УНИВЕРСИТЕТ ИТМО

С.М. Платунова

АДМИНИСТРИРОВАНИЕ ДАННЫХ WINDOWS SERVER 2012

Учебное пособие

Санкт-Петербург

2016

С.М. Платунова

АДМИНИСТРИРОВАНИЕ ДАННЫХ WINDOWS SERVER 2012

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2016

Платунова С.М. Администрирование данных Windows Server 2012. Учебное пособие по дисциплине «Администрирование вычислительных сетей». – СПб: НИУ ИТМО, 2016. – 135 с.

В учебном пособии содержатся основные сведения об управлении файловыми системами и дисками, настройке томов и RAID-массивов, общим доступом к данным, безопасности и аудите 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.

Содрежание

ГЛАВА 1 Управление файловыми системами и дисками

Жесткий диск — наиболее часто используемое устройство хранения данных, установленное на рабочих станциях и серверах сети. Пользователи зависят от жестких дисков, поскольку хранят на них текстовые документы, электронные таблицы и данные других типов. Диски организованы в файловые системы, к которым пользователи могут получить доступ либо локально, либо удаленно. Локальные файловые системы установлены на компьютерах пользователей, и доступ к ним может быть получен без установки удаленных сетевых соединений. Диск C:, доступный на большинстве рабочих станций и серверов, является примером локальной файловой системы. Получить доступ к диску C: можно с использованием пути C:\.

С другой стороны, получить доступ к удаленным файловым системам можно с помощью сетевого соединения с удаленным ресурсом. А подключиться к удаленной файловой системе можно, нажав кнопку Подключить сетевой диск (Map Network Drive) в Проводнике. Одна из задач системного администратора — управление всеми дисковыми ресурсами.

Инструменты и методы, используемые для управления файловыми системами и дисками, обсуждаются в этой главе. В главе 11 мы поговорим о настройке томов и RAID-массивов для обеспечения отказоустойчивости.

Управление ролью *Файловые службы*

Файловый сервер предоставляет централизованное место для хранения и совместного использования файлов по сети. Когда много пользователей нуждается в доступе к одним и тем же файлам и данным приложений, необходимо настроить файловые серверы в домене.

В более ранних версиях операционной системы Microsoft Windows Server все серверы устанавливались с базовыми файловыми службами.

В случае с Windows Server 2012 нужно специально настроить сервер в качестве файлового сервера, добавив роль Файловые службы (File Services) и настроив эту роль использовать надлежащие службы роли.

В табл. 1.1 предоставлен обзор служб роли, связанных с ролью Файловые службы. При установке роли Файловые службы может понадобиться также установка следующих дополнительных компонентов, доступных в мастере добавления компонентов (Add Roles And Features Wizard):

1. Система архивации данных Windows Server (Windows Server Backup) — стандартная утилита архивации, входящая в состав Windows Server 2012;
2. Enhanced Storage — предоставляет дополнительные функции устройств с поддержкой аппаратного шифрования и расширенного хранения. Такие устройства используют стандарт IEEE 1167 (Institute of Electrical and Electronic Engineers) для предоставления расширенной безопасности, которая может включать аутентификацию на аппаратном уровне устройства хранения данных;

3. Multipath I/O — предоставляет поддержку для использования множественных путей данных между файловым сервером и устройством хранения данных. Серверы используют пути ввода-вывода для избыточности в случае сбоя пути и для повышения производительности передачи данных.
4. Если двоичные файлы утилит были удалены, нужно установить утилиты из определенного источника.

Таблица 1.1. Службы ролей для Файловых служб

Служба роли	Описание
Служба BranchCache для сетевых файлов (BranchCache For Network Files)	Позволяет компьютерам в филиале кэшировать часто используемые файлы в совместно используемых папках. Такое решение использует методы дедупликации данных, чтобы оптимизировать передачу данных по глобальным сетям (WAN) к филиалам
Дедупликация данных (Data Deduplication)	Для достижения большей эффективности хранения использует разделение файлов на блоки переменного размера и сжатие. Суть процесса заключается в том, чтобы хранить большее количество данных на меньшем пространстве в небольших (32—128 Кбайт) блоках разного размера, определяя дублирующие блоки и сохраняя одну копию для каждого блока. Оптимизированные файлы хранятся как точки повторного анализа. После дедупликации файлы на томе больше не хранятся как потоки данных, а вместо этого они заменяются заглушками, указывающими на блоки данных, хранящиеся в общем хранилище блоков
Пространства имен распределенной файловой системы (DFS)	(DFS Namespaces) Позволяет группировать совместно используемые папки, находящиеся на разных серверах в одном или нескольких логически структурированных пространствах имен. Каждое пространство имен появляется как единственная общая

	папка с серией подпапок. Однако структура пространства имен может быть получена из совместно используемых папок на множественных серверах в различных сайтах
Репликация DFS (DFS Replication)	Позволяет синхронизировать папки на множественных серверах, находящихся в локальной или глобальной сети с использованием механизма репликации multimaster. Механизм репликации использует протокол RDC (Remote Differential Compression) для синхронизации порций файлов, которые изменились с момента последней репликации. Использовать репликацию DFS допускается с пространствами имен DFS или без них. Когда домен работает в режиме Windows Server 2008 или выше, контроллеры домена используют репликацию DFS для обеспечения большей отказоустойчивой репликации каталога SYSVOL
Файловый сервер (File Server)	Позволяет управлять совместно используемыми файлами, к которым пользователи могут получить доступ по всей сети
Диспетчер ресурсов файлового сервера (FSRM) File Server Resource Manager (FSRM)	Устанавливает набор утилит, которые администраторы могут использовать для лучшего управления хранимыми на сервере данными. Посредством FSRM администраторы могут генерировать отчеты хранения данных, настраивать квоты, определять политики файлов
Служба агента VSS файлового сервера (File Server VSS Agent Service)	Позволяет VSS-совместимым утилитам резервного копирования создавать непротиворечивые теневые копии (снимки) приложений, которые хранят файлы данных на файловом сервере
Сервер цели iSCSI (iSCSI Target Server)	Превращает любой Windows Server в доступное по сети блочное

	устройство хранения, которое может использоваться для тестирования приложений перед развертыванием SAN-хранилища. Поддерживает совместно используемые хранилища на не-Windows iSCSI-инициаторах и сетевую/бездисковую загрузки для бездисковых серверов
Поставщик целевого хранилища iSCSI (iSCSI Target Storage Provider)	Поддерживает управление виртуальными дисками iSCSI и теневыми копиями (снимками) из iSCSI-инициатора
Сервер для NFS (Server for NFS)	Предоставляет решение обмена файлами для предприятий со смешанной средой Windows и UNIX. После установки служб для сетевой файловой системы (Network File System, NFS) пользователи смогут обмениваться файлами между Windows Server и UNIX с помощью протокола NFS
Службы хранилища (Storage Services)	Позволяет управлять хранилищем, в том числе пулами и пространствами. Пулы хранилищ группируют диски так, что можно создать виртуальные диски из доступной емкости. Каждый созданный вами виртуальный диск — это пространство хранилища

Добавить роль Файловые службы на сервер можно с помощью следующих действий:

1. В окне диспетчер серверов в меню Управление выберите команду Добавить роли и компоненты или щелкните по ссылке Добавить роли и компоненты на плитке приветствия. В результате будет запущен мастер добавления ролей и компонентов (Add Roles And Features Wizard). Если мастер отобразит страницу Перед началом работы (Before You Begin), прочитайте текст приветствия и нажмите кнопку Далее.
2. На странице Выбор типа установки (Installation Type) по умолчанию отмечен переключатель Установка ролей или компонентов (Role-Based Or Feature-Based Installation). Нажмите кнопку Далее.
3. На странице Выбор целевого сервера (Server Selection) можно выбрать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите либо сервер из пула серверов, либо сервер, на котором можно смонтировать виртуальный жесткий диск (virtual hard disk, VHD). Если роли и компоненты добавляются на VHD, нажмите кнопку Обзор, а затем используйте окно Обзор виртуальных жестких

дисков (Browse For Virtual Hard Disks) для выбора виртуального жесткого диска. Когда будете готовы продолжить, нажмите кнопку Далее.

В списке диспетчера серверов приводятся только серверы, работающие под управлением Windows Server 2012.

4. На странице Выбор ролей сервера (Server Roles) выберите роль Файловые службы и службы хранилища (File And Storage Services). Если для установки роли требуются дополнительные компоненты, будет отображено дополнительное диалоговое окно. Нажмите кнопку Добавить компоненты (Add Features) для добавления необходимых компонентов в инсталляцию сервера. Нажмите кнопку Далее для продолжения.

   Краткое описание каждой службы роли приведено в табл. 1.1. Чтобы разрешить взаимодействие с UNIX, выберите Сервер для NFS (Server for NFS).
5. На странице Выбор компонентов (Features) выберите один или несколько компонентов для установки. Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, будет отображено дополнительное диалоговое окно. Нажмите кнопку Добавить компоненты для закрытия этого окна и установки требуемых компонентов на сервер. По окончанию выбора компонентов нажмите кнопку Далее.
6. На странице Подтверждение установки компонентов (Confirm) щелкните по ссылке Экспорт параметров конфигурации (Export Configuration Settings) для создания отчета установки, который можно просмотреть в Internet Explorer.
7. Если сервер, на котором необходимо установить роли или компоненты, не обладает всеми необходимыми двоичными файлами, сервер получит их через Windows Update (по умолчанию) или из местоположения, указанного групповой политикой.

   Также можно указать альтернативный источник для файлов. Чтобы сделать это, щелкните по ссылке Указать альтернативный исходный путь (Specify An Alternate Source Path), в появившемся окне укажите альтернативный путь и нажмите кнопку OK. Например, если образ Windows смонтирован и доступен на локальном сервере, можно ввести альтернативный путь в виде c:\mountdir\windows\winsxs. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer20120\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\ WinServer2-12\install.wim:4.
8. После просмотра опций установки (и их сохранения при необходимости) нажмите кнопку Установить (Install) для начала процесса установки. Страница Ход установки (Installation Progress) позволяет отслеживать процесс инсталляции. Если окно мастера было закрыто, щелкните по значку Уведомления (Notifications) в окне Диспетчер серверов, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.

9. Когда мастер закончит установку выбранных ролей и компонентов, страница Ход установки сообщит об этом. Просмотрите подробности установки и убедитесь, что все фазы инсталляции завершены успешно. Обратите внимание на любые действия, которые могут потребоваться для завершения установки, например перезагрузка сервера или осуществление дополнительных инсталляционных задач. Если какая-либо часть установки не увенчалась успехом, запомните причину сбоя. Просмотрите записи в окне Диспетчер серверов, чтобы понять суть проблемы, и примите соответствующие корректирующие действия.

Если роль Файловые службы уже установлена на сервере и необходимо установить дополнительные службы для файлового сервера, добавить службы роли на сервер можно аналогичным способом.

Добавление жестких дисков

Прежде чем сделать жесткий диск доступным для пользователей, необходимо настроить его и определить, как он будет использоваться. Windows Server 2012 позволяет настроить жесткие диски несколькими способами. Выбранный метод зависит, прежде всего, от типа данных, с которыми приходится работать, и от нужд сетевой среды. Для общих пользовательских данных, хранящихся на рабочих станциях, можно настроить отдельные диски как автономные устройства хранения. В этом случае пользовательские данные хранятся на жестком диске рабочей станции, где к ним осуществляется локальный доступ.

Несмотря на то, что хранить данные на единственном диске удобно, это не самый надежный способ хранения данных. Для улучшения надежности и производительности необходимо заставить работать вместе набор дисков. ОС Windows Server 2012 поддерживает наборы дисков и массивы с использованием технологии RAID (Redundant Array of Independent Disks, избыточный массив независимых жестких дисков), встроенной в операционную систему.

