютера в папке Script и информацию политики на базе реестра для раздела HKEY_LOCAL_MACHINE (HKLM) в файле Registry.pol;
- User — хранит сценарии пользователя в папке Script и информацию политики на базе реестра для раздела HKEY_CURRENT_USER (HKCU) в файле Registry.pol.

Не нужно редактировать эти папки и файлы вручную! Вместо этого используйте соответствующие функции одной из утилит групповой политики. По умолчанию эти файлы и папки скрыты. Если нужно просмотреть скрытые файлы и папки в Проводнике Windows, перейдите на вкладку Вид (View) окна Параметры папок (Folder Options) и установите флажок Показать или скрыть | Скрытые элементы (Hidden Items). Также можно отметить флажок Расширения имен файлов (File Name Extensions). Открыть это окно можно, выбрав команду меню Вид | Параметры.

Получение доступа к административной и неадминистративной политике и пользовательской политике

По умолчанию единственный локальный объект политики, существующий на компьютере, является локальным объектом групповой политики. Можно создать и управлять другими объектами при необходимости (за исключением объектов на контроллерах доменов). Можно создать или получить доступ к

административному объекту локальной групповой политики, к неадминистративному объекту локальной групповой политики и объекту пользовательской локальной групповой политики так:
1. В командной строке или в поле поиска приложений введите mmc и нажмите клавишу <Enter>. В консоли управления Microsoft выберите команду меню Файл | Добавить или удалить оснастку.
2. В диалоговом окне Добавление или удаление оснасток выберите оснастку Редактор объектов групповой политики и нажмите кнопку Добавить.
3. В окне Выбор объекта групповой политики нажмите кнопку Обзор. В окне Поиск объекта групповой политики (Browse For A Group Policy Object) перейдите на вкладку Пользователи (Users).
4. На вкладке Пользователи (Users) в колонке Объект групповой политики существует (Group Policy Object Exists) приводятся сведения о том, существует ли объект групповой политики для того или иного пользователя. Выполните следующие действия.

- Выберите запись Администраторы (Administrators) для создания или получения доступа к объекту административной локальной групповой политики.
- Выберите запись Не администраторы (Non-Administrators) для создания или полуения доступа к объекту административной локальной групповой политики.
- Выберите локального пользователя для создания или получения доступа к пользовательскому локальному GPO.

5. Нажмите кнопку OK. Если выбранный объект не существует, он будет создан. В противном случае будет открыт существующий объект для просмотра и редактирования.
Параметры политики для администраторов, неадминистраторов и пользователей хранятся в папке %SystemRoot%\System32\GroupPolicyUsers на каждом компьютере под управлением Windows Server. Поскольку эти локальные GPO применяются только к конфигурации пользователя, в папке %SystemRoot%\System32\GroupPolicyUsers находится подпапка User, а в ней будут сценарии в папке Script, а также информация реестра для раздела HKEY_CURRENT_USER в файле Registry.pol.

Управление политиками сайта, домена и организационного подразделения

При разворачивании сервисов Active Directory (AD DS) можно использовать групповую политику на базе Active Directory. Каждый сайт, домен и организационное подразделение могут иметь одну или больше групповых политик. У групповых политик, перечисленных выше в списке групповой политики, более высокий приоритет, чем у политик, перечисленных ниже в списке. Это позволяет удостовериться, что политики применены всюду по связанным сайтам, доменам и организационным подразделениям.

Политики домена и политики по умолчанию

У каждого домена в организации по умолчанию есть два GPO.

- GPO политики контроллера домена по умолчанию (Default Domain Controllers Policy GPO) создается и связывается для организационного подразделения контроллера домена. Этот GPO применим ко всем контроллерам домена в домене (до тех пор, пока они не будут перемещены из этого организационного подразделения). Используйте его для управления параметрами безопасности для контроллеров доменов в этом домене.
- GPO политики домена по умолчанию (Default Domain Policy GPO) создается и связывается для всего домена в пределах Active Directory. Используйте этот GPO для установки базовых значений для широкого круга настроек политик, которые применяются ко всем пользователям и компьютерам в домене.

Как правило, GPO политики домена по умолчанию — GPO высшего приоритета, связанный с уровнем домена. GPO политики контроллеров домена по умолчанию — GPO высшего приоритета, связанный с контейнером контроллеров домена. Можно присоединить дополнительные GPO уровня домена и контроллеров домена. При этом настройки в GPO наивысшего приоритета переопределяют настройки в объектах групповой политики более низкого приоритета. Эти GPO не предназначены для общего управления групповой политикой.

GPO политики домена по умолчанию используется только для управления настройками дефолтовых политик учетных записей, и, в частности, есть три области применения политик учетных записей: политика паролей, политика блокировки учетной записи и политика Kerberos. Через этот GPO можно управлять несколькими параметрами безопасности: Учетные записи: Переименование учетной записи администратора (Accounts: Rename Administrator Account), Учетные записи: Состояние учетной записи 'Администратор' (Accounts: Administrator Account Status), Учетные записи: Состояние учетной записи 'Гость' (Accounts: Guest Account Status), Учетные записи: Переименование учетной записи гостя (Accounts: Rename Guest Account), Сетевая безопасность: Принудительный вывод из сеанса по истечению допустимых часов (Network Security: Force Logoff When Logon Hours Expire), Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля (Network Security: Do Not Store LAN Manager Hash Value On Next Password Change).

Один из способов перезаписи этих настроек — создать GPO с соответствующими настройками и присоединить его к контроллеру домена с более высоким приоритетом. Объект GPO политики контроллера домена по умолчанию содержит параметры Назначение прав пользователя (User Rights Assignment) и Параметры безопасности (Security Options), которые ограничивают способы использования контроллеров домена. Один из способов перезаписи этих настроек — создать GPO с перезаписывающимися

настройками и присоединить его к контейнеру контроллеров домена с более высоким приоритетом.
Для управления другими областями политики нужно создать GPO и присоединить его к домену или соответствующему организационному подразделению в пределах домена.
Групповые политики сайта, домена и организационного подразделения хранятся в папке %SystemRoot%\Sysvol\Domain\Policies на контроллере домена. В этой папке находится по одной подпапке для каждой политики, определенной на контроллере домена. Имя папки политики — это уникальный глобальный идентификатор политики (GUID). Можно найти GUID политики на странице Свойства (Properties) вкладки Общие (General) раздела Сводка (Summary).
Внутри этих отдельных папок политик находятся следующие подпапки:

- Machine — содержит сценарии компьютера в папке Script и информацию реестра для раздела HKEY_LOCAL_MACHINE (HKLM) в файле Registry.pol;
- User — содержит сценарии пользователя в папке Script и информацию реестра для раздела HKEY_CURRENT_USER (HKCU) в файле Registry.pol.

Не редактируйте эти папки и файлы вручную. Вместо этого используйте соответствующие компоненты одной из утилит управления групповой политикой.

Консоль управления групповой политикой

Запустить консоль управления групповой политикой (GPMC) можно из меню Средства (Tools) диспетчера серверов. Также можно в командной строке или в поле поиска приложений ввести gpmc.msc и нажать клавишу <Enter>.
Используйте консоль управления групповой политикой для работы с объектом групповой политики сайта, леса и домена
Корневой узел консоли называется Управление групповой политикой (Group Policy Management), а ниже есть узел Лес (Forest). Узел Лес представляет лес, к которому консоль подключена в настоящий момент, и называется именем корневого домена этого леса (например, лес: HOME.DOMAIN). Если существуют соответствующие учетные данные, можно добавить соединения с другими лесами. Для этого щелкните пра-вой кнопкой мыши по узлу Управление групповой политикой и выберите команду Добавить лес (Add Forest). В диалоговом окне Добавление леса (Add Forest) введите имя корневого домена леса в поле Домен (Domain) и нажмите кнопку OK. В узле Лес находятся следующие узлы.

- Домены (Domains) — предоставляет доступ к параметрам политики для доменов в соответствующем лесе. По умолчанию консоль подключена к домену входа в систему. Если есть другие учетные данные, можете добавить соединения с другими доменами в связанном лесу. Для этого щелкните правой кнопкой мыши по узлу Домены и выберите команду Показать домены (Show Domains). В окне

Отображение доменов (Show Domains) выберите домены, которые нужно добавить, и нажмите кнопку OK.

- Сайты (Sites) — предоставляет доступ к настройкам политики для сайтов в соответствующем лесе. Сайты скрыты по умолчанию. Если есть соответствующие учетные данные, можно подключиться к сайтам. Для этого щелкните правой кнопкой мыши на узле Сайты и выберите команду Показать сайты (Show Sites). В окне Отображение сайтов (Show Sites) выберите сайты, которые нужно добавить, и нажмите кнопку OK.
- Моделирование групповой политики (Group Policy Modeling) — предоставляет доступ к мастеру моделирования групповой политики (Group Policy Modeling Wizard), который поможет спланировать развертывание групповой политики и симулировать настройки с целью тестирования. Также доступны любые сохраненные модели.
- Результаты групповой политики (Group Policy Results) — предоставляет доступ к мастеру результатов групповой политики (Group Policy Results Wizard). Для каждого домена, к которому подключена консоль, все связанные объекты групповой политики и организационные подразделения доступны для работы в одном месте.

Объекты GPO, перечисленные в контейнерах Домены, Сайты в GPMC, являются ссылками на GPO, а не самими GPO. Доступ к фактическому GPO можно получить через контейнер Объекты групповой политики (Group Policy Objects) выбранного домена. Обратите внимание на то, что у значков ссылок на GPO есть небольшие стрелки в левом нижнем углу, подобно ярлыку, а на значках самих GPO таких стрелок нет.

При запуске консоль GPMC подключится к Active Directory, запущенному на контроллере домена, который работает как PDC-эмулятор для домена входа и получает список всех объектов групповой политики и организационных подразделений в этом домене. Это возможно благодаря протоколам LDAP (Lightweight Directory Access Protocol) для доступа к хранилищу каталогов и SMB (Server Message Block) для доступа к каталогу SYSVOL. Если PDCэмулятор недоступен по какой-то причине, например, когда сервер находится в режиме оффлайн, GPMC отобразит подсказку, чтобы можно было работать с настройками политик на любом другом доступном контроллере домена. Для смены контроллера домена щелкните правой кнопкой мыши на узле домена, для которого нужно сменить активный контроллер домена, затем выберите команду Сменить контроллер домена (Change Domain Controller).

В окне Смена контроллера домена (Change Domain Controller) текущий контроллер домена приведен в области Текущий контроллер домена (Current Domain Controller). Используйте область Изменить на (Change To), выберите другой контроллер домена и нажмите кнопку OK.

Знакомство с редактором политик

С помощью консоли GPMC можно отредактировать GPO, щелкнув на нем правой кнопкой мыши и выбрав команду Изменить (Edit).

У редактора политики есть два основных узла:

- Конфигурация компьютера (Computer Configuration) — разрешает использовать политики, которые будут применены к компьютерам, вне зависимости от того, какой пользователь вошел в систему;
- Конфигурация пользователя (User Configuration) — позволяет установить политики, которые будут применены к пользователям, вне зависимости от того, на каких компьютерах они входят в домен.

В узлах Конфигурация компьютера и Конфигурация пользователя находятся узлы Политики (Policies) и Настройки (Preferences). Настройки общих политик находятся в узле Политики. Параметры общих настроек — в узле Настройки.

Когда автор этой книги ссылается на настройки в узле Политики, иногда используется сокращение Конфигурация пользователя\Административные шаблоны\Компоненты Windows (User Configuration\Administrative Templates\Windows Components) вместо Конфигурация пользователя\Политики\Административные шаблоны (User Configuration\ Policies\Administrative Templates: Policy Definitions\Windows Components). То есть рассматриваемая политика находится в узле Конфигурация пользователя (User Configuration), а не в узле Конфигурация компьютера (Computer Configuration) и далее может быть найдена в узле Административные шаблоны\Компоненты Windows (Administrative Templates\ Windows Components).

Точная конфигурация узлов Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration) зависит от установленных расширений и типа созданной политики. В узлах Конфигурация компьютера и Конфигурация пользователя есть следующие подузлы:

- Конфигурация программ (Software Settings) — политики для настроек программного обеспечения. При установке программного обеспечения в узле Конфигурация программ появятся новые подузлы;
- Конфигурация Windows (Windows Settings) — набор политик для перенаправления папок, сценариев и безопасности;
- Административные шаблоны (Administrative Templates) — набор политик для операционной системы, компонентов Windows и программ. Административные шаблоны настраиваются с помощью файлов шаблонов. При необходимости можно добавить или удалить файлы шаблонов.

Использование административных шаблонов для установки политик

Административные шаблоны предоставляют легкий доступ к настройкам реестра, которые можно изменить. Набор административных шаблонов по умолчанию настроен в редакторе политик для пользователей и компьютеров. При необходимости можно добавить/удалить административные шаблоны. Любые изменения, вносимые в политики, доступны через административные шаблоны, сохранены в реестре. Конфигурации компьютера хранятся в разделе

HKEY_LOCAL_MACHINE , а конфигурации пользователя — в разделе HKEY_CURRENT_USER .

Просмотреть настроенные в данный момент шаблоны можно в узле Административные шаблоны редактора политик. Этот узел содержит политики, которые можно сконфигурировать для локальных систем, организационных подразделений, доменов и сайтов. В конфигурации пользователя и конфигурации компьютера находятся разные наборы групповой политики. При установке новых компонентов Windows можно добавить шаблоны с новыми политиками.