Физические диски

Используются ли отдельные диски или целые наборы дисков, нам нужны физические диски. Физические диски — устройства, которые используются для хранения данных. Объем записанных на диск данных зависит от его размера и от того, используется ли сжатие. ОС Windows Server 2012 поддерживает диски стандартного и усовершенствованного форматов.

У дисков стандартного формата размер физического сектора равен 512 байтов, и такие диски также называются дисками 512b. Физический размер сектора дисков усовершенствованного формата — 4096 байтов, и они также называются дисками 512e. Формат 512e представляет качественный сдвиг в области технологий хранения больших, многотерабайтных объемов данных на жестких дисках.

Диски выполняют обновление физических носителей в зависимости от размера сектора. Диски 512b работают с 512 байтами данных за один раз; а диски 512e — с 4096 байтами данных за один раз. Для определения размера сектора нужно использовать утилиту командной строки Fsutil:

Fsutil fsinfo ntfsinfo DriveDesignator
Здесь DriveDesignator — буква диска, информацию о котором нужно получить:
Fsutil fsinfo sectorinfo c:
Наличие сектора большего физического размера позволяет перейти на новый уровень пределов физической емкости. При ограничении записи только 512 байтами за раз жесткие диски должны выполнить несколько операций записи, чтобы завершить запись. Для лучшей производительности нужно обновить приложения, чтобы обеспечить запись и чтение данных на новом уровне (4096 байтов).
ОС Windows Server 2012 поддерживает много разных интерфейсов дисков, в том числе:

1. Small Computer System Interface (SCSI);
2. Parallel ATA (PATA), также известен как IDE;
3. Serial ATA (SATA).

Термины SCSI, IDE и SATA означают тип интерфейса жестких дисков, который используется для связи с контроллером диска. SCSI-диски используют SCSI-контроллеры, IDEдиски — IDE-контроллеры и т. д.
SCSI — это один из наиболее часто используемых интерфейсов, здесь есть множество дизайнов шины и типов интерфейса. Параллельный SCSI (так же называемый как SPI), хоть и популярный, но уступает последовательному SCSI (Serial Attached SCSI, SAS). Интерфейс iSCSI (Internet Small Computer System Interface) базируется на архитектурной модели SCSI, но для транспорта использует TCP/IP, а не обычную физическую реализацию.
Интерфейс SATA был разработан для замены IDE. Диски SATA все более и более популярны как дешевая альтернатива SCSI. Наиболее распространены интерфейсы SATA II и SATA III, они могут передавать данные со скоростью 3 и 6 Гбит/с соответственно. ESATA (так же известный как внешний SATA, external SATA) предназначен для подключения внешних жестких дисков.
Операционная система Windows Server 2012 содержит расширения для улучшенной поддержки SATA-дисков, уменьшающие несогласованность метаданных и позволяющие дискам более эффективно кэшировать данные. Улучшенное кэширование помогает защищать кэшированные данные в случае неожиданных потерь питания.
При установке нового сервера нужно уделить пристальное внимание настройке диска. Начните с выбора дисков или систем хранения, предоставляющих надлежащий уровень производительности. Действительно, среди различных спецификаций диска есть существенные различия в скорости и производительности.
Нужно рассматривать не только емкость диска, но так же и следующие его параметры:

1. скорость вращения — мера того, как быстро вращается диск;
2. среднее время поиска — показывает, сколько времени нужно для поиска между дорожками диска во время последовательных операций ввода-вывода. Вообще говоря, при сравнении дисков, соответствующих той же спецификации, что и Ultra640 SCSI или SATA III, чем выше скорость

вращения (измеряется в тысячах вращений в минуту — rotations per minute, RPM) и ниже среднее время поиска (измеряется в миллисекундах, мс), тем лучше. Например, диск со скоростью вращения 15 000 RPM на 45—50% быстрее среднего диска на 10 000 RPM при прочих равных условиях. Диск со временем поиска 3,5 мс обеспечивает лучшее время отклика на 25—30% по сравнению с диском со временем поиска 4,7 мс.

3. Другие факторы, на которые нужно обратить внимание:
4. максимальная устойчивая скорость передачи данных показывает, сколько данных диск может передавать постоянно;
5. среднее время наработки на отказ (mean time to failure, MTTF) — через сколько часов работы следует ожидать отказ диска, перед тем как он перестанет работать;
6. нерабочие температуры — при каких температурах происходит сбой диска.

У большинства дисков сопоставимого качества скорость передачи данных и MTFF подобны. Так, если сравнивать диски SCSI Ultra320 со скоростью вращения 15 000 об/мин различных производителей, у многих дисков будут подобные скорости передачи и MTTF. Например, у Maxtor Atlas 15K II максимальная устойчивая скорость передачи данных равна 98 Мбайт/с. У Seagate Cheetah 15K.4 максимальная устойчивая скорость равна 96 Мбайт/с. У обеих моделей MTTF равен 1,4 млн часов. Скорости передачи данных могут быть также выражены в гигабитах в секунду (Гбит/с). Уровень 1,5 Гбит/с эквивалентен скорости передачи данных 187,5 Мбайт/с, а 3,0 Гбит/с эквивалентно 375 Мбайт/с. Иногда указывается максимальная скорость внешней передачи (на спецификацию, к которой относится диск) и средняя длительная скорость передачи. Средняя скорость длительной передачи — наиболее важный фактор. У Seagate Barracuda 7200 SATA II скорость вращения 7200 об/мин, а средняя скорость длительной передачи — 58 Мбайт/с. Со средним временем поиска в 8,5 мс и MTTF 1 млн часов диск выделяется среди других дисков SATA II со скоростью 7200 об/мин. Однако у большинства дисков SCSI Ultra320 производительность выше, особенно в многопользовательских операциях чтения/записи.

Нельзя путать единицы измерения Мбайт/с и Мбит/с. Мбайт/с — это мегабайт в секунду, Мбит/с — мегабит в секунду. Поскольку в байте 8 бит, частота передачи 100 Мбайт/с эквивалентна частота 800 Мбит/с. В случае с SATA максимальная частота передачи данных обычно около 150 Мбайт/с или 300 Мбит/с. При использовании PATA/IDE максимальная частота передачи данных обычно около 100 Мбайт/с.

Температура — другой важный фактор, на который нужно обратить внимание при выборе диска, но его принимают во внимание немного администраторов. Как правило, чем быстрее вращается диск, тем больше он греется. Это не всегда так, но при выборе диска нужно рассмотреть и фактор температуры. Например, диски со скоростью 15К более горячие, и необходимо убедиться, что температура тщательно контролируется. Для Maxtor Atlas 15K II и Seagate

Cheetah 15K.4 температура отказа составляет 70° С и выше (как и в случае с большинством других дисков).
Операционная система Windows Server 2012 поддерживает диски с аппаратным шифрованием (они также называются зашифрованными жесткими дисками). У зашифрованных жестких дисков есть встроенные процессоры, перемещающие функции шифрования с операционной системы на аппаратные средства, освобождая ресурсы операционной системы. ОС Windows Server 2012 будет использовать аппаратное шифрование с BitLocker, если это возможно. Другие средства защиты, доступные в Windows Server 2012, включают защищенную загрузку (Secure Boot) и разблокировку по сети (Network Unlock). Защищенная загрузка обеспечивает целостность начальной загрузки с проверкой настройки BCD (Boot Configuration Data) согласно настройкам профиля проверки TPM (Trusted Platform Module).
Разблокировка по сети может быть использована для автоматической разблокировки диска операционной системы на компьютерах, присоединенных к домену.

Подготовка физического диска для использования

После установки диска его необходимо настроить для использования. При этом осуществляется разбивка диска на разделы, создание файловых систем на этих разделах. Раздел — это секция физического диска, функционирующая как отдельная единица. После формирования раздела на нем нужно создать файловую систему.
На дисках используются разделы двух типов: главная загрузочная запись (Master Boot Record, MBR) и таблица разделов GUID (GUID partition table, GPT). MBR содержит таблицу разделов, которая описывает расположение разделов на диске. При использовании MBR
первый сектор на жестком диске содержит главную загрузочную запись, а файл двоичного кода называется главным загрузочным кодом, который используется для загрузки операционной системы. Этот сектор неделим и скрыт от просмотра для защиты системы.
При использовании MBR диски поддерживают тома до 4 Тбайт и используют один из двух типов разделов: первичный или расширенный. У каждого MBR-иска может быть до четырех первичных (основных) разделов или три первичных и один расширенный раздел. Первичные разделы — это разделы диска, к которым можно получить доступ непосредственно для файлового хранилища. После создания файловой системы первичный раздел станет доступным для пользователей. Получить прямой (непосредственный) доступ к расширенному разделу нельзя. Вместо этого в расширенном разделе создается один (или больше) логический диск, который используется для хранения файлов. Учитывая, что можно разделить расширенный раздел на логические диски, физический диск можно разделить больше, чем на четыре раздела.
Таблица разделов GPT была первоначально разработана для высокоэффективных компьютеров на базе процессора Itanium. GPT

рекомендуется использовать для дисков, больших 2 Тбайт на x86 и x64 или на любых дисках, установленных в компьютер на базе Itanium.
Основная разница между MBR и GPT — в способе хранения данных. В случае с GPT критические данные раздела хранятся на разных разделах, для улучшенной структурной целостности используются избыточные основные и резервные таблицы разделов. Также GPTдиски поддерживают тома до 18 Эбайт и целых 128 разделов. Несмотря на то, что у GPT и MBR есть базовые различия, большинство связанных с диском задач выполняется одинаково.
В дополнение к типу раздела у физических дисков есть еще один параметр — тип диска, который может быть либо базовым, либо динамическим, как будет показано далее. После установки типа раздела для физического диска можно отформатировать свободные области диска для создания логических дисков. Форматирование создает файловую систему на разделе. ОС Windows Server 2012 поддерживает следующие файловые системы:

1. FAT;
2. FAT32;
3. exFAT;
4. NTFS;
5. ReFS.

В случае с FAT число бит, используемых в таблице размещения файлов, определяет используемый вариант FAT и максимальный размер тома. Файловая система FAT16, также известная как просто FAT, определяет, что ее таблица размещения файлов использует 16 битов.
Тома с размером 4 Гбайт или меньше форматируются как FAT16.
В случае с FAT32 таблица размещения файлов использует 32 бита, и допускается создавать FAT32-тома с объемом 32 Гбайт или меньше посредством утилиты форматирования Windows. Хотя Windows может монтировать FAT32-тома большего размера, созданные сторонними утилитами, для томов размером больше 32 Гбайт необходимо использовать NTFS.
Файловая система Extended FAT (exFAT) — расширенная версия FAT. Технически, exFAT может называться FAT64 (и называется некоторыми пользователями). Файловая система exFAT определяет свои таблицы размещения файлов, используя 64 бита. Это позволяет exFAT преодолевать предел размера файла в 4 Гбайт и предел размера тома в 32 Гбайт, который был в FAT32. Файловая система exFAT поддерживает размеры кластера до 128 Кбайт для томов до 256 Тбайт.
У томов NTFS совсем другая структура и набор функций. Первая область тома — это загрузочный сектор, хранящий информацию о разметке диска и программу самозагрузки, которая выполняется при запуске и загружает операционную систему. Вместо таблицы размещения файлов, NTFS использует реляционную базу данных для хранения информации о файлах. Эту базу данных называют главной файловой таблицей (Main File Table, MFT).
MFT хранит файловую запись каждого файла и папки тома, информацию о томе и сведения о самой MFT. Файловая система NTFS предлагает много расширенных опций, в том числе поддержку шифрованной файловой системы

(Encrypting File System), сжатия, возможность создания отчетов экранирования и хранения файла, которые станут доступны при добавлении службы роли Диспетчер ресурсов файлового сервера (FSRM) как части роли
Файловые службы (File Services).
Файловая система ReFS (Resilient File System) — следующее поколение NTFS. Она остается совместимой с базовыми функциями NTFS при сокращении дополнительных функций, чтобы сфокусироваться на надежности. Это означает, что квоты дисков, файловая система с шифрованием, сжатие, отчеты экранирования и хранения файлов не доступны, но добавлены встроенные функции надежности.
Одна из основных функций обеспечения надежности файловой системы ReFS — это сканер целостности данных. Он обеспечивает превентивную идентификацию ошибок, изоляцию и коррекцию. Если сканер обнаруживает повреждение данных, используется процесс восстановления, чтобы локализировать область повреждения и выполнить автоматическую онлайн-коррекцию. С помощью процесса автоматического спасения поврежденные области, которые не могут быть восстановлены, например из-за сбойных блоков на физическом диске, удаляются из тома, чтобы они больше не могли оказать негативное влияние на хорошие данные. Поскольку ReFS использует автоматическую проверку и процесс восстановления, ReFS не нуждается в какой-либо дополнительной проверке (следовательно, нет никакой утилиты вроде Check Disk для ReFS).
При работе с файловыми службами и службами хранилища можно группировать доступные физические диски в пулы хранилищ, поэтому допускается создание виртуальных дисков из доступной емкости. Каждый созданный виртуальный диск является пространством хранения (storage spaces). Поскольку только NTFS поддерживает пространства хранения, помните об этом при форматировании тома на файловых серверах.

Использование оснастки *Управление дисками*

Оснастка консоли управления Microsoft (MMC) Управление дисками (Disk Management) используется для настройки дисков. Оснастка Управление дисками позволяет легко работать как с внутренними, так и с внешними дисками на локальной или удаленной системе.
Оснастка Управление дисками является частью консоли Управление компьютером (Computer Management). Данная оснастка может быть добавлена в пользовательскую консоль MMC. В оснастке Управление компьютером можно получить доступ к оснастке Управление дисками (Disk Management), развернув узел Запоминающие устройства (Storage) и затем выбрав узел Управление дисками (Disk Management).
Оснастка обладает тремя представлениями: Список дисков (Disk List), Список томов (Volume List) и Графическое представление (Graphical View). На удаленных системах функциональность оснастки ограничена: разрешается просмотреть подробную информацию о диске, изменить буквы дисков и пути, конвертировать типы дисков. Для съемных дисков удаленно также можно

извлечь носитель. Для осуществления расширенной манипуляции с удаленными дисками необходимо использовать утилиту командной строки DiskPart.

Перед тем как начать работу с оснасткой Управление дисками, необходимо знать несколько вещей. Если создается раздел, но не форматируется, то он отмечается как Свободное пространство (Free space). Если часть диска не назначается разделу, эта секция диска помечается как Не распределена (Unallocated).

В верхней части окна используется представление Список томов, а в нижней части — Графическое представление. Изменение представления верхней или нижней панели осуществляется следующим образом:

1. для изменения представления верхней панели выберите команды меню Вид | Верх (View | Top), а затем — тип представления;
2. для изменения представления нижней панели выберите команды меню Вид | Низ (View | Bottom), а затем — тип представления;
3. чтобы скрыть нижнюю панель, выберите команды меню Вид | Низ | Скрыть (View | Bottom | Hidden).
4. Базовый — стандартный тип жесткого диска (фиксированный), используемый в предыдущих версиях Windows. Базовые диски делятся на разделы и являются исходным типом диска для ранних версий Windows.
5. Динамический — расширенный тип жесткого диска (фиксированный) для Windows Server 2012, который можно обновлять без необходимости перезапуска системы (в большинстве случаев). Динамические диски делятся на тома.
6. Сменный — стандартный тип диска, ассоциируемый со сменными устройствами хранения данных.
7. Виртуальный — тип виртуального жесткого диска (Virtual Hard Disk, VHD), используемый в виртуализации. Компьютеры могут использовать VHD так же, как они используют обычные жесткие диски, могут даже загружаться с VHD.

Для получения информации о диске щелкните правой кнопкой мыши на нем и выберите команду Свойства. Откроется одноименное диалоговое окно.

Если настроено удаленное управление через диспетчер серверов и MMC, можно использовать оснастку Управление дисками, чтобы управлять дисками удаленного компьютера. Имейте в виду, что в этом случае функции управления удаленными дисками отличаются от функций управления локальными дисками. Можно выполнить следующие задачи:

1. просмотреть ограниченные свойства диска, но не свойства тома. При просмотре свойств диска доступны только вкладки Общие и Тома, но не доступны свойства диска;
2. изменить букву диска и путь монтирования;
3. отформатировать, уменьшить или расширить том. Есть возможность добавить и настроить параметры зеркальных, составных и чередующихся томов;
4. удалить том (кроме системных и загрузочных томов);

5. создать, присоединить и отключить виртуальный диск. При создании и присоединении VHD необходимо ввести полный путь к файлу, нет возможности выбрать vhd-файл (использовать кнопку Обзор).

Некоторые задачи, выполняемые с дисками и томами, основаны на службах Plug and Play и Remote Registry.

Сменные устройства хранения данных

Сменные устройства хранения данных могут быть отформатированы как NTFS, FAT, FAT32 или exFAT. Внешние устройства хранения данных подключают к компьютеру вместо того, чтобы устанавливать их внутри компьютера. Это делает использование сменных устройств проще и установку быстрее по сравнению с большинством фиксированных дисков. Большинство внешних устройств хранения данных подключаются либо по USB, либо с помощью интерфейса FireWire. При работе с USB или FireWire скорость передачи и общая производительность устройства с точки зрения пользователя зависит, прежде всего, от поддерживаемой версии. В настоящее время существует несколько версий USB и FireWire.

USB 2.0 является промышленным стандартом, пока мир переходит на USB 3.0. Устройства USB 2.0 могут быть отмечены как полноскоростные (full speed) — до 12 Мбит/с или как высокоскоростные (high speed) — до 480 Мбит/с. Несмотря на то, что USB 2.0 может передавать данные с максимальной скоростью до 480 Мбит/с, устойчивая скорость передачи данных обычно составляет 10—30 Мбит/с. Фактическая поддерживаемая скорость передачи зависит от многих факторов, в том числе от типа устройства, типа передаваемых данных и скорости компьютера. У каждого USB-контроллера на компьютере есть фиксированная пропускная способность, которую должны совместно использовать все подключенные устройства. Скорость передачи данных значительно медленнее, если USB-порт компьютера более ранней версии, чем поддерживается устройством. Например, если устройство USB 2.0 подключается к порту USB 1.0 или наоборот, устройство будет работать со скоростью USB 1.0, что значительно меньше скорости USB 2.0.

Порты USB 1.0, 1.1 и 2.0 выглядят одинаково. Однако у большинства портов USB 3.0 есть специальная окраска, чтобы отличать их от других портов. Лучший способ определить тип портов USB — обратиться к документации, которая поставляется с компьютером. У более новых мониторов есть порты USB 2.0, к которым также можно подключить устройства. При подключении USB-устройства к монитору, монитор действует как USB-хаб. Как и в случае с любым другим USB-хабом, все устройства, подключенные к хабу, совместно используют одну и ту же пропускную способность, при этом общая пропускная способность определена скоростью USB-входа, к которому подключен хаб на компьютере.

Стандарт FireWire (IEEE 1394) — высокопроизводительный стандарт подключения, использующий одноранговую архитектуру, в которой периферийные устройства согласовывают конфликты при обращении к шине для определения, какое устройство может лучше всего управлять передачей

данных. Как и в случае с USB, в настоящее время используются несколько версий FireWire. Максимальная скорость длительной передачи данных у FireWire 400 (У IEEE 1394a) составляет до 400 Мбит/с. IEEE 1394b позволяет передавать данные со скоростью 400 Мбит/с (S400), 800 Мбит/с (S800) и 1600 Мбит/с (S1600). Подобно USB, при подключении устройства IEEE 1394b к порту IEEE 1394a, устройство будет работать в режиме значительного снижения скорости — до уровня FireWire 400.

Подобно USB-портам, скорость длительной передачи для портов IEEE 1394a и IEEE 1394b будет значительно меньше, чем максимально возможная. Формы портов и кабелей IEEE 1394a и IEEE 1394b отличаются, что упрощает их идентификацию. У кабелей FireWire 400 без питания шины есть четыре контакта и четыре соединителя. У кабелей FireWire 400 с питанием шины — шесть контактов и шесть соединителей. У кабелей FireWire 800 и FireWire 1600 всегда есть питание шины, и они имеют 9 контактов и 9 соединителей.

Можно также использовать внешний SATA (eSATA), который доступен на более новых компьютерах. eSATA — это соединение ультравысокой производительности для передачи данных на устройство хранения данных и с него. eSATA работает на скорости до 3 Гбит/с. Добавить поддержку устройств eSATA можно с помощью установки контроллера eSATA.

При покупке внешнего устройства для компьютера нужно знать, какой интерфейс оно поддерживает. В некоторых случаях устройство поддерживает несколько интерфейсов, например USB 3.0 и eSATA. Устройство с несколькими интерфейсами предоставляет больше возможностей. Работа со сменными дисками подобна работе с фиксированными дисками:

1. Щелкните правой кнопкой мыши по сменному носителю и выберите команду Открыть (Open) или Проводник (Explore), чтобы исследовать содержимое диска в Проводнике.
2. Щелкните правой кнопкой мыши по сменному диску и выберите команду Форматировать (Format), чтобы отформатировать сменный диск (см. разд. "Форматирование разделов" далее в этой главе). На сменных дисках, как правило, создается один раздел.
3. Щелкните правой кнопкой мыши по сменному диску и выберите команду Свойства для просмотра или установки его свойств. На вкладке Общие окна Свойства можно установить метку тома.

При работе со сменными дисками есть возможность настроить представления диска и папки. Для этого щелкните на диске и выберите команду Свойства, а затем перейдите на вкладку Настройка (Customize). Далее нужно указать тип папки по умолчанию. Например, можно установить тип папки Документы (Documents) или Изображения (Pictures). Также есть возможность установить изображение и значок папки.

Сменные диски поддерживают общий доступ по сети. Настройка общего доступа к сменному диску производится аналогично настройке общего доступа для обычного диска. Настраиваются разрешения доступа, опции кэширования для использования файлов вне сети (оффлайн), ограничивается число одновременных пользователей. Предоставить общий доступ можно как ко

всему сменному диску, так и к отдельной папке, хранящейся на таком диске. При необходимости для одного ресурса можно создать несколько экземпляров общего ресурса.
Съемные диски отличаются от стандартных общих NTFS-ресурсов тем, что у них не обязательно есть базовая архитектура безопасности. При использовании файловой системы exFAT, FAT или FAT32 у папок и файлов, хранящихся на этом диске, нет никаких прав доступа или других функций, кроме атрибутов "только чтение" или "скрытый", доступных для установки.

Установка и проверка нового диска

Горячая замена (hot swap) — это функция, позволяющая демонтировать внутренние устройства, не отключая при этом компьютер. Как правило, внутренние диски, поддерживающие горячую замену, устанавливаются и извлекаются с передней части компьютера. Если компьютер поддерживает горячую замену внутренних дисков, разрешается устанавливать новые диски без необходимости выключения компьютера. После установки нового диска откройте оснастку Управление дисками и в меню Действие (Action) выберите команду Повторить проверку дисков (Rescan Disks). Новые найденные диски будут добавлены, а их тип надлежащим образом распознан. Если добавленный диск недоступен, перезагрузите компьютер.
Если компьютер не поддерживает горячую замену внутренних дисков, необходимо выключить компьютер и затем установить новые диски. Далее нужно просканировать диски, как было описано ранее. Новые диски, которые еще не были инициализированы, не имеют меток, и оснастка Управление дисками отобразит окно Инициализация дисков (Initialize Disk), как только обнаружит такие диски. Для инициализации дисков выполните следующие действия:

1. Каждый установленный вами диск нуждается в инициализации. Выберите установленный диск или диски.
2. Диски могут использовать тип разделов MBR или GPT. Выберите тип раздела для диска или дисков, которые необходимо инициализировать.
3. Нажмите кнопку OK. Если выбрана инициализация дисков, Windows запишет дисковую подпись на диски и инициализирует диски как диски базового типа.