Административные шаблоны могут использоваться для управления следующими настройками:

- Панель управления (Control Panel) — содержит настройки Панели управления и ее утилит;
- Рабочий стол (Desktop) — настраивает рабочий стол Windows и доступные опции рабочего стола;
- Сеть (Network) — настраивает сеть и параметры сетевых клиентов для оффлайн-файлов, DNS-клиентов и сетевых соединений;
- Принтеры (Printers) — настраивает параметры принтера, просмотра сети, спула и каталога;
- Общие папки (Shared folders) — разрешает публикацию общих файлов и распределенной файловой системы (DFS);
- Меню "Пуск" и панель задач (Start screen and taskbar) — контролирует доступные опции и конфигурацию экрана Пуск и панели задач;
- Система (System) — настраивает параметры системы для дисковых квот, профилей пользователей, входа пользователя, восстановления системы, отчетов об ошибках и т. д.;
- Компоненты Windows (Windows components) — определяет доступные опции и конфигурацию различных Windows-компонентов, в том числе средства Просмотр событий, Internet Explorer, установщик Windows и обновления Windows.

Просмотрите подузлы узла Административные шаблоны. Политики могут находиться в одном из трех состояний:

- Не задано (Not Configured) — политика не используется, и в реестр не записываются никакие значения;
- Включено (Enabled) — политика применена, ее значение сохранено в реестре;
- Выключено (Disabled) — политика выключена и не применяется, соответствующая настройка записана в реестре.

Для включения, выключения и настройки политики используются следующие действия:

1. В редакторе политик разверните узел Конфигурация пользователя\Администра-
2. тивные шаблоны (User Configuration\ Administrative Templates) или Конфигурация компьютера\Административные шаблоны (Computer

Configuration\Administrative Templates), в зависимости от типа политики, которую планируется использовать.
3. На панели слева выберите подпапку, содержащую политики, с которыми нужно работать. Соответствующие политики будут отображены на правой панели.
4. Дважды щелкните по политике, чтобы открыть окно Свойства. Описание политики можно прочитать на панели Справка (Help). Описание доступно, только если оно определено в соответствующем файле шаблона.
5. Чтобы установить состояние политики, выберите одну из опций:
   - Не задано (Not Configured) — политика не сконфигурирована;
   - Включено (Enabled) — политика включена;
   - Выключено (Disabled) — политика отключена.
6. Если политика включена, установите дополнительные параметры и нажмите кнопку OK.

Обычно в Windows Server у политик компьютера приоритет выше. Если есть конфликт между политикой компьютера и политикой пользователя, применяется политика компьютера.

Создание и связь объекта групповой политики

При работе с объектом политики создание и связь объекта со специфическим контейнером в пределах Active Directory — разные действия. Можно создать GPO и не соединять его ни с каким доменом, сайтом или организационным подразделением. Затем можно создать GPO и подсоединить его к определенному домену, сайту или организационному подразделению.

Также можно создать GPO и соединить его автоматически с доменом, сайтом или организационным подразделением. Выбранный метод зависит, прежде всего, от личных предпочтений и от того, как планируется работа с GPO. Имейте в виду, что при создании GPO и его соединении с доменом, сайтом, организационным подразделением, GPO будет применен к объектам "пользователь" и "компьютер" в этом сайте, домене или организационном подразделении согласно параметрам Active Directory, порядку приоритета GPO и другим параметрам.

Для создания и подсоединения GPO к сайту, домену и организационному подразделению выполните следующие действия:

1. В консоли GPMC разверните узел леса, с которым нужно работать, а затем разверните соответствующий узел Домены и выберите нужный домен.
2. Щелкните правой кнопкой мыши на узле Объекты групповой политики (Group Policy Objects) и выберите команду Создать (New). В окне Новый объект групповой политики (New GPO) введите описывающее имя GPO, например, GPO безопасной рабочей станции. Если нужно использовать исходный GPO в качестве источника для начальных настроек, выберите исходный GPO из списка Исходный объект групповой политики (Source

Starter GPO). После нажатия кнопки OK в контейнер Объекты групповой политики будет добавлен новый GPO.

3. Щелкните правой кнопкой мыши на созданном объекте и выберите команду Изменить (Edit). В редакторе политики установите необходимые параметры и закройте окно редактора политики.
4. В консоли GPMC выберите сайт, домен или организационное подразделение. Раскройте узел Сайты, если нужно работать с ним. На правой панели будет вкладка Связанные объекты групповой политики (Linked Group Policy Objects), которая показывает все GPO, связанные в данный момент с выбранным контейнером (если таковые есть).
5. Щелкните правой кнопкой мыши на сайте, домене или организационном подразделении, к которым нужно привязать GPO, а затем выберите команду Связать существующий объект групповой политики (Link An Existing GPO). В окне Выбор объекта групповой политики выберите GPO, который нужно связать, и нажмите кнопку OK. Когда групповая политика обновится для компьютеров и пользователей в выбранном сайте, домене или организационном подразделении, настройки политики в GPO будут применены.

Создать и связать GPO с помощью одной операции можно так:

1. В консоли GPMC щелкните правой кнопкой мыши на имени сайта, домена или организационного подразделения, к которым нужно привязать GPO, а затем выберите команду Создать объект групповой политики для этого домена и связать его (Create A GPO In This Domain, And Link It Here).
2. В окне Новый объект групповой политики введите описывающее имя GPO, например, GPO безопасной рабочей станции. Если нужно использовать исходный GPO в качестве источника для начальных настроек, выберите исходный GPO из списка Исходный объект групповой политики. После нажатия кнопки OK новый GPO будет добавлен в контейнер Объекты групповой политики и будет связан с ранее выбранным сайтом, доменом или организационным подразделением.
3. Щелкните правой кнопкой мыши (или нажмите) на новом GPO и выберите команду Изменить. В редакторе политики настройки задайте необходимые настройки и закройте редактор политики. Когда групповая политика обновится, будут применены настройки из GPO для сайта, домена или организационного подразделения.

Создание и использование исходных объектов групповой политики

При создании GPO в консоли GPMC в качестве базового объекта можно взять исходный GPO. Настройки из исходного GPO будут импортированы в новый GPO, что позволяет использовать исходный GPO для определения основных параметров конфигурации в новом GPO. В крупной организации нужно создать разные категории исходных объектов групповой политики на основе

пользователей и компьютере, они будут использоваться на требуемой конфигурации безопасности.

Создать исходный GPO можно с помощью следующих действий:

1. В консоли GPMC разверните узел леса, затем с помощью двойного щелчка (или нажатия) разверните нужный подузел узла Домены.
2. Щелкните правой кнопкой мыши по узлу Начальные объекты групповой политики (Starter GPOs), затем выберите команду Создать. В окне Новый стартовый объект групповой политики введите описательное имя для GPO, например, General Management User GPO (имя может быть любым). Можно также ввести комментарии, описывающие назначение GPO. Нажмите кнопку OK.
3. Щелкните правой кнопкой мыши по новому GPO и затем выберите команду Изменить. В редакторе групповой политики настройте необходимые параметры и закройте окно редактора.

Делегирование полномочий для управления групповой политикой

В Active Directory все администраторы имеют некоторый уровень привилегий для осуществления задач управления групповой политикой. С помощью делегации можно предоставить другим пользователям полномочия, чтобы они могли выполнить любые из следующих задач:

- создание GPO и управление созданными GPO;
- настройка представления, изменение настроек, удаление GPO и изменение безопасности;
- управление ссылками на существующие GPO или генерирование RSoP (Resultant Set of Policy).

В Active Directory администраторы могут создавать GPO, и любой создавший GPO имеет право управлять им. В GPMC можно определить, кто может создавать GPO в домене, выбрав узел Объекты групповой политики домена (Group Policy Objects) и перейдя на вкладку Делегирование (Delegation). На этой вкладке отображается список групп и пользователей, которые могут создавать GPO в домене. Для предоставления разрешения на создание GPO пользователю или группе нажмите кнопку Добавить. В окне Выбор: "Пользователь", "Компьютер" или "Группа" (Select User, Computer, Or Group) выберите пользователя или группу и затем нажмите кнопку OK.

В GPMC есть несколько способов определить, кто имеет разрешение на управление групповой политикой. Для домена, сайта и организационного подразделения выберите домен/сайт/организационное подразделение, а затем активизируйте вкладку Делегирование на правой панели (рис. 4.4). В раскрывающемся списке Разрешение (Permission) выберите разрешение, которое нужно проверить

Доступны следующие опции:

- Связанные объекты GPO (Link GPOs) — выводит перечень пользователей и групп, которые могут создавать и управлять ссылками на GPO в выбранном сайте, домене или организационном подразделении;

- Анализ моделирования групповой политики (Perform Group Policy Modeling Analyses) — выводит перечень пользователей и групп, которые могут определять RSoP в целях планирования;
- Чтение результирующих данных групповой политики (Read Group Policy Results Data) — выводит перечень пользователей и групп, которые могут определять текущий RSoP для проверки или протоколирования.

Для предоставления разрешений домену, сайту или организационному подразделению выполните следующие действия:

1. В консоли GPMC выберите домен, сайт или организационное подразделение, с которым планируется работать, а затем перейдите на вкладку Делегирование на правой панели.
2. В раскрывающемся списке Разрешения выберите разрешение, которое нужно предоставить.
3. Нажмите кнопку Добавить. В окне Выбор: "Пользователь", "Компьютер" или "Группа" выберите пользователи или группу и нажмите кнопку OK.
4. В окне Добавление группы или пользователя (Add Group Or User) укажите, как должны применяться разрешения. Для применения разрешений к текущему контейнеру и всем его текущим контейнерам установите переключатель Для этого контейнера и всех дочерних контейнеров (This Container And All Child Containers). Для применения разрешений только к этому контейнеру установите переключатель Только этот контейнер (This Container Only). Нажмите кнопку OK.

Для отдельных разрешений GPO выберите GPO в консоли GPMC, а затем перейдите на вкладку Делегирование на правой панели. Далее выберите одно или несколько разрешений для отдельных пользователей и групп:

- Чтение (Read) — указывает, что пользователь или группа может просматривать объекты групповых политик и их настроек;
- Изменение параметров (Edit Settings) — указывает, что пользователь или группа могут просматривать GPO и изменять его настройки. Пользователь или группа не могут удалить GPO или изменить его параметры безопасности;
- Изменение параметров, удаление и изменение параметров безопасности (Edit Settings, Delete, Modify Security) — пользователь или группа могут просматривать GPO и изменять его настройки. Также пользователь или группа могут удалить GPO и параметры безопасности.

Чтобы предоставить разрешения для работы с GPO, выполните следующие действия:

1. В консоли GPMC выберите GPO, с которым нужно работать, а затем перейдите на вкладку Делегирование на правой панели. Нажмите кнопку Добавить (Add).
2. Для предоставления разрешений GPO пользователю или группе нажмите кнопку Добавить (Add). В окне Выбор: "Пользователь", "Компьютер"

или "Группа" (Select User, Computer, Or Group) выберите пользователи или группу и нажмите кнопку OK.

3. В окне Добавление группы или пользователя (Add Group Or User) выберите уровень разрешений и нажмите кнопку OK.

Блокирование, переопределение и отключение политик

Наследование гарантирует, что каждый объект компьютера и пользователя в домене, сайте или организационном подразделении будет затронут групповой политикой. У большинства политик есть три параметра конфигурации: Не задано (Not Configured), Включено (Enabled), Отключено (Disabled). Состояние Не задано является состоянием по умолчанию для большинства настроек политики. Если политика включена, она применяется непосредственно или посредством наследования ко всем пользователям или компьютерам, которые относятся к политике. Если политика выключена, она не применяется.

Можно изменить способ наследования четырьмя способами:

- изменением порядка ссылки и приоритета;
- переопределением наследования;
- блокированием наследования (чтобы полностью предотвратить наследование);
- принудительным наследованием (чтобы заменить и предотвратить переопределение или блокирование).

Для групповой политики порядок наследования — от уровня сайта до уровня домена, а затем — по каждому уровню организационного подразделения. Надо помнить следующее.

- Когда несколько объектов соединено с определенным уровнем, порядок ссылки определяет порядок применения настроек политики. Сначала применяются политики с низким значением приоритета, затем обрабатываются объекты политики с более высоким рангом. Приоритет — у последнего обработанного объекта политики, поэтому любая настройка политики, созданная в этом объекте политики, будет последней и перезапишет настройки, определенные во всех предыдущих объектах политики (за исключением, если не будет заблокировано наследование или не будет использоваться принудительное наследование).
- Когда несколько объектов политики наследуются от более высокого уровня, порядок приоритета точно показывает, как будут обрабатываться объекты политики. Как и с порядком ссылки, объекты с младшим рангом будут обработаны перед объектами с более высоким рангом. Наивысший приоритет — у последнего обработанного объекта поли-тики, поэтому любая настройка политики, созданная в этом объекте политики, будет последней и перезапишет настройки, определенные во всех предыдущих объектах политики (если не будет заблокировано наследование или не будет использоваться принудительное наследование).

Когда несколько объектов политики связано с определенным уровнем, можно изменить порядок ссылки так:

1. В консоли GPMC выберите контейнер для сайта, домена или организационного подразделения, с которыми нужно работать.
2. На панели справа активизируйте вкладку Связанные объекты групповой политики (Linked Group Policy Objects) (рис. 4.5). Выберите объект политики, с которым нужно работать.
3. Нажмите кнопку Переместить связь вверх (Move Link Up) или Переместить связь вниз (Move Link Down) для изменения порядка ссылки выбранного объекта политики.
4. После того как порядок ссылок будет изменен, проверьте, что объекты политики обрабатываются в ожидаемом порядке, это можно сделать на вкладке Наследование групповой политики (Group Policy Inheritance).