Если хотите использовать окно Инициализация дисков, закройте его и используйте оснастку Управление дисками для просмотра и работы с диском. В представлении Список дисков неинициализированные диски отмечаются красной стрелкой вниз, при этом состояние диска будет указано как Не проинициализирован (Not Initialized), а тип диска — Нет данных (Unknown). Затем щелкните правой кнопкой мыши по значку диска и выберите команду В сети (Online). Снова щелкните правой кнопкой мыши по значку диска и выберите команду Инициализировать диск (Initialize Disk). Теперь можно инициализировать диск, как было показано ранее.

Статус диска

Знание статуса диска полезно при установке новых дисков или разрешении проблем с дисками. Оснастка Управление дисками показывает состояние диска в графическом представлении и в представлении Список томов. В табл. 1.2 представлены общие значения состояния.

Таблица 1.2. Общие значения состояния дисков

Состояние	Описание	Резолюция
В сети (Online) У диска нет никаких видимых проблем.	Нормальное состояние диска. Означает, что диск доступен и с ним нет никаких проблем. Это состояние показывают базовые и динамические диски	Не нужно предпринимать каких-либо корректирующих действий
В сети (Ошибки) (Online (Errors))	На динамическом диске были обнаружены ошибки вводавывода	Можно попытаться исправить временные ошибки, щелкнув правой кнопкой мыши по диску и выбрав команду Реактивировать диск (Reactivate Disk). Если это не поможет, у диска, вероятно, есть физические повреждения или необходимо запустить полную проверку диска
Вне сети (Offline)	Диск недоступен и может быть поврежден или временно недоступен. Если имя диска изменено на Отсутствует (Missing), диск больше может быть идентифицирован в системе	Проверьте наличие проблем с диском, с его контроллером и кабелями. Убедитесь, что к диску подключено питание и он подключен правильно (имеется в виду интерфейсный кабель). Используйте команду Рективировать диск, чтобы вернуть диск в состояние В сети (если возможно)
Чужой (Foreign)	Диск был перемещен в компьютер, но не был импортирован для использования.	Щелкните правой кнопкой мыши по диску и выберите команду Импорт чужих дисков

	Отказавший диск может иногда выводиться как Чужой	(Import Foreign Disks) для добавления диска в систему
Не читается (Unreadable)	Диск в данный момент недоступен, это может произойти, когда диски повторно сканируются. Такое состояние отображают и базовые, и динамические диски	Это состояние отображается на FireWire/USB-кардридерах, если карта памяти не форматирована или неверно форматирована. Также это состояние устанавливается после извлечения карты памяти из кардридера. В противном случае, если диски не сканируются, диск может быть поврежден или иметь ошибки ввода-вывода. Щелкните правой кнопкой мыши по диску и выберите команду Повторить проверку дисков, чтобы попытаться исправить проблему. Также можно перезагрузить систему
Неопознан (Unrecognized)	Диск неизвестного типа и не может использоваться в системе. Это состояние могут отображать не-Windows-диски	Если диск относится к другой операционной системе, ничего не делайте. Нельзя использовать этот диск на компьютере, поэтому попытайтесь использовать другой диск
Не проинициализирован (Not Initialized)	У диска нет верной подписи. Это состояние может отображать диск с не-Windows файловой системой	Если диск относится к другой операционной системе, ничего не делайте. Этот диск нельзя использовать на компьютере. Для подготовки диска с целью использования в Windows Server 2012

		щелкните правой кнопкой мыши по нему и выберите команду Инициализировать диск
Нет носителя (No Media)	В DVD или другой съемный дисковод не вставлен носитель или же носитель был удален. Это состояние могут отображать только DVD и другие типы сменных дисков	Чтобы перевести диск в состояние В сети, вставьте DVD или сменный диск. С кардридерами (FireWire или USB) это состояние обычно (но не всегда) отображается, когда карта памяти извлечена

Работа с базовыми, динамическими и виртуальными дисками

Операционная система Windows Server 2012 поддерживает базовые, дисковые и виртуальные конфигурации дисков. В этом разделе обсуждаются техники работы с диском каждого типа конфигурации.

Невозможно использовать динамические диски на портативных компьютерах или со сменными носителями.

Использование базовых и динамических дисков

Обычно разделы диска Windows Server 2012 инициализируются как базовые диски. Невозможно создать новые отказоустойчивые наборы дисков, используя базовый тип диска. Необходимо конвертировать базовые диски в динамические и затем создать тома, использующие чередование, зеркалирование или чередование с контролем четности (RAID 0, 1 и 5 соответственно). Отказоустойчивость и возможность смены дисков без необходимости перезапуска компьютера — ключевые возможности, которые отличают динамические диски от базовых. Другие функции дисков зависят от его форматирования.

На одном и том же компьютере могут использоваться базовые и динамические диски. Однако набор томов должен использовать однотипные диски и однотипные разделы. Например, если необходимо зеркалировать диски C: и D:, оба диска должны быть динамическими и использовать одинаковый тип разделов, который может быть или MBR, или GPT.

Обратите внимание на то, что оснастка Управление дисками позволяет выполнять много задач конфигурации диска независимо от используемого диска. Преимущество в том, что во время процесса конфигурации оснастка Управление дисками конвертирует диски в динамический тип. Чтобы узнать, как конвертировать диск из базового в динамический, см. разд. "Изменение типа диска" далее в этой главе.

Для базовых и динамических дисков можно осуществлять различные задачи конфигурации диска. Над базовыми дисками доступны следующие действия:

1. форматировать разделы и помечать их как активные;

2. создавать и удалять первичные и расширенные разделы;
3. создавать и удалять логические диски на расширенных разделах.

Операции над динамическими дисками:

1. создание и удаление простых, чередующихся, составных (spanned), зеркальных томов и томов RAID 5;
2. удаление зеркала из зеркального тома;
3. расширение простых или составных томов;
4. разделение тома на два тома;
5. восстановление зеркальных томов или томов RAID 5;
6. реактивирование отсутствующих дисков или дисков с состоянием "вне сети";
7. преобразование обратно к базовому диску (требует удаления томов и восстановления их из резервной копии).

Над дисками любого типа можно выполнить следующие операции:

1. просматривать свойства дисков, разделов и томов;
2. назначать буквы дискам;
3. настраивать безопасность и общий доступ к диску.

Особенности базовых и динамических дисков

При работе с основными и динамическими дисками нужно иметь в виду пять специальных типов секций диска.

1. Активен (Active) — активный раздел или том. Это секция диска, использующаяся для кэширования и запуска системы. Некоторые устройства со сменным носителем могут быть выведены как устройства с активным разделом.
2. Загрузка (Boot) — загрузочный раздел или том, содержащий операционную систему и ее вспомогательные файлы. Разделы Система и Загрузка могут быть одним и тем же разделом.
3. Аварийный дамп памяти (Crash dump) — раздел, на который компьютер пытается записать файлы дампа в случае отказа системы. По умолчанию файлы дампа записываются в папку %SystemRoot%, но они могут быть расположены на любом разделе или томе.
4. Файл подкачки (Page file) — раздел, содержащий файл подкачки, используется операционной системой. Поскольку компьютер может использовать для подкачки несколько дисков, в зависимости от настройки виртуальной памяти, у компьютера может быть несколько разделов/томов этого типа.
5. Система (System) — системный раздел или том содержит аппаратно-зависимые файлы, необходимые для загрузки операционной системы. Системный раздел не может быть частью составного или чередующегося тома.

Чтобы пометить раздел как активный, используйте оснастку Управление дисками. В этой оснастке щелкните правой кнопкой мыши по базовому разделу, который нужно сделать активным, и выберите команду Сделать раздел активным. Динамические диски нельзя пометить как активные. При

конвертировании базового диска, содержащего активный раздел, в динамический диск этот раздел автоматически станет обычным томом.

Изменение типа диска

Базовые диски разработаны для использования с предыдущими версиями Windows. Динамические диски позволят получить все преимущества последних функций Windows. Только компьютеры, работающие под управлением Windows 2000 и более поздних версий Windows, могут использовать динамические диски. Однако динамические диски могут использоваться и с другими операционными системами, например, в UNIX. Чтобы сделать это, необходимо создать отдельный том для не-Windows операционной системы. На портативных компьютерах использовать динамические диски невозможно.

Операционная система Windows Server 2012 предоставляет средства, необходимые для конвертирования базового диска в динамический и обратно в базовый. При конвертировании диска в динамический разделы автоматически становятся томами надлежащего типа. Обратно преобразовать эти тома в разделы невозможно. Вместо этого необходимо удалить тома на динамическом диске, а затем преобразовать диск в базовый. Удаление томов уничтожает всю информацию на диске.

Конвертирование базового диска в динамический

Перед конвертированием базового диска в динамический нужно убедиться, что больше не понадобится загружать компьютер в старых версиях Windows. Только компьютеры под управлением Windows 2000 и более поздних версий могут использовать динамические диски.

В случае с MBR-дисками также нужно убедиться, что диск имеет хотя бы 1 Мбайт свободного места в конце диска. Хотя оснастка Управление дисками резервирует это пространство при создании разделов и томов, средства управления дисками других операционных систем могут этого не делать. Без свободного пространства в конце диска конвертировать диск не получится.

В случае с GPT нужно иметь непрерывные, распознанные разделы данных. Если GPT-диск содержит разделы, которые Windows не распознала, например, созданные другой операционной системой, невозможно конвертировать этот диск в динамический. Следующее верно для диска любого типа.

1. Должно быть как минимум 1 Мбайт свободного места в конце диска. Оснастка Управление дисками резервирует это пространство автоматически, средства управления дисками других операционных систем могут этого не делать.
2. Невозможно использовать динамические диски на портативных компьютерах или на сменных носителях. Нельзя настроить эти диски только как базовые с первичными разделами.
3. Невозможно конвертировать диск, если он содержит несколько инсталляций операционной системы Windows, если это так и сделать, можно будет запустить только Windows Server 2012.

Для конвертирования базового диска в динамический выполните следующие действия:

1. В оснастке Управление дисками щелкните правой кнопкой мыши на базовом диске, который необходимо конвертировать (без разницы, какой режим используется — Список дисков или Графическое представление). Затем выберите команду Преобразовать в динамический диск (Convert To Dynamic Disk).
2. В окне Преобразование в динамические диски (Convert To Dynamic Disk) отметьте флажки напротив дисков, которые необходимо конвертировать. При преобразовании составного, чередующегося, зеркалируемого или RAID 5 тома убедитесь, что выбраны все базовые диски в этом наборе. Необходимо конвертировать набор дисков вместе. Нажмите кнопку OK для продолжения. Будет отображено окно Диски для преобразования (Disks To Convert).
3. Окно Диски для преобразования показывает диски, которые будут конвертированы. Здесь имеются следующие кнопки и колонки:
   - Имя (Name) — номер диска;
   - Оглавление диска (Disk Contents) — тип и состояние разделов, например, загрузочный раздел, активный раздел или используемый;
   - Будет преобразован (Will Convert) — будет ли диск преобразован. Если диск не соответствует критериям, он не будет преобразован, и нужно внести корректирующие действия, описанные ранее;
   - Сведения (Details) — тома на выбранном диске;
   - Преобразовать (Convert) — начинает преобразование.
4. Для начала преобразования нажмите кнопку Преобразовать. Оснастка Управление дисками предупредит, что после завершения преобразования будет невозможно загрузить предыдущие версии Windows с томов на выбранных дисках. Нажмите кнопку Да для продолжения.
5. Оснастка Управление дисками перезагрузит компьютер, если выбранный диск содержит загрузочный раздел, системный раздел или используется.

Преобразование динамического диска обратно в базовый

Перед преобразованием динамического диска в базовый необходимо удалить все динамические тома на этом диске. После этого щелкните правой кнопкой мыши на диске и выберите команду Преобразовать в базовый диск (Convert To Basic Disk). Это действие изменит тип диска на базовый. Затем можно создать новые разделы и логические диски.

Повторная активация диска

Если состояние динамического диска — В сети (ошибки) или Вне сети, повторная активация диска часто помогает решить проблему. Реактивировать диск можно так:

1. В оснастке Управление дисками щелкните правой кнопкой мыши по динамическому диску и выберите команду Реактивировать диск.

2. Если состояние диска не изменилось, перезагрузите компьютер. Если это не помогло решить проблему, проверьте сам диск, его контроллер и кабели. Также убедитесь, что диск правильно подключен и к нему поступает питание.

Повторная проверка дисков

Повторная проверка всех дисков в системе обновляет информацию о дисках на компьютерах. Повторная проверка иногда помогает решить проблему с дисками со статусом Не читается. Пересканировать диски можно с помощью команды Повторить проверку дисков (Rescan Disks), выбранной из меню Действие оснастки Управление дисками.

Перемещение динамического диска в новую систему

Важное преимущество динамических дисков над базовыми заключается в том, что такие диски можно легко переместить с одного компьютера на другой. Например, если после установки компьютера обнаружится, что на этом компьютере не нужен дополнительный жесткий диск, можно переместить его в другой компьютер, где он будет использоваться рациональнее.

Операционная система Windows Server 2012 значительно упрощает задачу перемещения дисков в новую систему. Перед перемещением дисков необходимо выполнить следующие действия:

1. Откройте оснастку Управление дисками в системе, где в данный момент установлены динамические диски. Проверьте состояние дисков и убедитесь, что все они находятся в состоянии Исправен (Healthy). Если состояние отличается от Исправен, нужно исправить все ошибки перед перемещением дисков.

Диски с технологией BitLocker Drive Encryption не могут быть перемещены этим методом. Шифрование BitLocker Drive Encryption изолирует любое оффлайн-вмешательство в диск, в результате диск будет недоступен, пока администратор не разблокирует его.

2. Проверьте подсистемы жестких дисков исходного компьютера и компьютера, на который нужно перенести диски. Оба компьютера должны иметь одинаковые подсистемы. Если это не так, идентификатор Plug and Play системного диска исходного компьютера не совпадет с тем, что ожидает компьютер-назначение. В результате целевой компьютер не сможет загрузить правильные диски, и попытка загрузки не удастся.
3. Проверьте, являются ли динамические диски, которые необходимо переместить, частью составного, расширенного и чередующегося набора. Если это так, то нужно переместить весь набор вместе. При перемещении только части набора необходимо знать о последствиях. Для составных, расширенных или чередующихся томов перемещение только части набора сделает все связанные тома недоступными, как на исходном компьютере, так и на компьютере, куда перемещается диск.

После выполнения предыдущих, подготовительных, действий нужно выполнить эти действия:

1. На исходном компьютере запустите оснастку Управление компьютером. Затем на левой панели выберите Диспетчер устройств (Device Manager). В списке устройств разверните узел Дисковые устройства (Disk Drives). Будет отображен список всех физических дисков компьютера. Щелкните на диске, который необходимо переместить, и выберите команду Удалить (Uninstall). Если вы не уверены, какие диски нужно удалить, щелкните правой кнопкой мыши по каждому диску и выберите команду Свойства.
1. В окне Свойства перейдите на вкладку Тома (Volumes) и нажмите кнопку Заполнить (Populate). После этого будут отображены тома на выбранном диске.
2. Далее на исходном компьютере выберите узел Управление дисками в оснастке Управление компьютером. Если диск или диски, которые необходимо переместить, все еще перечислены в списке, щелкните правой кнопкой мыши на каждом из них и выберите команду Изъять диск (Remove Disk).
3. После выполнения этих процедур можно переместить динамические диски. Если диски являются дисками горячей замены и горячая замена поддерживается обоими компьютерами, извлеките диски из исходного компьютера и поместите их в целевой компьютер.
4. В противном случае выключите оба компьютера, извлеките диски из исходного компьютера и затем установите их в компьютер назначения. По окончанию перезагрузите компьютеры.
5. На целевом компьютере запустите оснастку Управление дисками и выберите команду Повторить проверку дисков (Rescan Disks) в меню Действие. Когда оснастка Управление дисками завершит сканирование дисков, щелкните правой кнопкой мыши на каждом диске, помеченном как Чужой, и выберите команду Импорт чужих дисков.

В большинстве случаев тома на динамических дисках должны сохранить буквы дисков, которые им были присвоены на исходном компьютере. Однако если буква диска уже используется на целевом компьютере, том получит следующую доступную букву диска. Если у динамического тома ранее не было буквы диска, он не получит букву после перемещения в целевой компьютер. Дополнительно, если автомонтирование выключено, тома автоматически не будут смонтированы, и администратору нужно смонтировать их вручную и присвоить им буквы дисков.

Управление виртуальными дисками

Оснастка Управление дисками позволяет создавать, присоединять и отсоединять виртуальные жесткие диски. Создать виртуальный диск можно командой Действие | Создать виртуальный жесткий диск (Action | Create VHD). В окне Создать и присоединить виртуальный жесткий диск (Create And Attach Virtual Hard Disk) нажмите кнопку Обзор.

Используйте окно Просмотр файлов виртуального диска (Browse Virtual Disk Files) для выбора места, в котором будет создан vhd-файл виртуального диска, введите его имя и нажмите кнопку Сохранить (Save).

В поле Размер виртуального жесткого диска (Virtual Hard Disk Size) введите размер диска в МБ (MB), ГБ (GB) или ТБ (TB). Укажите, должен ли файл виртуального жесткого диска расширяться до максимального размера по мере записи данных на него или же место для файла виртуального жесткого диска будет выделено в полном объеме независимо от объема данных, сохраненных на нем. После нажатия кнопки OK оснастка Управление дисками создаст виртуальный жесткий диск.

Виртуальный диск будет присоединен автоматически и добавлен как новый диск. Чтобы инициализировать диск для использования, щелкните по нему правой кнопкой мыши в графическом представлении и выберите команду Инициализировать диск. В окне Инициализация дисков выберите диск для инициализации. Укажите стиль разделов — MBR или GPT — и нажмите кнопку OK.

После инициализации диска щелкните правой кнопкой мыши по нераспределенному пространству на диске и создайте том нужного типа. После создания тома VHD будет доступен для использования.

Как только VHD будет создан, присоединен, инициализирован и отформатирован, с ним можно будет работать точно так же, как и с другими дисками: записывать и читать данные; даже можно загрузить компьютер с VHD. Виртуальный диск может быть переведен в состояние В сети и Вне сети, для этого щелкните на диске правой кнопкой мыши в графическом представлении и выберите команду В сети и Вне сети соответственно. Если VHD больше не нужен, его можно отсоединить. Для этого в графическом представлении щелкните правой кнопкой мыши по диску и выберите команду Отсоединить виртуальный жесткий диск (Detach VHD), а затем нажмите кнопку OK в окне Отсоединить виртуальный жесткий диск (Detach Virtual Hard Disk).

Возможно использование виртуальных дисков, созданных другими программами. Если VHD создан в другой программе или нужно присоединить отключенный VHD, выполните эти действия:

1. В оснастке Управление дисками выберите команду Присоединить виртуальный жесткий диск (Attach VHD) из меню Действие.
2. В окне Присоединить виртуальный жесткий диск нажмите кнопку Обзор. Используйте окно Просмотр файлов виртуального диска для выбора vhd-файла и нажмите кнопку Открыть (Open).
3. Если нужно подключить VHD в режиме "только для чтения", выберите опцию Только для чтения (Read-Only). Нажмите кнопку OK для подключения VHD.

Использование базовых дисков и разделов

При установке нового компьютера или обновлении уже существующего часто нужно создать разделы на дисках компьютера. Для этого используется оснастка Управление дисками.

Основы управления разделами

В Windows Server 2012 физический диск, использующий стиль разделов, может иметь до четырех первичных разделов и один расширенный раздел. Это позволяет настраивать MBRдиски одним из двух способов: или использовать четыре первичных раздела, или использовать от одного до трех первичных разделов и один расширенный раздел. Основной раздел может заполнить весь диск или же можно установить подходящий для рабочей станции или сервера размер. В расширенном разделе допускается создание одного или больше логических дисков. Логический диск — это просто секция раздела с его собственной файловой
системой. Обычно логические диски используются, чтобы разделить большой диск на управляемые разделы. При желании можно разделить расширенный раздел размером 600 Гбайт на три логических диска по 200 Гбайт. У физических дисков со стилем разделов GPT может быть до 128 разделов.

После разделения диска на разделы нужно отформатировать их, чтобы присвоить буквы логическим дискам. Речь идет о высокоуровневом форматировании, создающем структуру файловой системы, а не о низкоуровневом, инициализирующем диск для начального использования. Все мы знакомы с диском C:, используемым Windows Server 2012. Диск C: — это просто указатель раздела диска. Если диск поделен на несколько разделов, у каждого раздела будет своя буква диска. Буквы дисков используются для доступа к файловым системам на разных разделах физического диска. В отличие от MS-DOS, которая присваивает буквы дисков автоматически, начиная с буквы C, Windows Server 2012 позволяет администратору определять буквы дисков. Обычно доступны буквы от C до Z.

Буква диска A назначается системой дисководу для гибких дисков. Если система обнаружит второй дисковод для гибких дисков, она назначит ему букву B. Поэтому администратору доступны только буквы C—Z. Помните, что DVD-диски и другие типы сменных дисков также нуждаются в букве дисков. Общее количество букв дисков, которые можно использовать — 24. Если необходимы дополнительные тома, используйте пути дисков.

Доступно всего 24 буквы диска. Чтобы преодолеть это ограничение, можно монтировать диск к путям дисков. Путь диска 1 — это каталог, через который осуществляется доступ к другому диску. Например, в системе могут быть дополнительные диски E:\Data1, E:\Data2 и E:\Data3. Пути дисков можно использовать с базовыми и динамическими дисками. Есть только одно ограничение — пути дисков должны быть пустыми папками на NTFS-дисках.

Чтобы было проще различать первичные и расширенные разделы в оснастке Управление дисками, используются цветовые коды. Например, темно-синей полосой отмечаются первичные разделы, а логические диски в расширенном разделе отмечаются голубой полосой.

Ключ для цветовой схемы показан внизу окна оснастки Управление дисками. Изменить цвета можно в диалоговом окне Параметры (Settings), которое появится при выборе команды Параметры (Settings) в меню Вид (View).

Создание разделов и простых томов

ОС Windows Server 2012 упрощает интерфейс пользователя оснастки Управление дисками, используя один набор диалоговых окон и мастеров для разделов и томов. Первые три тома на базовом диске создаются автоматически как первичные разделы. При попытке создать четвертый том на базовом диске оставшееся пространство на диске будет автоматически преобразовано в расширенный раздел. Любые последующие тома автоматически создаются в расширенных разделах как логические диски.