Переопределение наследования является основным методом изменения работы наследования. Когда политика включена в высокоуровневом объекте политики, переопределите наследование, отключив политику в объекте политики низшего уровня. Когда политика отключена в высокоуровневом объекте политики, можно переопределить наследование, включив политику в объекте политики низшего уровня. Пока политика не блокирована или не применяется принудительно, этот метод работает так, как нужно.

Иногда необходимо блокировать наследование так, чтобы никакие настройки политики от контейнеров более высокого уровня не были применены к пользователям и компьютерам в определенном контейнере. Когда наследование заблокировано, будут применены только сконфигурированные настройки политики от объектов политики, связанных с этим уровнем (пока нет принудительного применения политики).

Администраторы домена могут использовать блокирование наследования для блокирования настроек политики от уровня сайта. Администраторы организационных подразделений могут использовать блокирование наследования для блокирования настроек политики от уровня сайта или домена. С помощью блокирования можно обеспечить автономность домена или организационного подразделения, а также убедиться, что администраторы домена или организационного подразделения полностью контролируют политики, которые применяются к пользователям и компьютерам, администрируемым ими.

Для блокирования наследования выполните следующие действия: щелкните правой кнопкой мыши на домене или организационном подразделении, которые не должны наследовать настройки от высокоуровневых контейнеров, и выберите команду Блокировать наследование (Block Inheritance). Если эта команда уже выбрана, для отмены блокирования выберите ее еще раз. Когда наследование блокировано, в GPMC добавляется голубой кружок с восклицательным знаком к значку контейнера, для которого блокируется наследование. Такой значок позволяет быстро понять, блокируется ли наследование для домена/организационного подразделения или нет.

Чтобы администраторы других контейнеров не переопределяли и не блокировали настройки групповой политики, можно использовать принудительное наследование. Когда используется принудительное наследование, все сконфигурированные настройки политики из объектов политики более высокого уровня будут применены независимо от того, что определено в объектах более низкого уровня. Таким образом, блокирование наследования позволяет запретить переопределение или блокирование настроек политики.

Администраторы леса могут использовать принудительное наследование, чтобы убедиться, что настроенные параметры политики уровня сайта будут применены и не будут блокироваться или переопределяться администраторами домена или организационного подразделения. Администраторы домена могут использовать принудительное наследование, чтобы убедиться, что настроенные параметры политики уровня домена будут применены и не будут блокироваться или переопределяться администраторами организационного подразделения.

Используя консоль GPMC, можно принудительно применить наследование так: разверните контейнер высокого уровня, от которого начнется наследование, щелкните правой кнопкой мыши на GPO и выберите команду Принудительный (Enforced). Например, если нужно убедиться, что GPO уровня домена будет наследован всеми организационными подразделениями домена, разверните контейнер домена, щелкните правой кнопкой мыши на GPO контейнера и выберите команду Принудительный. Если команда уже выбрана, выберите ее снова для отмены принудительного наследования. В GPMC можно легко определить, какой GPO наследуется принудительно — к его значку будет добавлено изображение замка́. Также легко можно определить, какие политики вообще наследуются, а какие политики наследуются принудительно. Выберите объект политики в консоли GPMC и затем просмотрите вкладку Область (Scope) на правой панели. Если политика принудительная, в колонке Принудительный области Связи (Links) будет значение Да (Yes), как показано на рис. 4.6.

После того как объект политики будет выбран, можно щелкнуть правой кнопкой мыши на записи в колонке Размещение (Location) вкладки Область (Scope) для отображения контекстного меню, позволяющего управлять связями и принудительным наследованием.

Включить или выключить связь можно включением/выключением команды Связь включена (Link Enabled). Включить/выключить принудительный режим наследования можно включением/выключением команды Принудительный (Enforced).

Обслуживание, поиск и устранение неисправностей групповой политики

Групповая политика — широкая область администрирования, требующая внимательного управления. Как любая другая область администрирования, групповая политика предполагает осторожное обслуживание, чтобы можно

было гарантировать ее надлежащее функционирование. Администратор должен диагностировать и решать любые возникающие проблемы. Чтобы диагностировать групповую политику, необходимо четко понимать, как политика обновляется и обрабатывается. Также нужно четко понимать задачи общего техобслуживания и поиска/устранения неисправностей.

Обновление групповой политики

При внесении изменения в политику эти изменения применяются немедленно. Однако они не распространяются автоматически. Клиентские компьютеры запрашивают политики в следующих случаях:

- при запуске компьютера;
- при входе пользователя;
- когда приложение или пользователь запрашивает обновления;
- когда истекает интервал обновления групповой политики, установленный для нее.

Настройки конфигурации компьютера применяются во время запуска операционной системы. Настройки конфигурации пользователя — при входе пользователя в систему. Если произошел конфликт между настройками пользователя и компьютера, у конфигурации компьютера более высокий приоритет, и именно ее настройки будут применены.

Как только настройки политики будут применены, настройки будут обновлены автоматически, чтобы можно было гарантировать, что они являются текущими. По умолчанию интервал обновления для контроллеров домена — 5 минут. Для других компьютеров интервал обновления — 90 минут с 30-минутными вариациями, чтобы избежать перегрузки контроллера домена многочисленными параллельными запросами клиентов. Это означает, что актуальный временной промежуток обновления для компьютеров, не являющихся контроллерами домена, составляет 90—120 минут.

Во время обновления групповой политики клиентский компьютер обращается к доступному контроллеру домена в его локальном сайте. Если есть изменения в одном или более объекте политики в домене, контроллер домена предоставляет список объектов политики, которые применяются к компьютеру и к пользователям, которые в данный момент вошли в систему.

Контроллер домена делает это независимо от того, изменились ли номера версий на всех перечисленных объектах политики. По умолчанию компьютер обрабатывает объекты политики, только если изменился номер версии по крайней мере одного из объектов политики. Если какая-то из связанных политик изменилась, все политики должны быть обработаны снова из-за наследования и взаимозависимостей между политиками.

Настройки безопасности — известное исключение к правилу обработки. По умолчанию эти настройки обновляются каждые 16 часов (960 минут) независимо от того, содержат ли объекты политики изменения. Чтобы уменьшить влияние на контроллеры домена и сеть, во время обновлений добавляется случайное смещение до 30 минут (эффективное окно обновления 960—990 минут). Кроме того, если клиентский компьютер обнаруживает, что

подключается по медленному сетевому соединению, он сообщает об этом контроллеру домена, и по сети передаются только настройки безопасности и административные шаблоны. Это означает, когда компьютер работает по медленному соединению, будут применены лишь настройки безопасности и административные шаблоны. Можно настроить способ обнаружения медленного соединения.

Необходимо тщательно сбалансировать частоту обновления политики с учетом частоты ее изменения. Если политика изменяется редко, можно увеличить окно обновления, чтобы уменьшить использование ресурсов. Например, можно установить интервал обновления 20 минут на контроллерах домена и 180 минут на других компьютерах.

Настройка интервала обновления

Интервал обновления групповой политики для каждого объекта политики можно настроить индивидуально. Для установки интервала обновления для контроллеров домена выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте групповой политики, который нужно изменить, и выберите команду Изменить. Этот GPO должен быть связан с контейнером, который содержит объекты компьютеров контроллера домена.
2. В узле Конфигурация компьютера\Административные шаблоны\Система\Групповая политика дважды щелкните на политике Установить интервал обновления групповой политики для контроллеров домена (Set Group Policy Refresh Interval For Domain Controllers). В результате будет отображено окно Свойства .
3. Включите политику, выбрав переключатель Включено (Enabled). Установите базовый интервал обновлений в первом поле Мин (Minutes). Обычно интервал обновления устанавливают от 5 до 59 минут.
4. Во втором поле Мин (Minutes) установите случайную величину времени, которая будет добавлена к интервалу обновления. Эта случайная величина создает окно обновления, что препятствует перегрузке сервера при многочисленных параллельных запросах групповой политики клиентами. Нажмите кнопку OK.

Чем чаще обновляется политика, тем актуальнее конфигурация политики у компьютера. Чем реже обновляется политика, тем меньше используется системных ресурсов контроллера домена и сети, но в то же время у компьютера не будет самой актуальной конфигурации политики.

Для установки интервала обновления для рабочих станций выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте групповой политики, который нужно изменить, и выберите команду Изменить. Этот GPO должен быть связан с контейнером, который содержит объекты компьютеров контроллера домена.
2. В узле Конфигурация компьютера\Административные шаблоны\Система\Групповая политика дважды щелкните на политике

Установить интервал обновления групповой политики для компьютеров (Set Group Policy Refresh Interval For Computers). В результате будет отображено окно Свойства.

3. Включите политику, отметив переключатель Включено (Enabled). Установите базовый интервал обновлений в первом поле Мин (Minutes). Обычно интервал обновления устанавливают от 60 до 240 минут.
4. Во втором поле Мин (Minutes) установите случайную величину времени, которая будет добавлена к интервалу обновления. Эта случайная величина создает окно обновления, что препятствует перегрузке сервера при многочисленных параллельных запросах групповой политики клиентами. Нажмите кнопку OK.

Убедитесь, что обновления не происходят слишком часто и в то же время достаточно своевременны, чтобы оправдать ожидания и соответствовать требованиям. Чем чаще обновляется политика, тем больше сетевого трафика генерируется. В большой сети обычно нужно установить больший интервал обновления, чтобы уменьшить сетевой трафик, особенно когда политика затрагивает сотни пользователей или компьютеров. Если пользователи жалуются на периодическое снижение производительности своих компьютеров, также нужно увеличить интервал обновления. Рассмотрите обновления раз в день или даже раз в неделю, чтобы сохранить политики достаточно актуальными и в то же время соответствующими потребностям организации. администратору, возможно, понадобится обновить групповую политику вручную.

Например, если нет желания ждать, пока автоматически произойдет обновление или нужно решить проблему с обновлением. Вызвать обновление групповой политики вручную можно командой gpupdate.

Инициировать обновление можно несколькими способами. Можно ввести команду gpupdate в командной строке или в поле поиска приложений, в результате будут обновлены и конфигурация компьютера, и конфигурация пользователя на локальном компьютере. Будут обработаны и применены только измененные настройки политики. Для обновления всех настроек политики нужно использовать параметр /Force .

Также можно обновлять конфигурации пользователя и компьютера раздельно. Для обновления только конфигурации компьютера введите gpupdate /target:computer в командной строке. Для обновления только конфигурации пользователя предназначена другая команда — gpupdate /target:user .

Также можно использовать команду gpupdate для выхода пользователя или перезапуска компьютера после обновления групповой политики. Это полезно, поскольку некоторые политики могут быть применены лишь тогда, когда пользователь входит в систему или только при запуске компьютера. Для выхода пользователя после обновления добавьте параметр / Logoff , а для перезапуска компьютера после обновления — параметр /Boot .

Моделирование групповой политики для планирования

Моделирование групповой политики для планирования полезно, когда нужно протестировать различные реализации и сценарии конфигурации. Например, можно смоделировать эффект петлевой обработки или обнаружения медленного соединения. Также можно смоделировать эффект перемещения пользователей или компьютеров в другой контейнер в Active Directory или эффект изменения состава группы безопасности для пользователей и компьютеров.

У всех администраторов домена и предприятия есть разрешение моделировать групповую политику для планирования, также доступ к планированию есть у всех, кто обладает разрешением Анализ моделирования групповой политики (Perform Group Policy Modeling.

Analyses). Для моделирования групповой политики и тестирования различных сценариев реализации и обновления выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши по узлу Моделирование групповой политики (Group Policy Modeling), выберите команду Мастер моделирования групповой политики (Group Policy Modeling Wizard), а затем нажмите кнопку Далее.
2. На странице Выбор контроллера домена (Domain Controller Selection) из списка Контроллеры домена в этом домене (Show Domain Controllers) выберите контроллер домена, который нужно моделировать. По умолчанию политика моделируется на любом доступном контроллере домена в выбранном домене. Если необходимо использовать определенный контроллер домена, установите переключатель Указанный контроллер домена (This Domain Controller). Затем выберите нужный контроллер домена и нажмите кнопку Далее.
3. На странице Выбор компьютера и пользователя (User And Computer Selection) можно выбрать контейнеры или отдельные учетные записи. Используйте один из двух методов выбора учетных записей и затем нажмите кнопку Далее.
   - Используйте контейнеры для имитации изменений для всего организационного подразделения или других контейнеров. В группе Сведения о пользователе (User Information) установите переключатель Контейнер (Container) и нажмите кнопку Обзор. Появится окно Выбор контейнера пользователя (Choose User Container). Используйте его для выбора любых доступных контейнеров пользователей в выбранном домене. В группе Сведения о компьютере (Computer Information) установите переключатель Контейнер (Container) и нажмите кнопку Обзор. В появившемся диалоговом окне Выбор контейнера компьютера (Choose Computer Container) выберите любой доступный контейнер компьютера в текущем домене.
   - Выберите определенные учетные записи для имитации изменений для отдельного пользователя и компьютера. В группе Сведения о пользователе установите переключатель Пользователь (User), затем

нажмите кнопку Обзор и в окне Выбор: "Пользователь" (Select User) выберите учетную запись пользователя. В группе Сведения о компьютере установите переключатель Компьютер (Computer), нажмите кнопку Обзор и в окне Выбор: "Компьютер" (Select Computer) выберите учетную запись компьютера.