В оснастке Управление дисками создаются разделы, логические диски и простые тома:

1. В графическом представлении оснастки Управление дисками щелкните правой кнопкой мыши на нераспределенной или свободной области, а затем выберите команду Создать простой том (New Simple Volume). Будет запущен мастер создания простых томов (New Simple Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку Далее.
2. Появится страница Указание размера тома (Specify Volume Size) (рис. 10.3), показывающая минимальный и максимальный размеры тома в мегабайтах. Введите размер создаваемого тома в пределах ограничений в поле Размер простого тома (МБ) (Simple Volume Size In MB) и нажмите кнопку Далее.
3. На странице Назначение буквы диска или пути (Assign Drive Letter Or Path) (рис. 10.4) укажите, что нужно назначить букву диска или путь, а затем нажмите кнопку Далее.

   Доступны следующие опции.

   - Назначить букву диска (Assign The Following Drive Letter) — выберите эту опцию, чтобы назначить букву диска. Затем выберите доступную букву в предоставленном списке. По умолчанию Windows Server 2012 выбирает наименьшую доступную букву диска и исключает зарезервированные буквы, назначенные локальным и сетевым дискам.
   - Подключить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder) — выберите эту опцию для монтирования раздела к пустой NTFS-папке. Затем нужно ввести путь к существующей папке или же нажать кнопку Обзор для поиска или создания папки, которая будет использоваться.
   - Не назначать буквы диска или пути диска (Do Not Assign A Drive Letter Or Drive Path) — выберите эту опцию, если нужно создать раздел без назначения разделу буквы или пути. Если позже нужно назначить разделу букву или диск, это можно сделать в любое время.

     Допускается не присваивать томам буквы диска или путь. Том без указателей будет размонтирован и по большей части неприменим. Размонтированный том может быть смонтирован с присвоением буквы диска или пути позже (см. разд. "Назначение буквы диска или путей" главы 11).
4. На странице Форматирование раздела (Format Partition) (рис. 10.5) определите, будет ли отформатирован том. Если это необходимо сделать,

выберите Форматировать этот том следующим образом (Format This Volume With The Following Settings) и укажите следующие параметры.

- Файловая система (File System) — выберите тип файловой системы: FAT, FAT32, exFAT, NTFS или ReFS. Типы файловых систем доступны в зависимости от размера форматируемого тома. При использовании FAT32 можно позже конвертировать том в NTFS утилитой Convert. Однако нельзя конвертировать NTFS-разделы в FAT32.
- Размер кластера (Allocation Unit Size) — устанавливает размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно задать определенный размер кластера. При наличии большого количества маленьких файлов можно установить наименьший размер кластера, например 512 или 1024 байта. Так маленькие файлы используют меньше дискового пространства. Обратите внимание, что у томов ReFS фиксированный размер кластера, и его нельзя изменить.
- Метка тома (Volume Label) — устанавливает текстовую метку раздела. Эта метка — имя тома раздела и по умолчанию используется значение Новый том (New Volume). Метку тома можно изменить в любое время, щелкнув по диску правой кнопкой мыши в окне Проводника и выбрав команду Свойства. Новую метку можно ввести в поле Метка (Label) на вкладке Общие.
- Быстрое форматирование (Perform A Quick Format) — указывает операционной системе Windows Server 2012, что нужно отформатировать раздел без проверки ошибок. На больших разделах эта опция может сэкономить несколько минут. Однако обычно лучше производить проверку на ошибки, в результате которой оснастка Управление дисками пометит плохие секторы диска и заблокирует их.
- Применять сжатие файлов и папок (Enable File And Folder Compression) — включает сжатие для диска. Встроенное сжатие доступно только для файловой системы NTFS (и не поддерживается FAT, FAT32, exFAT и ReFS). При использовании NTFS сжатие будет прозрачным для пользователей, и доступ к сжатым файлам ничем не будет отличаться от доступа к обычным файлам. При выборе этой опции файлы и каталоги на этом диске автоматически будут сжиматься. Более подробную информацию о сжатых дисках, файлах см. в разд. "Сжатие дисков и данных" далее в этой главе.

5. Нажмите кнопку Далее, подтвердите выбранные параметры и нажмите кнопку Готово.

Форматирование разделов

Форматирование делит файловую систему на разделы и удаляет все существующие данные.

Здесь идет речь о высокоуровневом форматировании, создающем структуру файловой системы, а не о низкоуровневом, инициализирующем диск для начального использования. Для форматирования раздела щелкните на нем правой кнопкой мыши и выберите команду Форматировать (Format). Откроется окно Форматирование (Format), показанное на рис. 10.6.

Параметры форматирования:

1. Метка тома (Volume Label) — текстовая метка для раздела. Эта метка — имя тома раздела;
2. Файловая система (File System) — тип файловой системы — FAT, FAT32, exFAT, NTFS или ReFS. Доступные типы файловых систем зависят от размера форматируемого тома;
3. Размер кластера (Allocation Unit Size) — размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно задать определенный размер кластера. При наличии большого количества маленьких файлов можно установить наименьший размер кластера, например 512 или 1024 байта. Так маленькие файлы используют меньше дискового пространства;
4. Быстрое форматирование (Perform A Quick Format) — указывает ОС Windows Server 2012, что нужно отформатировать раздел без проверки ошибок. На больших разделах эта опция может сэкономить несколько минут. Однако обычно лучше производить проверку на ошибки, в результате которой оснастка Управление дисками пометит плохие секторы диска и заблокирует их.

Для продолжения нажмите кнопку OK. Поскольку форматирование раздела разрушает все существующие данные, оснастка Управление дисками предоставляет последний шанс отменить эту процедуру. Нажмите кнопку OK для начала форматирования раздела. Оснастка Управление дисками изменяет состояние диска и отображает процент завершения форматирования. По завершению форматирования состояние диска будет вновь изменено.

Сжатие дисков и данных

При форматировании диска в файловую систему NTFS Windows Server 2012 позволяет включить встроенную функцию сжатия. При включенном сжатии все файлы и каталоги, хранящиеся на диске, автоматически будут сжиматься при создании. Поскольку сжатие прозрачно для пользователя, то к сжатым данным пользователь получает доступ точно так же, как к обычным файлам. Разница в том, что на сжатый диск можно записать больше данных. Обратите внимание, что Проводник отмечает имена сжатых ресурсов синим цветом.

Несмотря на то, что сжатие — конечно, полезная функция, когда нужно сэкономить дисковое пространство, однако нельзя зашифровать сжатые

данные. Сжатие и шифрование — это взаимоисключающие функции для NTFS-томов: можно использовать либо сжатие, либо шифрование. Нельзя использовать оба метода. Для получения дополнительной информации о шифровании см. разд. "Шифрование дисков и данных" далее в этой главе. При попытке сжать зашифрованные данные Windows Server 2012 автоматически расшифрует их, а затем выполнит сжатие. Аналогично, при попытке зашифровать сжатые данные Windows Server 2012 сначала распакует их, а затем зашифрует.

Сжатие дисков

Для сжатия диска и всего его содержимого выполните следующие действия:

1. В Проводнике или оснастке Управление дисками щелкните правой кнопкой мыши по диску, который нужно сжать, и выберите команду Свойства.
2. На вкладке Общие окна Свойства отметьте флажок Сжать этот диск для экономии места (Compress Drive To Save Disk Space) и нажмите кнопку OK.
3. В окне Подтверждение изменения атрибутов (Confirm Attribute Changes) выберите применение ко всем подпапкам и файлам и нажмите кнопку OK.

Сжатие каталогов и файлов

Если не нужно сжимать весь диск, Windows Server 2012 позволяет сжать каталоги и файлы выборочно. Для сжатия файла или папки выполните такие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или каталоге, который нужно сжать, а затем выберите команду Свойства.
2. На вкладке Общие окна Свойства нажмите кнопку Другие. В окне Дополнительные атрибуты (Advanced Attributes) установите флажок Сжимать содержимое для экономии места на диске (Compress Contents To Save Disk Space). Нажмите кнопку OK дважды.

В случае с файлом Windows Server помечает файл как сжатый и затем сжимает его. В случае с каталогом Windows Server отмечает его как сжатый и затем сжимает все файлы в нем. Если каталог содержит подпапки, Windows Server выводит на экран диалоговое окно, позволяющее сжать все подпапки в выбранном каталоге. Просто установите переключатель К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files) и нажмите кнопку OK. После сжатия каталога любые новые файлы, добавленные или скопированные в этот каталог, будут автоматически сжаты.

При перемещении несжатого файла с другого диска этот файл будет сжат. Однако если перемещается несжатый файл в сжатую папку на том же NTFS-диске, файл не будет сжат.

Заметьте также, что нельзя зашифровать сжатые файлы.

Декомпрессия сжатых дисков

Проводник отмечает имена сжатых файлов и папок синим цветом. Действия по декомпрессии сжатых файлов таковы:

1. В Проводнике или в оснастке Управление дисками щелкните правой кнопкой мыши по диску, который нужно развернуть (декомпрессировать), и выберите команду Свойства.
2. Снимите флажок Сжать этот диск для экономии места и нажмите кнопку OK.
3. В окне Подтверждение изменения атрибутов выберите применение ко всем подпапкам и файлам и нажмите кнопку OK.

Windows всегда проверяет доступное дисковое пространство перед разворачиванием сжатых данных. Если доступное свободное пространство меньше, чем нужно, невозможно завершить декомпрессию. Например, если сжатый диск использует 150 Гбайт пространства, но свободного пространства всего 70 Гбайт, то дискового пространства будет недостаточно, чтобы развернуть данные. Обычно нужно в 1,5—2 раза больше свободного пространства, чем сжато данных.

Декомпрессия сжатых каталогов и файлов

Если необходимо развернуть сжатый файл или папку, выполните эти действия:

1. В Проводнике щелкните правой кнопкой мыши по файлу или каталогу и выберите команду Свойства.
2. На вкладке Общие окна Свойства нажмите кнопку Другие. В окне Дополнительные атрибуты снимите флажок Сжимать содержимое для экономии места на диске. Нажмите кнопку OK дважды.

В случае с файлами Windows Server удаляет атрибут сжатия и разворачивает файл. В случае с каталогами Windows Server декомпрессирует все файлы в каталоге. Если каталог содержит подпапки, можно также удалить сжатие и с подпапок. Чтобы сделать это, выберите переключатель К данной папке и ко всем вложенным папкам и файлам и нажмите кнопку OK.

Для сжатия и декомпрессии данных в Windows Server можно также использовать утилиты командной строки. Для сжатия используется утилита compact (Compact.exe), а для распаковки — утилита expand (Expand.exe).

Шифрование дисков и данных

У файловой системы NTFS есть много преимуществ над другими файловыми системами. Одно из основных преимуществ — возможность автоматического шифрования и расшифровки данных с использованием шифрованной файловой системы (Encrypting File System, EFS). При шифровании данных добавляется экстрауровень защиты важных данных, и этот экстрауровень работает как полная защита, блокирующая доступ всех других пользователей к содержимому зашифрованных файлов. Одно из преимуществ шифрования в том, что только конкретный пользователь может получить доступ к данным. Это преимущество — также и недостаток, ведь пользователь должен расшифровать данные прежде, чем авторизованные пользователи смогут получить к ним доступ.

Как было упомянуто ранее, невозможно зашифровать сжатые файлы. Шифрование и сжатие — взаимоисключающие функции NTFS. Можно использовать одну из этих функций, но не обе одновременно.

Шифрование и файловая система EFS

Файловая система EFS позволяет зашифровать как отдельные файлы, так и целые каталоги.

Любой файл, помещенный в зашифрованную папку, автоматически будет зашифрован. Зашифрованные файлы могут быть прочитаны только тем лицом, кто их зашифровал. Прежде, чем другие пользователи смогут прочитать зашифрованный файл, пользователь должен расшифровать файл или добавить в файл ключ шифрования пользователя.

У каждого зашифрованного файла должен быть уникальный ключ шифрования пользователя, создавшего файл, точнее, того, кто в данный момент является владельцем файла. Зашифрованный файл может быть скопирован, перемещен или переименован, как любой другой файл, и в большинстве случаев эти файлы никак не отражаются на шифровании данных (более подробно см. разд. "Работа с зашифрованными файлами и папками" далее в этой главе). Пользователь, зашифровавший файл, всегда имеет доступ к файлу при условии, что сертификат пользователя с открытым ключом доступен на компьютере, который он использует. Для этого пользователя процесс шифрования и дешифрования обрабатывается автома
тически и полностью прозрачно.

EFS — это процесс, выполняющий шифрование и расшифровку. Настройки по умолчанию для EFS позволяют пользователям зашифровывать файлы без специальных полномочий.

Файлы шифруются с использованием публичного/частного ключа, которые EFS автоматически генерирует для каждого пользователя.

Сертификаты шифрования хранятся как часть данных в профиле пользователя. Если пользователь работает с несколькими компьютерами и желает использовать шифрование, администратор должен настроить перемещаемый профиль для этого пользователя. Перемещаемый профиль гарантирует, что данные профиля пользователя и сертификаты публичного
ключа будут доступны с других компьютеров. Без этого пользователь не сможет получить доступ к своим зашифрованным файлам на другом компьютере.

Альтернативой перемещаемому профилю может стать копирование сертификата шифрования пользователя на компьютеры, которые он должен использовать. О том, как сделать это, рассказано в главе 3. Просто заархивируйте сертификат пользователя на исходном компьютере и восстановите его на каждом компьютере, который использует пользователь.

У EFS есть встроенная система восстановления данных, защищающая от потери данных. Эта система восстановления позволяет убедиться, что зашифрованные данные могут быть восстановлены, если сертификат публичного ключа пользователя будет потерян или удален.

Наиболее вероятный сценарий этого — удаление учетной записи пользователя после его увольнения. У руководителя должна быть возможность войти в учетную запись пользователя, проверить файлы и сохранить важные файлы в другие папки, но если учетная запись
пользователя была удалена, зашифрованные файлы будут доступны, только если было отключено шифрование или файлы перемещены в файловые системы exFAT, FAT или FAT32 (где шифрование не поддерживается).
Для доступа к зашифрованным файлам после удаления учетной записи пользователя нужно использовать агент восстановления. Агент восстановления имеет доступ к ключу шифрования файла и при необходимости может разблокировать данные в зашифрованных файлах.
Однако для защиты важных данных агент восстановления не имеет доступа к приватному ключу пользователя.
Windows Server не будет расшифровывать файлы без назначенных агентов восстановления EFS. Поэтому агенты восстановления назначаются автоматически, также автоматически генерируются сертификаты, необходимые для восстановления. Это гарантия, что зашифрованные файлы всегда будут восстановлены.
Агенты восстановления EFS настраиваются на двух уровнях.

- Домен. Агент восстановления для домена настраивается автоматически при первой установке первого контроллера домена Windows Server. По умолчанию агент восстановления — это администратор домена. С помощью групповой политики администраторы домена могут назначить дополнительных агентов восстановления. Администраторы также могут делегировать привилегии агентов восстановления определенным администраторам безопасности.
- Локальный компьютер. Когда компьютер — часть рабочей группы или же полностью автономен, агент восстановления — по умолчанию администратор локального компьютера. Дополнительные агенты восстановления могут быть назначены. В дальнейшем, если нужно в среде домена использовать локальных агентов восстановления, а не агентов восстановления уровня домена, необходимо удалить политику восстановления из групповой политики домена.

Агенты восстановления можно удалить, если в них нет необходимости. Однако, если удалить всех агентов восстановления, EFS больше не сможет шифровать файлы. Для работы функции EFS нужно настроить одного или более агента восстановления.

Шифрование каталогов и файлов

При использовании файловой системы NTFS операционная система Windows Server позволяет выбрать файлы и каталоги для шифрования. Когда файл зашифрован, данные файла конвертируются в зашифрованный формат, который может быть прочитан только лицом, которое зашифровало файл. Пользователи могут зашифровывать файлы, только если у них есть надлежащие права доступа. При шифровании папки она отмечается как зашифрованная, но

на самом деле шифруются только файлы внутри нее. Все файлы, которые были созданы или добавлены в зашифрованную папку, шифруются автоматически. Проводник отмечает имена зашифрованных объектов зеленым цветом.
Для шифрования файла или каталога выполните эти действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или каталоге, который нужно зашифровать, и выберите команду Свойства.
2. На вкладке Общие окна Свойства нажмите кнопку Другие, а затем установите флажок Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data). Нажмите кнопку OK дважды.

Невозможно зашифровать сжатые файлы, системные файлы и файлы с атрибутом "только для чтения". При попытке зашифровать сжатые файлы они будут автоматически распакованы, а затем зашифрованы. При попытке зашифровать системные файлы будет отображено сообщение об ошибке.
В случае с отдельными файлами Windows Server помечает файлы как зашифрованные и затем шифрует их. В случае с каталогами Windows Server отмечает каталог как зашифрованный и затем шифрует все файлы в нем. Если каталог содержит подпапки, Windows отобразит окно, позволяющее зашифровать все вложенные подпапки. Просто установите переключатель К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files) и нажмите кнопку OK.
На NTFS-томах файлы остаются зашифрованными, даже если их переместить, скопировать или переименовать. Если скопировать или переместить зашифрованный файл на exFAT, FAT или FAT32, файл автоматически будет расшифрован перед копированием или перемещением. Для копирования или перемещения файла нужны надлежащие полномочия.
Чтобы предоставить специальный доступ к зашифрованному файлу или каталогу, щелкните правой кнопкой мыши на файле или папке в окне Проводника и выберите команду Свойства. На вкладке Общие окна Свойства нажмите кнопку Другие. В окне Дополнительные атрибуты нажмите кнопку Подробно (Details). В появившемся окне будут перечислены пользователи, обладающие доступом к зашифрованному файлу. Чтобы предоставить другому пользователю доступ к файлу, нажмите кнопку Добавить. Если доступен сертификат пользователя, выберите имя пользователя в предоставленном списке и нажмите кнопку OK. В противном случае нажмите кнопку Найти пользователя (Find user) для выбора сертификата пользователя.

Работа с зашифрованными файлами и папками

Ранее было отмечено, что можно копировать, перемещать и переименовывать зашифрованные файлы и папки подобно любым другим файлам. Это так, но была оговорка — "в большинстве случаев". При работе с зашифрованными файлами, пока они находятся на NTFStомах того же компьютера, проблем не будет. При работе с другими файловыми системами
или компьютерами можно столкнуться с настоящими проблемами. Наиболее вероятны два следующих сценария.

- Копирование между томами одного и того же компьютера. При копировании или перемещении зашифрованных файлов или папок с одного NTFS-тома на другой NTFStом на том же компьютере файлы остаются зашифрованными. Однако, если скопировать или переместить зашифрованные файлы на FAT-том, файлы будут расшифрованы перед передачей и преобразованы в стандартные файлы, поэтому скопированы будут незашифрованные файлы. Файловая система FAT не поддерживает шифрование.
- Копирование между томами на разных компьютерах. При копировании или перемещении зашифрованных файлов или папок с одного NTFS-тома на другой NTFS-том на другом компьютере файлы останутся зашифрованными, пока целевой компьютер позволяет шифровать файлы и удаленному компьютеру доверяют делегирование. В противном случае файлы будут расшифрованы и затем переданы как обычные файлы. То же самое произойдет при копировании или перемещении файлов на FAT-том на другом компьютере. Файловая система FAT не поддерживает шифрование.

После копирования важных зашифрованных файлов нужно убедиться, что шифрование все еще применено. Щелкните на файле правой кнопкой мыши и выберите команду Свойства. На вкладке Общие окна Свойства нажмите кнопку Другие. Убедитесь, что атрибут Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data) включен.

Настройка политики восстановления

Политики восстановления автоматически настраиваются для контроллеров домена и рабочих станций. По умолчанию контроллеры домена назначаются агентами восстановления для доменов, а локальные администраторы назначаются агентами восстановления для автономных рабочих станций.

С помощью групповой политики можно просмотреть, назначить и удалить агентов восстановления. Чтобы сделать это, выполните следующие действия:

1. Откройте групповую политику локального компьютера, сайта, домена или организационного подразделения. Более подробная информация об этом была приведена в главе 4.
2. Откройте узел Агент восстановления зашифрованных данных (Encrypted Data Recovery Agents) в групповой политике. Для этого разверните узел Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики открытого ключа\Шифрованная файловая система (EFS) (Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System).
3. На правой панели отображается список назначенных в данный момент сертификатов восстановления. Для каждого сертификата выводится, кто его выпустил, дата истечения, назначение и т. д.
4. Для назначения дополнительных агентов восстановления щелкните правой кнопкой мыши на узле Шифрованная файловая система (EFS) (Encrypting File System) и выберите команду Добавить агент

восстановления данных (Add Data Recovery Agent). Будет открыт мастер добавления агента восстановления (Add Recovery Agent Wizard), который используется для выбора ранее сгенерированных сертификатов, назначенных пользователю. Затем можно пометить выбранный сертификат как назначенный сертификат восстановления. Нажмите кнопку Далее.

5. На странице Выбор агентов восстановления (Select Recovery Agents) можно выбрать сертификаты, опубликованные в Active Directory, или использовать файлы сертификатов. Если нужно использовать опубликованный сертификат, нажмите кнопку Обзор каталога (Browse Directory), используйте окно Поиск: Пользов., контакты и группы (Find Users, Contacts, And Groups), выберите пользователя. Будет предоставлена возможность использовать опубликованный сертификат этого пользователя. Если нужно использовать файл сертификата, нажмите кнопку Обзор папок. В окне Открытие (Open) выберите файл сертификата, который нужно использовать.
   Перед назначением дополнительных агентов восстановления нужно рассмотреть настройку корневого центра сертификации в домене. Затем можно использовать оснастку Сертификаты (Certificates) для создания персональных сертификатов, которые используют шаблон EFS Recovery Agent. Корневой центр сертификации должен потом утвердить запрос сертификата, чтобы тот мог использоваться.
6. Для удаления агента восстановления выберите сертификат агента восстановления в правой панели и нажмите кнопку Удалить. Затем нажмите кнопку Да для удаления сертификата без возможности восстановления. Если политика безопасности пуста (это означает, что не назначено выделенных агентов восстановления), EFS будет выключена так, что файлы больше не будут зашифровываться, а существующие уже зашифрованные ресурсы EFS не будут иметь агента восстановления.

Расшифровка файлов и каталогов

Проводник отмечает зеленым цветом имена зашифрованных файлов. Для расшифровки файла или каталога выполните такие действия:

1. В Проводнике щелкните по файлу или каталогу правой кнопкой мыши и выберите команду Свойства.
2. На вкладке Общие окна Свойства нажмите кнопку Другие. Установите флажок Шифровать содержимое для защиты данных. Нажмите кнопку OK дважды.

В случае с файлами Windows Server расшифрует и восстановит файл в его исходный формат. В случае с папками Windows Server расшифрует все файлы внутри папки. Если каталог содержит подпапки, будет предоставлена возможность снять шифрование и с подпапок.

Для этого выберите переключатель К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files) и нажмите кнопку OK.

Windows Server также предоставляет утилиту командной строки Cipher (Cipher.exe), которая используется для шифрования и расшифровки данных. Запуск Cipher в командной строке без дополнительных параметров выведет состояние шифрования всех папок в текущем каталоге.