4. На странице Дополнительные параметры эмуляции (Advanced Simulation Options) выберите любые дополнительные параметры, например Медленное сетевое подключение (Slow Network Connections) или Обработка петлевого адреса (Loopback Processing), Сайт (Site), если это необходимо, и нажмите кнопку Далее.
5. На странице Группы безопасности пользователя (User Security Groups) можно эмулировать изменения в составе группы безопасности для одного или нескольких пользователей. Любые изменения, вносимые в состав группы, влияют на ранее выбранного пользователя или контейнер пользователя. Например, если нужно увидеть, что произойдет, если пользователь в контейнере пользователей — член группы CorpManagers, добавьте эту группу в список Группы безопасности (Security Groups) и нажмите кнопку Далее.
6. На странице Группы безопасности компьютера (Computer Security Groups) можно эмулировать изменения в составе группы безопасности для компьютера или компьютеров. Любые изменения, вносимые в состав группы, влияют на ранее выбранный компьютер или контейнер компьютеров. Например, если нужно увидеть, что произойдет, если компьютер в выбранном контейнере — член группы RemoteComputers, добавьте эту группу в список Группы безопасности и нажмите кнопку Далее.
7. Можно связать Фильтры WMI (Windows Management Instrumentation) с объектами групповой политики. По умолчанию предполагается, что выбранные пользователи и компьютеры соответствуют всем требованиям WMI-фильтра, который в большинстве случаев подходит для планирования. Нажмите кнопку Далее дважды, чтобы принять параметры по умолчанию.
8. Просмотрите указанные параметры и нажмите кнопку Далее. После того как мастер соберет необходимую информацию политики, нажмите кнопку Готово. Когда мастер закончит генерирование отчета, созданный отчет будет выбран в левой области окна, а его результаты — в правой области.
9. На вкладке Сведения (Details) (рис. 4.9), просматривая отчет, можно определить настройки, которые будут применены. Информация политики компьютера выводится в области Сведения о компьютере (Computer Details). Информация политики пользователя — в области Сведения о пользователе (User Details).

Копирование, вставка и импорт объектов политики

Консоль GPMC поддерживает встроенные операции копирования, вставки и импорта. Использование функций копирования и вставки довольно простое. Команды Копировать (Copy) и Вставить (Paste) доступны в контекстном меню объекта групповой политики. Можно скопировать GPO и все его настройки в одном домене, затем переместиться в другой домен и вставить копию объекта политики. Исходный и целевой домены могут быть любыми доменами, с которыми можно соединиться в GPMC и для которых существует разрешение управлять связанными объектами политики. В исходном домене требуется разрешение чтения (для создания копии объекта). В целевом домене — разрешение записи, чтобы вставить скопированный объект политики. Такое разрешение есть у администраторов, а также у тех, кто был специально делегирован создавать объекты политики.

Копирование объектов политики между доменами работает хорошо, если есть связь между доменами и надлежащие полномочия. Даже если администратор находится в удаленном офисе или имеет делегированные разрешения, он может не иметь доступа к исходному домену для создания копии объекта политики. В этом случае другой администратор может сделать резервную копию объекта политики и затем отправить ее администратору в удаленный офис. Когда первый администратор получит эту резервную копию, он может импортировать объект политики в домен для создания объекта политики с такими же настройками.

Любой пользователь с полномочиями Изменение параметров (Edit Settings) может осуществить операцию импорта. Операция импорта перезаписывает все настройки выбранного объекта политики. Для импортирования резервной копии объекта политики в домен выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши по узлу Объекты групповой политики, затем выберите команду Создать. В окне Новый объект групповой политики введите описательное имя нового GPO и нажмите кнопку OK.
2. Теперь в контейнере Объекты групповой политики появится новый GPO. Щелкните правой кнопкой мыши на созданном объекте и выберите команду Импорт параметров (Import Settings). Запустится мастер импорта параметров (Import Settings Wizard).
3. Нажмите кнопку Далее дважды, чтобы пропустить страницу Архивирование объекта групповой политики (Backup GPO). Не нужно архивировать текущий GPO, поскольку он новый и в нем ничего нет.
4. На странице Расположение архива (Backup Location) нажмите кнопку Обзор. В окне Обзор папок (Browse For Folder) выберите папку, содержащую резервную копию объекта политики, который нужно импортировать, затем нажмите кнопку OK. Нажмите кнопку Далее, чтобы продолжить.
5. Если в выбранной папке хранится несколько резервных копий, будет отображен их список на странице Исходный объект групповой политики

(Source GPO). Выберите объект, который нужно использовать, и нажмите кнопку Далее.

6. Мастер импорта настроек просканирует объект политики в поисках ссылок на субъекты безопасности и путей UNC, которые должны быть перемещены. Если такие пути или субъекты будут найдены, будет предоставлена возможность составить или использовать существующие таблицы миграции.
7. Продолжите работу мастера, нажав кнопку Далее, а затем — кнопку Готово для начала процесса импорта. Когда импорт будет завершен, нажмите кнопку OK.

Резервное копирование и восстановление объектов политики

Для защиты GPO нужно сделать их резервные копии. Для создания резервных копий отдельных объектов политик домена или всех политик объекта в домене можно использовать консоль GPMC:

1. В консоли GPMC разверните и затем выберите узел Объекты групповой политики. Если нужно сделать резервную копию всех объектов политики в домене, щелкните правой кнопкой мыши на узле Объекты групповой политики и выберите команду Архивировать все (Back Up All). Если нужно сделать резервную копию определенного объекта в домене, щелкните на нем правой кнопкой мыши и выберите команду Архивировать (Back Up).
2. В окне Архивация объекта групповой политики (Back Up Group Policy Object) нажмите кнопку Обзор. В окне Обзор папок выберите папку, в которой будет сохранен объект GPO.
3. В поле Описание (Description) введите описание содержимого резервной копии. Нажмите кнопку Архивировать (Back Up) для начала резервного копирования.
4. Состояние процесса резервного копирования и индикатор хода архивирования отображается в окне Архивирование (Backup). Нажмите кнопку OK после создания резервной копии. Для создания резервной копии нужны разрешения чтения и записи. По умолчанию такие разрешения есть у групп Администраторы домена (Domain Admins) и Администраторы предприятия (Enterprise Admin).

Используя консоль GPMC, можно восстановить объект политики в состояние, в котором он был архивирован. Консоль GPMC отслеживает резервные копии каждого объекта политики отдельно, даже если архивируются сразу все объекты политик. Поскольку информация о версии тоже отслеживается по штампу времени резервной копии и описанию, можно восстановить последнюю версию каждого объекта политики или определенную версию любого объекта политики.

Для восстановления объекта политики выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на узле Объекты групповой политики и выберите команду Управление архивацией (Manage Backups). Появится одноименное диалоговое окно.

2. В поле Расположение архива (Backup Location) нажмите кнопку Обзор. В окне Обзор папок найдите папку, в которой находится резервная копия, и нажмите кнопку OK.
3. Все резервные копии объекта политики в выбранной папке перечислены в узле Архивированные объекты групповой политики (Backed Up GPOs). Чтобы увидеть только последнюю версию объектов политики по метке времени, включите параметр Показывать только последнюю версию каждого объекта групповой политики (Show Only The Latest Version Of Each GPO).
4. Выберите GPO, который нужно восстановить. Если необходимо подтвердить его параметры, нажмите кнопку Просмотреть параметры (View Settings). После этого в окне Internet Explorer можно проверить параметры объекта политики. Когда будете готовы продолжить, нажмите кнопку Восстановить (Restore). Подтвердите свое намерение, нажав кнопку OK.
5. Диалоговое окно Восстановление (Restore) покажет состояние процесса восстановления и индикатор хода восстановления. Если операция восстановления завершилась неудачно, проверьте разрешения на объекте политики и папке, из которой осуществляется чтение резервной копии. Для восстановления GPO у пользователя должно быть разрешение Изменение параметров, удаление и изменение параметров безопасности (Edit Settings, Delete, and Modify Security) на объекте политики и разрешение на чтение из папки с архивом. По умолчанию такие разрешения имеют пользователи из групп Администраторы домена и Администраторы предприятия.

Определение текущих настроек групповой политики и статуса определения

Для анализа RSoP (Resultant Set of Policy) можно использовать моделирование групповой политики. Если моделирование групповой политики используется именно так, можно просмотреть все объекты политики, которые применяются к компьютеру, и время последней обработки (обновления) объектов политики. Доступ к моделированию групповой политики для анализа имеют все администраторы домена и предприятия, а также все пользователи, у которых есть разрешение Чтение результирующих данных групповой политики (Read Group Policy Results Data). В консоли GPMC можно моделировать групповую политику для анализа, щелкнув правой кнопкой мыши на узле Результаты групповой политики (Group Policy Results) и выбрав команду Мастер результатов групповой политики (Group Policy Results Wizard). Когда откроется окно мастера, следуйте его инструкциям.

Отключение неиспользуемой части групповой политики

Другой способ отключения политики — отключить неиспользуемую часть GPO. В результате будут заблокированы настройки конфигурации компьютера и конфигурации пользователя (или обе), и им будет запрещено применяться.

При отключении неиспользуемой части политики применение GPO будет осуществляться быстрее.
Включить и отключить политики можно с помощью следующих действий:

1. В консоли GPMC выберите контейнер сайта, домена или организационного подразделения, с которыми нужно работать.
2. Выберите объект политики, с которым нужно работать, и затем перейдите на вкладку Сведения (Details) на правой панели.
3. Выберите одно из значений из списка Состояние GPO (GPO Status) и нажмите кнопку OK, когда консоль попросит подтвердить изменение состояния GPO:
   - Все параметры отключены (All Settings Disabled) — отключает обработку объекта политики и всех его параметров;
   - Параметры конфигурации компьютера отключены (Computer Configuration Settings Disabled) — отключает параметры конфигурации компьютера. Это означает, что будут обработаны только параметры конфигурации пользователя;
   - Параметры конфигурации пользователя отключены (User Configuration Settings Disabled) — отключает параметры конфигурации пользователя. Это означает, что будут обработаны только параметры конфигурации компьютера;
   - Включено (Enabled) — разрешает обработку объекта политики и всех его параметров.

Изменение свойств обработки политики

В групповой политике параметры конфигурации компьютера обрабатываются при запуске компьютера и получении доступа к сети. Параметры конфигурации пользователя обрабатываются, когда пользователь входит в сеть. В случае конфликта между настройками в конфигурации компьютера и конфигурации пользователя будут применены параметры конфигурации компьютера. Также важно помнить, что параметры компьютера применяются из GPO компьютера, а параметры пользователя — из GPO пользователя. В некоторых особых ситуациях данное поведение — не то, что нужно. Возможно, будет необходимо, чтобы на общем компьютере параметры пользователя применялись из GPO компьютера, и в то же время нужно разрешить применение настроек пользователя из GPO пользователя. В безопасной лаборатории нужно применять пользовательские настройки из GPO компьютера, чтобы настройки соответствовали строгим правилам безопасности или инструкциям лаборатории. Эти типы исключений можно получить с помощью замыкания групповой политики.
Для изменения режима обработки замыкания групповой политики выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте GPO, который необходимо модифицировать, и выберите команду Изменить.
2. В узле Конфигурация компьютера\Политики\Административные шаблоны\Система\ Групповая политика (Computer Configuration\Policies\

Administrative Templates\System\ Group Policy) выберите политику Настройка режима обработки замыкания пользовательской групповой политики (Configure User Group Policy Loopback Processing Mode). Будет отображено окно свойств этой политики.

3. Включите политику, выбрав переключатель Включено (Enabled). Выберите один из режимов обработки из списка Режим (Mode) и затем нажмите кнопку OK.
   - Замена (Replace) — параметры политики пользователя, определенные в GPO компьютера, заменят параметры политики пользователя, обычно применяемые для этого пользователя. Это означает, что пользовательские настройки из GPO компьютера заменят настройки пользователя, которые обычно к нему применялись.
   - Слияние (Merge) — выберите этот режим, чтобы убедиться, что сначала будут обработаны пользовательские настройки в GPO компьютера, а далее пользовательские настройки из GPO пользователя, а затем снова — пользовательские настройки в GPO компьютера. Эта техника обработки применяется для комбинации пользовательских настроек в GPO компьютера и GPO пользователя. В случае конфликта приоритет будет у пользовательских настроек в GPO компьютера: они перезапишут пользовательские настройки в GPO пользователя.

Настройка обнаружения медленного соединения

Обнаружение медленного соединения используется клиентами групповой политики для определения увеличения задержки и уменьшения скорости отклика в сети и принятия мер по ликвидации последствий, чтобы уменьшить вероятность прекращения применения групповой политики в сети. Как только обнаружено медленное соединение, клиенты групповой политики снижают свои запросы, чтобы уменьшить нагрузку на сеть, ограничивая количество обрабатываемых политик.

По умолчанию, если скорость соединения меньше 500 Кбит/с (это значение может быть интерпретировано как высокий уровень задержки/снижения скорости отклика в быстрой сети), клиентские компьютеры воспринимают это соединение как медленное и уведомляют об этом контроллер домена. В результате при обновлении политики будут применены только параметры безопасности и административные шаблоны.

За определение медленного соединения отвечает политика Настройка определения медленных подключений (Configure Group Policy Slow Link Detection), которая находится в узле Конфигурация компьютера\Политики\Административные шаблоны\Система\ Групповая политика (Computer Configuration\Policies\Administrative Templates\System\ Group Policy). Если отключить эту политику или не настраивать ее, клиенты будут использовать значение по умолчанию — 500 Кбит/с для определения, медленное ли соединение.

Если включить эту политику, можно установить скорость, при которой соединение будет считаться медленным, например, 384 Кбит/с. Также помните, что 3G-соединения практически всегда будут считаться медленными. С другой стороны, если нужно полностью отключить обнаружение медленного соединения, установите параметр Скорость подключения (Connection Speed) в 0. Для клиента это будет сигналом, что больше не нужно определять медленные соединения, и все соединения будут рассмотрены как быстрые.

Microsoft называет сотовые и широкополосные соединения платными сетями. Разработано несколько политик, чтобы помочь указать, как должна использоваться сеть на мобильных устройствах, работающих через платные сети. Администратор может:

- контролировать синхронизацию автономных файлов на платных сетях с помощью политики Включить синхронизацию файлов в платных сетях (Enable File Synchronization On Costed Networks), которая находится в узле Конфигурация компьютера\ Политики\Административные шаблоны\Сеть\Автономные файлы (Computer Configuration\Policies\Administrative Templates\Network\Offline Files);
- контролировать фоновую передачу по платным сетям с помощью политики Установить логику загрузки по умолчанию для заданий BITS в тарифицируемых сетях (Set Default Download Behavior For BITS Jobs On Costed Networks), которая находится в узле Конфигурация компьютера\Политики\Административные шаблоны\Сеть\Фоновая интеллектуальная служба передачи (BITS) (Computer Configuration\Policies\ Administrative Templates\Network\Background Intelligent Transfer Services (BITS));
- указать стоимость платного соединения. Платные сети могут иметь фиксированную, переменную или неограниченную плату за соединение. Установить тип оплаты можно в узле Конфигурация компьютера\Политики\Административные шаблоны\Сеть\ Служба WLAN\Стоимость использования WLAN (Computer Configuration\Policies\ Administrative Templates\Network\WLAN Service\WLAN Media Cost) с помощью политики Задать стоимость (Set Cost policy);
- указать стоимость 3G/4G-соединения. Стоимость 3G- и 4G-доступа может отличаться и тоже может быть фиксированной, переменной и неограниченной. Задать тип стоимости можно с помощью политик Задать стоимость 3G (Set 3G Cost) и Задать стоимость 4G (Set 4G Cost) в узле Конфигурация компьютера\Политики\ Административные шаблоны\Сеть\ Служба WWAN\ Стоимость использования WWAN (Computer Configuration\Policies\Administrative Templates\Network\WWAN Service\WWAN Media Cost).

В случае необходимости можно оптимизировать механизм обнаружения медленного соединения для различных областей обработки групповой

политики. По умолчанию следующие области групповой политики не обрабатываются, когда обнаружено медленное соединение:

- обработка политик дисковых квот;
- обработка политик восстановления EFS;
- обработка политик перенаправления папок;
- обработка политик установки программного обеспечения.

Обработка политик безопасности всегда включена для медленных соединений. По умолчанию политика обновляется каждые 16 часов, даже если политика безопасности не изменялась. Единственный способ остановить принудительное обновление — настроить обработку политики безопасности так, чтобы она не применялась во время периодических фоновых обновлений. Чтобы сделать это, установите опцию Не применять во время периодической фоновой обработки (Do Not Apply During Periodic Background Processing) (см. далее).

Однако поскольку политики безопасности очень важна, отключение применения означает, что обработка политика безопасности будет остановлена, когда пользователь зарегистрирован и использует компьютер. Единственная причина, по которой нужно остановить обновление политики безопасности — если приложения перестали работать во время операций обновления.

Обнаружение медленного соединения и обработку соответствующих политик можно настроить так:

1. В консоли GPMC щелкните правой кнопкой мыши по объекту политики, который необходимо модифицировать, и выберите команду Изменить.
2. Дважды щелкните на политике Настроить определения медленных подключений для групповой политики (Configure Group Policy Slow Link Detection) в узле Конфигурация компьютера\Политики\Административные шаблоны\Система\Групповая политика (Computer Configuration\ Policies\Administrative Templates\System\Group Policy).
3. Установите переключатель Включено (Enabled), как показано на рис. 4.10. В поле Скорость подключения (Connection Speed) задайте скорость, которая будет считаться медленной. Также можно указать, будут ли считаться 3G-соединения медленными. Нажмите кнопку OK.

Для настройки медленного соединения и фоновой обработки ключевых областей групповой политики выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на объекте политики, который нужно модифицировать, и выберите команду Изменить.
2. Разверните узел Конфигурация компьютера\ Административные шаблоны\Система\ Групповая политика.
3. Дважды щелкните на политике обработки, которую необходимо настроить. Установите переключатель Включено для определения политики и сделайте соответствующую настройку. Опции могут немного отличаться, в зависимости от выбранной политики:

- Разрешить обработку через медленное сетевое подключение (Allow Processing Across A Slow Network Connection) — гарантирует, что политика будет обработана даже в медленной сети;
- Не применять во время периодической фоновой обработки (Do Not Apply During Periodic Background Processing) — переопределяет настройки обновления, когда связанные политики изменяются после запуска или входа в систему;
- Обрабатывать, даже если объекты групповой политики не изменились (Process Even If The Group Policy Objects Have Not Changed) — политика будет применена, даже если ее настройка не изменилась.

4. Нажмите кнопку OK для сохранения изменений.

Удаление ссылок и удаление GPO

В консоли GPMC можно остановить использование связанных объектов групповой политики двумя способами:

- удалить ссылку на GPO, но не удалять сам GPO;
- удалить GPO и все ссылки на него.

Удаление ссылки на GPO предотвращает использование соответствующих настроек политик в сайте, домене или организационном подразделении, но не удаляет сам GPO. Однако GPO остается соединенным с другими сайтами, доменами или организационными подразделениями. В GPMC можно удалить ссылку на GPO, щелкнув правой кнопкой мыши по ссылке на GPO в контейнере и выбрав команду Удалить (Delete). Когда консоль попросит подтвердить намерение, нажмите кнопку OK. Если удалить все ссылки на GPO с сайтов, доменов и организационных подразделений, GPO продолжит существование в контейнере Объекты групповой политики, но его настройки не будут иметь никакого эффекта в организации.

Удаление GPO означает удаление GPO и всех ссылок на него. GPO больше не будет существовать в контейнере Объекты групповой политики и не будет связан ни с одним сайтом, доменом или организационным подразделением. Есть только один способ восстановить удаленный GPO — это восстановить его из ранее созданной резервной копии (если она доступна). Удалить GPO и все ссылки на этот объект можно в консоли GPMC из узла Объекты групповой политики. Щелкните правой кнопкой мыши на GPO и выберите команду Удалить. Для подтверждения своего намерения нажмите кнопку Да.

Поиск и устранение неисправностей групповой политики

При попытке определить, почему политика не применяется, как ожидалось, первым делом нужно исследовать результаты групповой политики для пользователя и компьютера, чтобы понять суть проблемы. Определить, что политики GPO применены, можно так:

1. В консоли GPMC щелкните правой кнопкой мыши по узлу Результаты групповой политики (Group Policy Results) и выберите команду Мастер

результатов групповой политики (Group Policy Results Wizard). Когда мастер запустится, нажмите кнопку Далее.

2. На странице Выбор компьютера (Computer Selection) установите переключатель Этот компьютер (This Computer), чтобы просмотреть информацию для локального компьютера. Чтобы просмотреть информацию для удаленного компьютера, отметьте переключатель Другой компьютер (Another Computer) и затем нажмите кнопку Обзор. В окне Выбор: "Компьютер" (Select Computer) введите имя компьютера и нажмите кнопку Проверить имена (Check Names). После того как выберете правильное имя компьютера, нажмите кнопку Далее.
3. На странице Выбор пользователя (User Selection) выберите пользователя, чью информацию о политике нужно просмотреть. Можно просмотреть информацию о политике для любого пользователя, который ранее был зарегистрирован на компьютере. Нажмите кнопку Далее.
4. Просмотрите установленные параметры и нажмите кнопку Далее. После того как мастер получит необходимую информацию, нажмите кнопку Готово. По окончанию создания отчета он будет выбран в левой панели, а результаты будут отображены в правой панели.
5. Чтобы определить, какие параметры были применены, просмотрите отчет. Информация политики для компьютера и пользователя выводится отдельно: для компьютера — в разделе Сводка о компьютере (Computer Configuration Summary), для пользователя — в разделе Сводка о пользователе (User Configuration Summary).

Используя утилиту командной строки Gpresult, можно просмотреть RSoP. Эта утилита предоставляет следующие сводки:

- специальные параметры, примененные для перенаправления папок, установки программы, дисковых квот, IPsec и сценариев;
- время последнего применения групповой политики;
- контроллер домена, от которого была получена политика и членство группы безопасности для компьютера и пользователя;
- полный список всех примененных GPO, а также список GPO, которые не были использованы из-за фильтров.

Базовый синтаксис утилиты Gpresult следующий:

gpresult /s ComputerName /user Domain\UserName

Здесь ComputerName — имя компьютера, для которого нужно просмотреть результаты политики; Domain\UserName — имя пользователя. Например, для просмотра RSoP для компьютера CorpPC85 и пользователя Tedg в домене Cpandl нужно ввести команду:

gpresult /s corppc85 /user cpandl\tedg

Дополнительную информацию можно получить, добавив две следующие опции. Параметр /v включает подробный вывод и отображает результаты только для актуальных настроек политик. Параметр /z также включает подробный вывод и отображает результаты только для актуальных политики и всех других GPO, где установлены политики. Поскольку вывод Gpresult очень

длинный, нужно создать HTML-отчет, добавив параметр /h или XML-отчет, добавив параметр /x .
Примеры:
gpresult /s corppc85 /user cpandl\tedg /h gpreport.html
gpresult /s corppc85 /user cpandl\tedg /x gpreport.xml

Исправление объектов групповой политики по умолчанию

Объекты групповой политики Default Domain Policy и Default Domain Controller Policy жизненно важны для доменных служб Active Directory (AD DS). Если по некоторым причинам эти политики будут повреждены, то групповая политика перестанет функционировать должным образом. Для решения проблемы нужно восстановить эти объекты из резервной копии. Если резервные копии объектов Default Domain Policy и Default Domain Controller Policy отсутствуют, можно использовать утилиту Dcgpofix, чтобы восстановить настройки безопасности в этих политиках.
Состояние, к которому Dcgpofix восстанавливает эти объекты, зависит от того, как изменили безопасность, и от состояния безопасности контроллера домена перед запуском Dcgpofix. Для запуска утилиты нужно быть членом групп Администраторы домена или Администраторы предприятия.
При запуске Dcgpofix объекты групповых политик Default Domain Policy и Default Domain Controller Policy будут восстановлены со значениями по умолчанию, и любые изменения, внесенные в эти GPO, будут потеряны. Некоторые настройки политики сохраняются отдельно и не будут потеряны, в том числе Windows Deployment Services (WDS), параметры безопасности и Encrypting File System (EFS). Настройки безопасности, не являющиеся настройками по умолчанию, не обслуживаются, а это означает, что они могут быть потеряны.
Все другие настройки политики будут восстановлены в их предыдущие значения, и любые сделанные вами изменения будут потеряны.
Для запуска Dcgpofix войдите в контроллер домена, где нужно починить групповую политику по умолчанию, а затем введите команду dcgpofix в командной строке. Утилита проверит версию схемы Active Directory, чтобы гарантировать совместимость версий Dcgpofix и конфигурации схемы Active Directory. Если версии не совместимы, Dcgpofix завершит работу без исправления GPO по умолчанию. При указании параметра /Ignoreschema Dcgpofix будет принудительно работать с другой версией Active Directory. Однако GPO по умолчанию могут быть не восстановлены в их исходное состояние. Поэтому убедитесь, что используете версию Dcgpofix, которая устанавливалась с текущей операционной системой.
Можно исправить только GPO Default Domain Policy или GPO Default Domain Controller Policy. Если нужно исправить объект Default Domain Policy, введите команду dcgpofix /target:domain . Если нужно исправить объект Default Domain Controller Policy, введите команду dcgpofix /target:dc .

Управление пользователями и компьютерами с помощью групповой политики

Групповая политика используется для управления пользователями и компьютерами. В этом разделе мы рассмотрим некоторые специфические области управления, в том числе:

- перенаправление папок;
- сценарии компьютера и пользователя;
- развертывание программного обеспечения;
- регистрацию сертификатов компьютера и пользователя;
- параметры автоматического обновления.

Централизованное управление специальными папками

Посредством перенаправления папок можно управлять специальными папками, которые используются Windows Server. Это можно сделать с помощью перенаправления специальных папок в центральное сетевое хранилище вместо использования множества хранилищ по умолчанию — на каждом компьютере. Список папок, которыми можно управлять централизованно для Windows XP Professional и более ранних выпусков Windows: Application Data, Главное меню, Рабочий стол, Мои документы и Мои изображения. Для Windows Vista и более поздних версий: AppData (Roaming), Рабочий стол, Главное меню, Документы, Изображения, Музыка, Видео, Избранное, Контакты, Загрузки, Ссылки, Поиски и Сохраненные игры.

Обратите внимание: хотя перечень специальных папок в Windows Vista и более поздних версиях ОС немного отличается, управлять ними можно точно так же.

Имеются две основные опции перенаправления. Можно перенаправить специальную папку в одно общее для всех пользователей сетевое хранилище (расположение) или определить хранилище на основании членства пользователя в группах безопасности. В любом случае нужно убедиться, что сетевое расположение, которое планируется использовать, доступно как сетевой ресурс (см. главу 12).

По умолчанию пользователи могут перенаправить папки независимо от того, какой компьютер они используют в домене. Windows 8 и Windows Server 2012 позволяют изменять это поведение, определяя, с каких компьютеров пользователь может получить доступ к профилям роуминга и перенаправленным папкам. Это можно сделать с помощью определения основных компьютеров и задания политики домена, которая бы ограничивала загрузку профилей, перенаправленных папок (или и профилей, и перенаправленных папок) на основные компьютеры.

Перенаправление специальных папок в единое расположение

Перенаправить специальную папку в общее расположение можно с помощью этих действий:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO сайта, домена или организационного подразделения, с которыми нужно работать, и выберите команду Изменить. Откроется редактор политики для GPO.
2. В редакторе политики разверните следующие узлы: Конфигурация пользователя\ Политика\Конфигурация Windows\Перенаправление папки (User Configuration\ Windows Settings\Folder Redirection).
3. В узле Перенаправление папки (Folder Redirection) щелкните правой кнопкой мыши по названию папки, параметры которой нужно изменить. Например, пусть это будет AppData (перемещаемая) (AppData(Roaming)). В появившемся меню выберите команду Свойства. Откроется одноименное диалоговое окно.
4. В списке Политика (Setting) на вкладке Конечная папка (Target) установите значение Перенаправлять папки всех пользователей в одно расположение (Basic-Redirect Everyone's Folder To The Same Location).
5. В группе Расположение целевой папки (Target Folder Location) есть несколько опций, определяющих, с какой папкой происходит работа.
   - Перенаправлять в домашний каталог пользователя (Redirect To The User's Home Directory) — если выбрать эту опцию, папка будет перенаправлена в подкаталог в пределах пользовательского домашнего каталога. Можно указать расположение пользовательского домашнего каталога с помощью переменных среды %HomeDrive% и %HomePath% .
   - Создать папку для каждого пользователя на корневом пути (Create A Folder For Each User Under The Root Path) — если выбрать эту опцию, для каждого пользователя в указанном расположении (поле Корневой путь (Root Path)) будет создан отдельный каталог. Имя папки пользователя — это имя пользователя, заданное переменной %UserName% . Если указан корневой путь \\Zeta\UserDocuments, то папка пользователя Williams будет размещена в \\Zeta\UserDocuments\Williams.
   - Перенаправлять в следующее расположение (Redirect To The Following Location) — при выборе этой опции папка будет перенаправлена в расположение, указанное в поле Корневой путь. Здесь обычно хочется использовать переменные среды, чтобы разграничить расположения для каждого пользователя. Например, можно установить такое расположение в качестве корневого пути: \\Zeta\ UserData\ %UserName% \docs.
   - Перенаправлять в расположение, определяемое локальным профилем (Redirect To The Local Userprofile Location) — при выборе этой опции папка будет перенаправлена в подкаталог в каталоге профилей пользователей. Можно выбрать расположение профиля пользователя с помощью переменной среды %UserProfile% .

6. Перейдите на вкладку Параметры (Settings) для настройки дополнительных параметров и нажмите кнопку OK для завершения процесса:
   - Предоставить права монопольного доступа к (Grant The User Exclusive Rights To) — предоставляет пользователям полные права доступа к своим данным в специальной папке;
   - Перенести содержимое <название папки> в новое расположение (Move The Contents Of FolderName To The New Location) — перемещает данные в специальные папки из отдельных систем сети в центральную папку или папки;
   - Применить политику перенаправления также к (Also Apply Redirection Policy To) — применяет политику перенаправления к предыдущим версиям Windows.

Перенаправление специальных папок на основании членства в группе

Можно перенаправить специальную папку на основании членства в группе, для этого выполните следующие действия:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO сайта, домена или организационного подразделения, с которыми нужно работать, и выберите команду Изменить. Откроется редактор политики для GPO.
2. В редакторе политики разверните следующие узлы: Конфигурация пользователя\Политика\Конфигурация Windows\Перенаправление папки (User Configuration\ Windows Settings\Folder Redirection).
3. В узле Перенаправление папки (Folder Redirection) щелкните правой кнопкой мыши по названию папки, параметры которой нужно изменить. Например, пусть это будет AppData (перемещаемая) (AppData(Roaming)). В появившемся меню выберите команду Свойства.
4. На вкладке Конечная папка в списке Политика выберите значение Указать различные расположения для разных групп пользователей (Advanced-Specify Locations For Various User Groups). Как показано на рис. 4.13, появится группа Членство в группе безопасности (Security Group Membership).
5. Нажмите кнопку Добавить, чтобы открыть окно Выбор группы и расположения (Specify Group And Location). Или выберите запись группы и нажмите кнопку Изменить для редактирования ее параметров.
6. В поле Членство в группе безопасности (Security Group Membership) введите имя группы безопасности, для которой нужно настроить перенаправление, или нажмите кнопку Обзор для поиска группы безопасности.
7. Как и в случае базового перенаправления, доступны опции, позволяющие определить папку.
   - Перенаправлять в домашний каталог пользователя (Redirect To The User’s Home Directory) — если выбрать эту опцию, папка будет перенаправлена в подкаталог в пределах пользовательского домашнего каталога. Можно указать расположение

пользовательского домашнего каталога с помощью переменных среды %HomeDrive% и %HomePath% .

- Создать папку для каждого пользователя на корневом пути (Create A Folder For Each User Under The Root Path) — если выбрать эту опцию, для каждого пользователя в указанном расположении (поле Корневой путь) будет создан отдельный каталог. Имя папки пользователя — это имя пользователя, заданное переменной %UserName% . Если указан корневой путь \\Zeta\UserDocuments, то папка пользователя Williams будет размещена в \\Zeta\UserDocuments\Williams.
- Перенаправлять в следующее расположение (Redirect To The Following Location) — при выборе этой опции папка будет перенаправлена в расположение, указанное в поле Корневой путь. Здесь обычно нужно использовать переменные среды, чтобы разграничить расположения для каждого пользователя. Например, можно установить такое расположение в качестве корневого пути: \\Zeta\UserData\ %UserName% \docs.
- Перенаправлять в расположение, определяемое локальным профилем (Redirect To The Local Userprofile Location) — при выборе этой опции папка будет перенаправлена в подкаталог в каталоге профилей пользователей. Можно выбрать расположение профиля пользователя с помощью переменной среды %UserProfile%

1. Нажмите кнопку OK. Повторите действия 5—7 для других групп, которые нужно настроить.
2. Когда закончите создание записей групп, перейдите на вкладку Параметры, чтобы настроить дополнительные параметры, и нажмите кнопку OK для завершения процесса:
   - Предоставить права монопольного доступа к — предоставляет пользователям полные права доступа к своим данным в специальной папке;
   - Перенести содержимое <название папки> в новое расположение — перемещает данные в специальные папки из отдельных систем сети в центральную папку или папки;
   - Применить политику перенаправления также к — применяет политику перенаправления к предыдущим версиям Windows.

Удаление перенаправления

Иногда нужно удалить перенаправление определенной папки. Сделать это можно следующим образом:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которыми нужно работать. Выберите команду Изменить, чтобы открыть редактор GPO.

2. В редакторе политики разверните следующие узлы: Конфигурация пользователя, Конфигурация Windows (Windows Settings) и Перенаправление папки (Folder Redirection).
3. В узле Перенаправление папки щелкните правой кнопкой мыши на специальной папке и выберите команду Свойства.
4. Перейдите на вкладку Параметры появившегося диалогового окна и убедитесь, что выбрана нужна опция в группе Удаление политики (Policy Removal). Доступны следующие опции.
   - После удаления политики оставить папку в новом расположении (Leave The Folder In The New Location When Policy Is Removed). При выборе этой опции папка и все ее содержимое останутся в переадресованном местоположении, а действующим пользователям будет разрешен доступ к папке и ее содержимому в этом местоположении.
   - После удаления политики перенаправить папку обратно в локальный профиль пользователя (Redirect The Folder Back To The Local Userprofile Location When Policy Is Removed). При выборе этой опции папка и все ее содержимое будет скопировано обратно в оригинальное расположение. Контент не будет удален из предыдущего расположения.
5. Если вы изменили опцию Политика удаления (Policy Removal), нажмите кнопку Применить (Apply), а затем перейдите на вкладку Целевая папка. Если не было никаких изменений, просто перейдите на вкладку Целевая папка.
6. Для удаления всех определений перенаправлений для специальной папки выберите переключатель Не задана (Not Configured) в списке Политика (Setting).
7. Для удаления перенаправления определенной группы выберите группу в области Членство в группе безопасности (Security Group Membership) и нажмите Удалить (Remove). Нажмите кнопку OK.

Управление сценариями пользователя и компьютера

В Windows Server можно настроить четыре типа сценариев:

Computer Startup — выполняется при запуске;
Computer Shutdown — выполняется при завершении работы;
User Logon — выполняется, когда пользователь входит в систему;
User Logoff — выполняется, когда пользователь выходит из системы.

Windows 2000 и более поздние версии поддерживают сценарии, написанные на языке командной оболочки, с расширением bat и cmd или сценарии, которые используют Windows Script Host (WSH).

WSH - это компонент Windows Server, позволяющий использовать сценарии, написанные на языке сценариев вроде VBScript без необходимости вставки сценария в веб-страницу. Для предоставления доступа к многоцелевой среде WSH основывается на движках сценариев. Движок сценариев — это компонент, определяющий основной синтаксис и структуру определенного

языка сценариев. Windows Server поддерживает движки сценариев для VBScript и JScript. Также доступны другие движки.
Операционные системы Windows 7, Windows 8, Windows Server 2008 R2 и Windows Server 2012 также поддерживают сценарии PowerShell. Если Windows PowerShell установлен на компьютеры, которые обрабатывают определенные GPO, можно использовать сценарии Windows PowerShell так же, как и остальные сценарии. Есть возможность запуска сценариев Windows PowerShell до или после других типов сценариев.

Назначения сценариев *Computer Startup* и *Computer Shutdown*

Сценарии Computer Startup и Computer Shutdown назначаются как часть GPO. Таким образом, все компьютеры, которые являются членами сайта, домена и организационного подразделения или всех трех структур одновременно, выполняют сценарии автоматически, когда загружаются или завершают работу. Чтобы назначить сценарий запуска или завершения работы, выполните следующие действия:

1. В Проводнике Windows откройте папку, содержащую сценарии, которые нужно использовать.
2. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которыми будете работать. Выберите команду Изменить, чтобы открыть редактор GPO.
3. В узле Конфигурация компьютера (Computer Configuration) дважды щелкните на папке Конфигурация Windows (Windows Settings), затем перейдите в подпапку Сценарии (запуск/завершение) (Scripts).
4. Для работы со сценариями запуска щелкните правой кнопкой мыши на элементе Автозагрузка (Startup) и выберите команду Свойства (Properties). Для работы со сценариями завершения работы щелкните правой кнопкой на элементе Завершение работы (Shutdown) и выберите команду Свойства.
5. На вкладке Сценарии (Scripts) можно управлять сценариями командной строки (с расширениями bat или cmd) и сценариями Windows Scripting Host. На вкладке Сценарии PowerShell (PowerShell Scripts) можно управлять сценариями Windows PowerShell. Для перехода к папке, в которой находятся сценарии, нажмите кнопку Показать файлы (Show Files).
6. Скопируйте файлы в окне Проводника Windows и вставьте их в окно, которое будет открыто после нажатия кнопки Показать файлы.
7. Нажмите кнопку Добавить для назначения сценария. Откроется окно Добавление сценария (Add A Script). В поле Имя сценария (Script Name) введите имя сценария, который был скопирован в папку Machine\Scripts\Startup или папку Machine\Scripts\Shutdown.
8. В поле Параметры сценария (Script Parameters) введите любые параметры, которые нужно передать сценарию. Повторите этот шаг для других сценариев.

9. Во время запуска и завершения работы сценарии будут выполнены в том порядке, в котором они указаны в окне Свойства. На вкладке Сценарии используйте кнопки Вверх (Up) и Вниз (Down) для изменения порядка выполнения сценариев. Такие же кнопки есть на вкладке Сценарии PowerShell. На вкладке Сценарии PowerShell есть также список, позволяющий выбрать, когда должны запускаться сценарии Windows PowerShell: до или после запуска других типов сценариев.
10. Если нужно отредактировать имя сценария или его параметры, выберите сценарий и нажмите кнопку Изменить. Для удаления сценария выберите его и нажмите кнопку Удалить.
11. Для сохранения изменений нажмите кнопку OK.

Назначение сценариев входа и выхода пользователя

Сценарии пользователя можно назначить с помощью одного из трех способов.

Можно назначить сценарии входа/выхода как часть GPO. В этом случае все пользователи, являющиеся членами сайта, домена или организационного подразделения (или всех трех сразу) автоматически запустят сценарии при входе или выходе.

Можно назначить сценарии входа индивидуально, используя консоль Active Directory — пользователи и компьютеры (Active Directory Users And Computers). В этомслучае можно назначить каждому пользователю или каждой группе отдельный сценарий входа. Подробно этот способ будет рассмотрен в главе 9.

Также можно назначить отдельные сценарии выхода как запланированные задачи. Для создания расписаний задач используется мастер создания задачи (Scheduled Task Wizard).

Чтобы назначить сценарии входа или выхода в GPO, выполните следующие действия:

1. В Проводнике Windows откройте папку, содержащую сценарии, которые нужно использовать.
2. В консоли GPMC щелкните правой кнопкой мыши по GPO сайта, домена или организационного подразделения, с которыми планируете работать. Выберите команду Изменить, чтобы открыть редактор GPO.
3. В узле Конфигурация пользователя (User Configuration) дважды щелкните на папке Конфигурация Windows (Windows Settings), затем перейдите в узел Сценарии (вход/выход из системы) (Scripts).
4. Для работы со сценариями входа щелкните правой кнопкой мыши на папке Вход в систему (Logon) и выберите команду Свойства. Для работы со сценариями выхода щелкните правой кнопкой мыши на папке Сценарии выхода (Logoff) и выберите команду Свойства.
5. На вкладке Сценарии можно управлять сценариями командной строки (с расширениями bat или cmd) и сценариями Windows Scripting Host. На вкладке Сценарии PowerShell можно управлять сценариями Windows PowerShell. Для перехода к папке, в которой находятся сценарии, нажмите кнопку Показать файлы.

6. Скопируйте файлы в окне Проводника Windows и вставьте их в окно, которое будет открыто после нажатия кнопки Показать файлы.
7. Нажмите кнопку Добавить для назначения сценария. Откроется окно Добавление сценария. В поле Имя сценария введите имя сценария, который скопирован в папку User\Scripts\Startup или папку User\Scripts\Shutdown. В поле Параметры сценария введите любые параметры, которые нужно передать сценарию. Повторите этот шаг для других сценариев.
8. Во время входа в систему и выхода из нее сценарии будут выполнены в том порядке, в котором они определены в окне Свойства. На вкладке Сценарии используйте кнопки Вверх и Вниз для изменения порядка сценариев в случае необходимости. Такие же кнопки есть на вкладке Сценарии PowerShell. На вкладке Сценарии PowerShell существует также список, позволяющий выбрать, когда должны запускаться сценарии Windows PowerShell: до или после запуска других типов сценариев.
9. Если нужно отредактировать имя сценария или его параметры, выберите сценарий и нажмите кнопку Изменить. Для удаления сценария выберите его и нажмите кнопку Удалить.
10. Для сохранения изменений нажмите кнопку OK.

Развертывание программного обеспечения через групповую политику

Для развертывания ПО в групповой политики есть базовая функциональность, называемая политикой установки программного обеспечения. Хотя она не разработана для замены решений для предприятий вроде SMS (Systems Management Server), можно использовать ее для автоматизации развертывания и обслуживания ПО в организации практически любого размера при условии, что все компьютеры работают под управлением бизнес-выпусков Windows 2000 или более поздних версий.

Знакомство с политикой установки программного обеспечения

В групповой политике можно развертывать ПО на основе компьютеров и пользователей. Приложения на базе компьютеров доступны всем пользователям компьютера и настраиваются в узле Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation). Можно развернуть программы тремя основными способами.

Назначение компьютеру (Computer assignment) — назначает программное обеспечение на компьютеры клиента, чтобы установка ПО выполнялась при запуске компьютера. Эта техника не требует какого-либо вмешательства со стороны пользователя, но она нуждается в перезагрузке системы для установки программ. Установленное программное обеспечение будет доступно всем пользователям компьютера.

Назначение пользователю (User assignment) — назначает программное обеспечение пользователям так, что оно будет установлено при входе пользователя в систему. Эта техника не требует какого-либо вмешательства со стороны пользователя, но предполагает вход в систему для установки программы. Установленное программное обеспечение будет доступно только конкретному пользователю.

Публикация пользователю (User publishing) — публикует программное обеспечение так, что пользователи могут установить его вручную с помощью утилиты Программы и компоненты (Programs And Features). Эта техника требует вмешательства пользователя для установки программы или активации установки. Установленное программное обеспечение будет доступно только конкретному пользователю.

При использовании назначения пользователю или публикации пользователю можно объявлять программное обеспечение так, чтобы компьютер мог установить программу при ее первом использовании. В этом случае программное обеспечение может быть установлено автоматически в следующих ситуациях:

- когда пользователь пытается открыть документ, для работы с которым нужна программа;
- когда пользователь открывает ярлык приложения;
- когда другому приложению требуется компонент программы.

При настройке политики Установка программ (Software Installation) не нужно использовать существующие GPO. Вместо этого следует создать объекты GPO, которые будут настраивать установку программ и затем привязать эти GPO к соответствующим контейнерам в групповой политике. При использовании этого подхода значительно проще повторно развернуть программное обеспечение и применить обновления.

После создания GPO для разворачивания программного обеспечения нужно настроить точку распространения. Точка распространения — это общая папка, которая доступна компьютерам и пользователям, для которых вы разворачиваете ПО. Как правило, можно подготовить точку распространения путем копирования файла пакета инсталлятора и всех необходимых приложению файлов на общий ресурс и настройкой разрешений так, чтобы все эти файлы были доступны. Для других приложений, например Microsoft Office, можно подготовить точку восстановления путем административной установки на общий ресурс. В случае с MS Office нужно запустить программу установки с параметром /a и указать общий ресурс как назначение установки. Преимущество административной установки состоит в том, что программное обеспечение может быть обновлено и повторно развернуто через политику Установка программ.

Можно обновить приложения, развернутые через политику Установка программ либо с помощью обновления или сервис-пака, либо с помощью развертывания новой версии приложения. Эти задачи немного отличаются друг от друга.

Развертывание программ в организации

Политика Установка программ используется только с пакетами установщика Windows (msi) и пакетами приложений нижнего уровня ZAW (zap). При использовании назначения компьютера, назначения пользователя или публикации можно развернуть ПО с помощью пакетов установщика Windows. При использовании публикации можно применять как msiпакеты, так и zap-пакеты. Необходимо установить разрешения на файле пакета установщика так, чтобы у соответствующих компьютеров и пользователей был доступ для чтения.

Поскольку политика Установка программ применяется во время обработки настроек политики, развертывание приложения на компьютере обрабатывается при его запуске, а развертывание приложения для пользователя осуществляется при входе в систему. Можно настроить установку с использованием файлов преобразований (mst). Эти файлы изменяют процесс установки согласно настройкам, которые заданы для определенных компьютеров и пользователей.

Развернуть программное обеспечение можно с помощью следующих действий:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO, который нужно модифицировать для распространения, и затем нажмите кнопку Изменить.
2. В редакторе политики разверните узел Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation) или узел Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation) в зависимости от типа разворачивания ПО.
3. Щелкните правой кнопкой мыши на политике Установка программ. В появившемся контекстном меню выберите команду Создать | Пакет (New | Package).
4. В окне Открытие (Open) перейдите к сетевому ресурсу, в котором размещены пакеты, щелкните на пакете для его выбора и нажмите кнопку Открыть (Open).
5. В окне Развертывание программ (Deploy Software), показанном на рис. 4.16, выберите один из следующих методов развертывания и нажмите кнопку ОК:
   - публичный (Published) — публикует приложение без изменений;
   - назначенный (Assigned) — назначает приложение без изменений;
   - особый (Advanced) — развертывание приложения с использованием расширенных параметров настройки.

В списке типов файлов (в диалоговом окне открытия файла) по умолчанию выбраны пакеты установщика Windows (msi). Если нужно выполнить публикацию программного обеспечения, можно также выбрать тип файла Пакеты приложений нижнего уровня ZAW (.zap).

Настройка параметров развертывания программного обеспечения

Просмотреть и установить основные параметры для пакета программного обеспечения можно с использованием следующих действий:

1. В консоли GPMC щелкните правой кнопкой мыши на GPO, который используете для развертывания, и выберите команду Изменить.
2. В редакторе политики разверните узел Конфигурация компьютера\Конфигурация программ\Установка программ или узел Конфигурация пользователя\Конфигурация программ\Установка программ в зависимости от типа разворачивания ПО.
3. Дважды щелкните по пакету установки ПО. В окне Свойства можно просмотреть или модифицировать параметры развертывания ПО.
4. На вкладке Развертывание (Deployment) (рис. 4.17) можно изменить тип развертывания и настроить следующие параметры развертывания и установки.
   - Автоматически устанавливать приложение при обращении к файлу с соответствующим расширением (Auto-Install This Application By File Extension Activation) — связывает приложение с файлами, которое оно обрабатывает. Программа будет установлена при первом обращении к файлу связанного типа. Используется по умолчанию.
   - Удалять это приложение, если его использование выходит за рамки, допустимые политикой управления (Uninstall This Application When It Falls Out Of The Scope Of Management) — удаляет приложение, если оно больше не применимо к пользователю.
   - Не отображать этот пакет в окне мастера установки и удаления программ панели управления (Do Not Display This Package In The Add/Remove Programs Control Panel) — запрещает отображение приложения в окне Установка/удаление программ, что предотвращает удаление приложения пользователем.
   - Устанавливать это приложение при входе в систему (Install This Application At Logon) — при входе пользователя в систему будет произведена полная установка программы, а не "объявление" приложения. Эта опция не может быть выбрана, когда приложение публикуется для пользователя.
   - Пользовательский интерфейс при установке (Installation User Interface Options) — контролирует, как будет произведена установка. Значение по умолчанию — Полный (Maximum), при этом пользователь увидит все экраны программы установки и все сообщения. При значении Простой (Basic) пользователь увидит только сообщения об ошибках и сообщение о завершении установки.
5. Нажмите кнопку OK.

Обновление развернутого программного обеспечения

Когда приложение использует пакет установщика Windows, можно применить обновление или пакет обновлений к развернутому приложению с помощью следующих действий:

1. После получения msi- или msp-файла (патч), содержащего обновления или пакет обновлений, который будет применен, скопируйте его и любые другие установочные файлы в папку, содержащую оригинальный msi-файл. В случае необходимости перезапишите любые повторяющиеся файлы.
2. В консоли GPMC щелкните правой кнопкой мыши на GPO, который вы используете для развертывания, и выберите команду Изменить.
3. В редакторе политики разверните узел Конфигурация компьютера\Конфигурация программ\Установка программ или узел Конфигурация пользователя\Конфигурация программ\Установка программ в зависимости от типа разворачивания ПО.
4. Щелкните правой кнопкой мыши по пакету, затем в контекстном меню выберите команды Все задачи | Развернуть приложение заново (All Tasks | Redeploy Application).
5. Когда консоль попросит подтвердить действие, нажмите кнопку Да. Приложение будет заново развернуто для всех пользователей и компьютеров, в соответствии с выбранным GPO.

Когда приложение не использует пакеты установщика Windows, можно обновить развернутое приложение или применить пакет обновлений следующим образом:

В консоли GPMC щелкните правой кнопкой мыши на GPO, который используется для развертывания, и выберите команду Изменить.

В редакторе политики разверните узел Конфигурация компьютера\Конфигурация программ\Установка программ или узел Конфигурация пользователя\Конфигурация программ\Установка программ в зависимости от типа разворачивания ПО.

Щелкните правой кнопкой мыши по пакету, а затем в контекстном меню выберите команды Все задачи | Удалить (All Task | Remove).

Скопируйте новый zap-файл и все дополнительные файлы на сетевой ресурс и заново разместите приложение.

Обновление развернутого приложения

Обновить ранее развернутое приложение можно до более новой версии следующим образом:

1. Получите новый файл установщика Windows, содержащий новую версию программного обеспечения, скопируйте его и все необходимые файлы на сетевой ресурс. Альтернативно можно осуществить административную установку на сетевой ресурс.
2. В консоли GPMC щелкните правой кнопкой мыши на GPO, который используется для развертывания, и выберите команду Изменить.

3. В редакторе политики разверните узел Конфигурация компьютера\Конфигурация программ\Установка программ или Конфигурация пользователя\Конфигурация программ\Установка программ в зависимости от типа разворачивания ПО.
4. Щелкните правой кнопкой мыши на политике Установка программ. В появившемся контекстном меню выберите команды Создать | Пакет (New | Package). Создайте и назначьте или опубликуйте приложение с использованием пакета установщика Windows для новой версии ПО.
5. Щелкните правой кнопкой мыши по названию пакета и выберите команду Свойства. На странице Обновления (Upgrades) нажмите кнопку Добавить. В окне Добавление обновления (Add Upgrade Package) выполните одно из следующих действий.
   - Если исходное приложение и обновление находятся в текущем GPO, выберите переключатель из текущего объекта групповой политики (GPO) (Current Group Policy Object), а затем выберите ранее развернутое приложение в списке Обновляемое приложение (Package To Upgrade).
   - Если исходное приложение и обновление находятся в разных GPO, выберите переключатель из указанного объекта групповой политики (A Specific GPO). Далее нажмите кнопку Обзор и выберите GPO в окне Поиск объекта групповой политики (Browse For A Group Policy Object). Затем выберите ранее развернутое приложение из списка Обновляемое приложение (Package To Upgrade).
6. Выберите опции обновления. Если нужно заменить приложение новой версией, выберите переключатель Удалить приложение, затем установить его обновление (Uninstall The Existing Package). Если же нужно осуществить именно обновление поверх существующей инсталляции, выберите переключатель Обновление возможно поверх имеющегося приложения (Package Can Upgrade Over The Existing Package).
7. Нажмите кнопку OK для закрытия окна Добавление обновления. Если нужно сделать это обновление обязательным, выберите переключатель Обязательное обновление для уже установленных приложений (Required Upgrade For Existing Packages), а затем нажмите кнопку OK для закрытия окна Свойства.

Автоматическая регистрация сертификатов компьютера и пользователя

Сервер, определенный как центр сертификации, отвечает за выпуск цифровых сертификатов и управление списками аннулированных сертификатов (Certificate Revocation Lists, CRLs). Серверы под управлением Windows Server могут быть сконфигурированы как центры сертификации, для этого нужно установить Службы сертификатов Active Directory
(Active Directory Certificate Services, AD CS). Компьютеры и пользователи могут использовать сертификаты для аутентификации и шифрования.

На предприятии используются корпоративные центры сертификации для автоматической регистрации сертификатов. Это означает, что авторизированные пользователи и компьютеры могут запросить сертификат, а центр сертификации — автоматически обработать запрос сертификата так, чтобы пользователи и компьютеры могли сразу установить сертификат. Групповая политика контролирует способ работы автоматической регистрации. При установке корпоративного центра сертификации политика автоматической регистрации для пользователей и компьютеров включается автоматически. Политика для регистрации сертификатов компьютера называется Клиент служб сертификации: автоматическая регистрация (Certificate Services Client — Auto-Enrollment Settings) и находится в узле Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\ Политики открытого ключа (Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies). Политика для регистрации сертификатов пользователя называется Клиент служб сертификации: автоматическая регистрация и находится в узле Конфигурация пользователя\Политики\Конфигурация Windows\Параметры безопасности\Политики открытого ключа (User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies).

Настроить автоматическую регистрацию можно так:

- В консоли GPMC щелкните правой кнопкой мыши по GPO и выберите команду Изменить.
- В редакторе политик разверните узел Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики открытого ключа или узел Конфигурация пользователя\Политики\Конфигурация Windows\Параметры безопасности\Политики открытого ключа в зависимости от политики, настройки которой нужно просмотреть.
- Дважды щелкните на политике Клиент служб сертификации: автоматическая регистрация. Для отключения автоматической регистрации установите переключатель Отключено (Disabled) из списка Модель конфигурации (Configuration Model) и нажмите кнопку OK. Далее пропустите все последующие шаги этой процедуры. Для включения автоматической регистрации установите переключатель Включено (Enable) из списка Модель конфигурации.
- Для автоматического возобновления истекших сертификатов, обновления сертификатов в состоянии ожидания и удаления отозванных сертификатов установите соответствующий флажок.
- Чтобы убедиться, что используется последняя версия шаблонов сертификатов, отметьте флажок Обновлять сертификаты, использующие шаблоны сертификатов (Update Certificates That Use Certificate Templates).
- Для уведомления пользователей о том, что срок сертификата скоро выйдет, определите, когда будут отправлены уведомления пользователям. По умолчанию уведомления отправляются, когда осталось 10% от времени жизни сертификата.

Нажмите кнопку OK для сохранения настроек.

Управление автоматическими обновлениями с помощью групповой политики

Автоматические обновления помогают поддерживать операционную систему в актуальном состоянии. Хотя можно настроить автоматические обновления на основе компьютеров, обычно необходимо настроить эту функцию для всех пользователей и компьютеров, которые обрабатывают GPO — это более эффективная техника управления.

Заметьте, что по умолчанию Windows 8 и Windows Server 2012 используют Windows Update для загрузки компонентов Windows, а также двоичных файлов для ролей, служб ролей и компонентов. Если средства диагностики Windows определят, что компонент Windows требует ремонта, Windows использует Windows Update для загрузки компонента. Если администратор пытается установить роль, службу роли или компонент, а полезные данные отсутствуют (payloads), Windows использует Windows Update для загрузки нужных бинарных файлов.

Настройка автоматических обновлений

При управлении автоматическими обновлениями через групповую политику можно выбрать конфигурацию обновления.

1. Автоматическая загрузка и установка по расписанию (Auto Download And Schedule The Install) — обновления будут автоматически загружены и установлены в соответствии с созданным расписанием. Когда обновления будут загружены, операционная система уведомит пользователя, что он может просмотреть запланированные обновления. Пользователь может установить обновления или подождать, пока придет время запланированной установки.
2. Автоматическая загрузка и уведомление об установке (Auto Download And Notify For Install) — операционная система получит все обновления и, когда они станут доступны, уведомит пользователя, что они готовы к установке. Пользователь может принять или отклонить обновления. Принятые обновления будут установлены. Отклоненные обновления не будут установлены, но останутся в системе и их можно будет установить позже.
3. Уведомление о загрузке и установке (Notify For Download And Notify For Install) — операционная система уведомляет пользователя перед получением любых обновлений. Если пользователь выберет загрузку обновлений, у него есть еще возможность принять или отклонить их. Принятые обновления будут установлены. Отклоненные обновления не будут установлены, но останутся в системе, и их можно будет установить позже.
4. Разрешить локальному администратору выбирать параметры (Notify For Download And Notify For Install) — позволяет локальному администратору настраивать автоматическое обновление. Заметьте, что

используются любые другие опции, локальные пользователи и администраторы не могут изменить параметры автоматического обновления.

Настроить автоматическое обновление можно так:

В консоли GPMC щелкните правой кнопкой мыши по GPO, с которым нужно работать, и выберите команду Изменить.

В редакторе политик разверните узел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\ Центр обновления Windows (Computer Configuration\ Administrative Templates\Windows Components\Windows Update).

Дважды щелкните на политике Настройка автоматического обновления (Configure Automatic Updates). В появившемся окне можно включить или отключить управление автоматическими обновлениями с помощью групповой политики. Для включения управления автоматическими обновлениями установите переключатель Включено, для отключения управления — переключатель Отключено. Нажмите кнопку OK и пропустите следующие шаги.

Из списка Настройка автоматического обновления (Configure Automatic Updating) выберите опцию обновления.

Если выбрана опция Автоматическая загрузка и установка по расписанию (Auto Download And Schedule The Install), можете выбрать день и время установки обновлений. Нажмите кнопку OK для сохранения изменений.

Оптимизация автоматических обновлений

В целом, большинство автоматических обновлений устанавливается только при перезагрузке компьютера. Некоторые автоматические обновления могут быть установлены немедленно без прерывания системных служб и перезапуска системы. Чтобы убедиться, что эти обновления устанавливаются немедленно, выполните следующие шаги:

1. В консоли GPMC щелкните правой кнопкой мыши по GPO, с которым нужно работать, и выберите команду Изменить.
2. В редакторе политик разверните узел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\ Центр обновления Windows.
3. Дважды щелкните на политике Разрешить немедленную установку автоматических обновлений (Allow Automatic Updates Immediate Installation). В окне Свойства установите переключатель Включено и нажмите кнопку OK.

По умолчанию только пользователи с привилегиями локальных администраторов получают уведомления об обновлениях. Можно разрешить любому зарегистрированному пользователю получать уведомления об обновлениях так:

В консоли GPMC щелкните правой кнопкой мыши по GPO, который нужно модифицировать, и выберите команду Изменить.

В редакторе политик разверните узел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows.

Дважды щелкните на политике Разрешать пользователям, не являющимися администраторами, получать уведомления об обновлениях (Allow Non-Administrators To Receive Update Notifications). В окне Свойства установите переключатель Включено и нажмите кнопку OK.

Другая полезная политика — Запретить использование любых средств Центра обновления Windows (Remove Access To Use All Windows Update Features). Она запрещает доступ

ко всем функциям Центра обновления. Если политика включена, все функции Центра обновления будут удалены и не могут быть настроены, в том числе будет недоступна вкладка Центр обновления (Windows Update) в утилите Система (System) и обновление драйверов от сайта Windows Update в диспетчере устройств. Данная политика находится в узле Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Центр обновления Windows.

Использование службы обновлений в интрасети

В сетях с сотнями и тысячами компьютеров процесс автоматического обновления может использовать значительную часть пропускной способности сети, в конечном итоге не целесообразно, чтобы каждый компьютер проверял обновления и загружал их по Интернету. Вместо этого рассмотрите использование политики службы обновления Microsoft в интрасети, которая обязывает отдельные компьютеры проверять обновления на выделенном внутреннем сервере.

На выделенном сервере обновлений должны быть запущены службы Windows Server Update Services (WSUS), также он должен быть настроен как веб-сервер (на нем должен быть запущен Microsoft Internet Information Services, IIS), и он должен выдержать дополнительную нагрузку, которая будет значительной в большой сети во время пикового использования службы обновления. Дополнительно, у сервера обновлений должен быть открыт порт 80 для доступа к внешней сети. Использование брандмауэра или прокси-сервера на этом порту не должно вызвать какие-либо проблемы.

Процесс обновления также отслеживает конфигурационную информацию и статистику для каждого компьютера. Эта информация необходима для корректной работы процесса обнов-ления и может быть сохранена на отдельном сервере статистики (сервере внутренней сети, на котором запущен IIS) или же на самом сервере обновления.

Чтобы указать внутренний сервер обновления, выполните следующие действия:

1. После установки и настройки сервера обновлений откройте GPO, который нужно отредактировать. В редакторе политик разверните узел Конфигурация компьютера\ Административные шаблоны\Компоненты Windows\Центр обновления Windows.

2. Дважды щелкните на политике Указать размещение службы обновления Майкрософт в интрасети (Specify Intranet Microsoft Update Service Location).
3. В поле Укажите службу обновлений в интрасети для поиска обновлений (Set The Intranet Update Service For Detecting Updates) укажите URL сервера обновления, например, http://CorpUpdateServer01.
4. В поле Укажите сервер статистики в интрасети (Set The Intranet Statistics Server) введите URL сервера статистики. Сервер статистики не обязательно должен быть отдельным сервером, в этом поле можно указать адрес сервера обновлений.
5. Нажмите кнопку OK. После обновления GPO системы, работающие под определенными версиями Windows, будут использовать внутренний сервер для обновлений. Необходимо контролировать серверы обновлений и статистики несколько дней или даже недель, чтобы убедиться, что они работают корректно. На сервере обновлений и сервере статистики будут созданы файлы и каталоги.

Если нужно использовать один сервер и для обновлений, и для статистики, введите один и тот же URL в оба поля. В противном случае, введите разные URL в соответствующие поля.

Литература

- Моримото Р., Ноэл М. Microsoft Windows Server 2012. Полное руководство. – М.:Вильямс, 2013. – 1456 с.: с ил.
- Станек У. Р. Microsoft Windows Server 2012. Справочник администратора. – М.:БВХ-Петербург, 2014, – 688 с.: с ил.
- Internet-ресурсы:
  www.microsoft.com/ru/ru/
  www.technet.microsoft.com/ru-ru
  www.intuit.ru

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра аппаратно-программных комплексов вычислительной техники входит в состав Академии ЛИМТУ Университета ИТМО и имеет более чем 40-летний опыт научно-педагогической деятельности в области профессиональной переподготовки и повышения квалификации специалистов. За последние 20 лет на кафедре прошли обучение более 11 тысяч человек не только из Санкт-Петербурга, но и из различных городов России, а также стран ближнего и дальнего зарубежья. Наши выпускники работают руководителями проектов и начальниками IT-отделов, системными инженерами и системными администраторами, программистами и специалистами по эксплуатации аппаратно-программных комплексов вычислительной техники.

На сегодняшний день на кафедре реализуются следующие направления деятельности:

- подготовка магистров по направлению 09.04.01 «Информатика и вычислительная техника»;
- подготовка бакалавров (без отрыва от производства – вечерняя форма обучения) по направлению 09.03.01 Информатика и вычислительная техника;
- переподготовка специалистов, имеющих высшее образование, с выдачей государственного диплома о дополнительном (к высшему) образовании с присвоением квалификации;
- переподготовка специалистов, имеющих высшее и среднее профессиональное образование с выдачей государственного диплома о переподготовке с правом работы по новой специальности;
- повышение квалификации с выдачей государственного свидетельства (удостоверения)/сертификата Университета ИТМО.

С сентября 2003 года при кафедре функционирует Учебный центр, в котором проводится обучение по программным продуктам фирмы 1С последних версий.

С 2007 года на базе кафедры создан авторизованный Учебный центр фирмы ZyXEL, в котором проводится обучение по теории и практике применения

современного сетевого оборудования для построения LAN-WAN сетей с использованием оборудования и технологий ZyXEL.

В 2012 году был создан Авторизованный Учебный центр фирмы QNAP для подготовки сертифицированных специалистов по системам IP-видеонаблюдения и сетевых хранилищ данных.

Программы обучения ориентированы на приобретение устойчивых профессиональных навыков и имеют практическую направленность. Основное время слушатели проводят за компьютером, выполняя большой объем практических заданий. Обучающиеся также получают минимальный объем теоретических знаний, необходимых для грамотного выполнения практических заданий.

Занятия проводятся в пяти специализированных классах, оснащенных современными компьютерами, объединенными в локальную вычислительную сеть с выходом в Интернет. Последние версии программных продуктов ведущих фирм производителей используются не только в учебном процессе, но и выдаются слушателям для установки на домашние компьютеры.

Постоянным заказчиком кафедры на переподготовку специалистов является Департамент федеральной государственной службы занятости населения по Санкт-Петербургу. Обучение слушателей осуществляется также на бюджетной и коммерческой основе.

Светлана Михайловна Платунова

Windows Server 2012. Управление серверами. Автоматизация административных задач

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж 100 экз.
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49