ГЛАВА 2 Настройка томов и RAID-массивов

Управление хранилищем существенно изменилось за прошедшие несколько лет, как и технологии, которые Microsoft Windows Server использует для работы с дисками. Хотя традиционные методы управления хранилищем относятся к физическим дискам, расположенным в сервере, сегодня много серверов использует присоединенные хранилища и виртуальны диски.

Обычно при работе с внутренними жесткими дисками нужно часто выполнять процедуры настройки диска: создание томов или настройку избыточного массива независимых жестких дисков (Redundant Array of Independent Disks, RAID). Администратор создает тома или массивы, которые могут состоять из нескольких дисков, и при этом он знает точное физическое расположение тех дисков.

При работе с присоединенным хранилищем администратор может не знать, на каком физическом диске или дисках находится том, с которым он работает. Вместо этого используется виртуальный диск, называемый также LUN (Logical Unit Number), который является логическим указателем на часть подсистемы хранения. Несмотря на то, что виртуальный диск может находиться на одном или более физических дисках, разметка физических дисков контролируется отдельно от операционной системы (подсистемой хранения).

В этой главе сначала будут рассмотрены традиционные методы создания массива томов, а потом методы — стандартизированные. Управление томом осуществляется одинаково, независимо от того, используется ли традиционный подход или подход на основе стандартов. Поэтому в заключительном разделе этой главы будут рассмотрены методы работы с существующими томами и дисками.

Способы стандартизированного управления хранилищами могут быть использованы также с внутренними дисками сервера. Когда внутренние диски используются таким образом (как виртуальные диски, подключенные к хранилищу), выделенные ресурсы будут использовать стандартизированные методы. Это означает, что можно создать тома виртуального диска на физических дисках, добавить физические диски к пулам носителей данных, а также создать виртуальные диски iSCSI. Также можно включить дедупликацию данных на своих виртуальных дисках. Однако нельзя использовать массив томов и функции RAID операционной системы. Причина заключается в том, что способы стандартизированного управления хранилищем основываются на подсистеме хранения для управления архитектурой физического диска.

Использование томов и массивов томов

При использовании массива томов можно создать один том, состоящий из нескольких дисков. Пользователи могут получить доступ к этому тому, как

будто это единственный диск, независимо от того, сколько дисков входит в состав тома. Том, находящийся на одном диске, называется простым томом. Том, охватывающий множество дисков, называется составным томом.
С помощью RAID-массивов можно защитить важные деловые данные и в некоторых случаях улучшить производительность дисков. RAID может быть реализован посредством встроенных функций операционной системы (программный RAID) или с помощью аппаратных средств (аппаратный RAID). Windows Server 2012 поддерживает три уровня программного RAID: 0, 1 и 5. RAID-массивы реализуются как зеркальные, чередующиеся и чередующиеся с контролем четности.
Массивы томов и RAID-массивы создаются на динамических дисках, которые доступны только в Windows 2000 и более поздних версиях. Однако компьютеры под управлением ранних версий Windows смогут получить доступ к таким дискам по сети, как и к любому другому сетевому диску.
Создание и управление томами осуществляется так же, как и создание и управление разделами. Том — это часть диска, которую можно использовать для хранения данных непосредственно.
При использовании составных и чередующихся томов на базовых дисках можно удалить том, но нельзя создать или расширить том. При использовании зеркальных томов на базовых дисках можно удалять, чинить и синхронизировать зеркало. Также можно разбить зеркало. При использовании чередования с контролем четности (RAID 5) на базовых дисках можно удалить или чинить том, но нельзя создавать новые тома.

Понимание базовых томов

В оснастке Управление дисками тома разных типов помечаются цветом аналогично разделам. Тома имеют следующие свойства:

- Расположение (Layout) — может быть: простой, составной, зеркальный чередующийся и чередующийся с контролем четности;
- Тип (Type) — тома всегда имеют тип динамический;
- Файловая система (File System) — подобно разделам, каждый том может иметь собственную файловую систему, например FAT или NTFS. Обратите внимание, что FAT16 доступна только, если размер раздела или тома 2 Гбайт или меньше;
- Состояние (Status) — состояние диска. В графическом представлении показано состояние диска как Исправен (Healthy), Отказавшая избыточность (Failed Redundancy) и т. д. В следующем разделе мы обсудим массивы томов и различные состояния;
- Емкость (Capacity) — емкость диска;
- Свободно (Free Space) — сколько свободного пространства осталось на томе;
- Свободно % (%Free) — процентное соотношение свободного пространства к емкости тома.

Важное преимущество динамических томов по сравнению с базовыми томами в том, что они позволяют вносить изменения в тома и диски без необходимости перезапуска системы (в большинстве случаев). Тома также позволяют использовать улучшения отказоустойчивости Windows Server 2012. Можно установить другие операционные системы и использовать двойную загрузку. Чтобы сделать это, нужно создать отдельный том для другой операционной системы. Например, можно установить Windows Server 2012 на томе C, а Windows 8 на томе D.

С томами можно сделать следующее:

- назначать буквы и пути дисков, как будет описано в разд. "Назначение букв и путей дисков" далее в этой главе;
- создавать любое количество томов на диске — столько, на сколько хватит свободного пространства;
- создавать тома, состоящие из двух или более дисков, если необходимо, настроить толерантность отказа;
- расширить тома до полной емкости тома;
- назначить активный, системный и загрузочный том.

Массивы томов

При работе с массивами томов можно создать тома, состоящие из нескольких дисков. Для этого объедините свободное пространство на разных дисках, чтобы пользователи увидели его как общий том. Файлы хранятся в массиве томов посегментно. Когда первый сегмент свободного пространства заполняет, используется второй сегмент и т. д.

Можно создать массив томов, основанный на свободном пространстве до 32 жестких дисков. Основное преимущество массивов томов заключается в том, что они позволяют использовать свободное пространство и создавать используемую файловую систему. Основной недостаток — если какой-то жесткий диск в массиве выйдет из строя, массив томов больше нельзя будет использовать, т. е. все данные массива томов будут потеряны.

Полезно разбираться в состояниях тома, особенно при установке новых томов или диагностировании проблем. Оснастка Управление дисками показывает состояние диска в графическом представлении и списке томов. В табл. 2.1 приведены значения состояния динамических дисков.

Таблица 2.1. Состояния диска и решение проблем

Состояние	Описание	Решение
Неполные данные (Data Incomplete)	Составные тома на чужом диске неполные. Администратор забыл добавить другие диски из составного массива томов	Добавьте диски, содержащие оставшуюся часть составного тома, и затем импортируйте все диски за один раз
Нет избыточности	Была импортирована только часть зеркального	Добавьте оставшиеся диски и затем импортируйте все диски

данных (Data Not Redundant)	тома. Администратор забыл добавить другие диски зеркала или массива RAID 5	сразу
Неисправен (Failed)	Состояние ошибки диска. Диск недоступен или поврежден	Убедитесь, что динамический диск находится в состоянии В сети. При необходимости щелкните правой кнопкой мыши на томе и выберите команду Реактивировать диск (Reactivate Volume). Для базового диска нужно проверить диск на неправильное подключение
Отказавшая избыточность (Failed Redundancy)	Состояние ошибки. Один из дисков в зеркале или массиве RAID 5 находится в состоянии Вне сети	Убедитесь, что динамический диск находится в состоянии В сети. При необходимости реактивируйте том. Далее нужно заменить отказавшее зеркало или починить отказавший том RAID 5
Форматирование (Formatting)	Временное состояние, показывающее, что том в данный момент форматируется	Индикатор процесса форматирования показывает процент готовности, за исключением быстрого форматирования
Исправен (Под угрозой) (Healthy (At Risk))	Windows обнаружила проблемы чтения или записи на физическом диске, на котором расположен динамический том. Состояние появляется, когда Windows обнаружила ошибки	Щелкните правой кнопкой мыши на диске и выберите команду Реактивировать диск. Если это не поможет (состояние не изменится или состояние отказа диска возвращается), нужно выполнить резервное копирование всех данных диска
Исправен (Неизвестный раздел) (Healthy (Unknown Partition))	Windows не может распознать раздел. Ситуация возникает, если раздел принадлежит другой операционной системе или это раздел, созданный производителем для	Не требует корректирующих действий

	хранения системных файлов	
Инициализация (Initializing)	Временное состояние, диск в данный момент инициализируется	Состояние диска должно измениться через несколько секунд
Регенерация (Regenerating)	Временное состояние, данные и четность для RAID 5 тома регенерируются	Индикатор хода процесса показывает процент выполнения этого процесса. Том должен вернуться в состояние Исправен
Ресинхронизация (Resynching)	Временное состояние, показывающее, что зеркало в данный Момент ресинхронизируется	Индикатор хода процесса показывает процент выполнения этого процесса. Том должен вернуться в состояние Исправен (Healthy).
Устаревшие данные (Stale Data)	Сбой данных на чужих дисках	Пересканируйте диски или перезагрузите компьютер, а затем проверьте состояние. Будет отображено новое состояние, например, Отказавшая избыточность
Нет данных (Unknown)	Нет доступа к тому. Скорее всего, поврежден загрузочный сектор	Возможен вирус в загрузочном секторе. Проверьте диск антивирусной программой. Проверьте диск или перезагрузите компьютеры, а затем проверьте состояние

Создание томов и массивов томов

Простые тома можно отформатировать как exFAT, FAT, FAT32 или NTFS. Для упрощения управления составные тома должны быть отформатированы как NTFS. NTFS-форматирование позволяет расширить тома в случае необходимости. Если понадобится больше пространства на томе, можно расширить простой или составной том. Это можно сделать, выбрав свободное пространство и добавив его в том. Можно расширить простой том в пределах этого же диска. Также можно расширить простой том на другие диски. После этого будет создан расширенный том, который должен быть отформатирован как NTFS.

Создать тома или массивы томов можно с помощью следующих действий:

1. В графическом представлении оснастки Управление дисками щелкните правой кнопкой мыши на нераспределенном пространстве и выполните команду Создать составной том (New Spanned Volume) или Создать чередующийся том (New Striped Volume). Прочтите страницу приветствия и нажмите кнопку Далее.

2. На странице Выбор дисков (Select Disks) выберите диски, которые должны быть частью тома, а также укажите размер сегментов тома на этих дисках.
3. Доступные диски показаны в списке Доступны (Available). Если необходимо, выберите диск в этом списке и нажмите кнопку Добавить для добавления диска в список Выбраны (Selected). Если будет допущена ошибка, можно удалить диск из списка Выбраны: выберите диск и нажмите кнопку Удалить (Remove).
   Мастера дисков в Windows Server 2012 показывают и базовые, и динамические диски, где есть свободное пространство. Если добавите пространство из базового диска, мастер автоматически конвертирует диск в динамический перед созданием массива томов. Перед нажатием кнопки Да для продолжения убедитесь, что действительно это нужно, поскольку это может повлиять на то, как диск используется операционной системой.
4. Выберите диск в списке Выбраны (Selected), а затем укажите размер тома на диске в поле Выберите размер выделяемого пространства (МБ) (Select The Amount Of Space In MB). Поле Максимальное доступное пространство (МБ) (Maximum Available Space In MB) показывает наибольшую область свободного пространства, доступного на диске. Общий размер тома (МБ) (Total Volume Size In Megabytes) показывает общее дисковое пространство, которое будет использовано для тома. Нажмите кнопку Далее. Хотя можно установить размер тома любым способом, примите во внимание, как массивы томов будут использоваться в системе. Простые и составные тома не отказоустойчивы. Вместо создания одного огромного тома на всем доступном свободном пространстве можно создать несколько меньших томов, чтобы отказ одного тома не стал причиной потери всех данных.
5. Укажите, нужно ли назначить букву диска тому или том будет подключен как пустая NTFS-папка, а затем нажмите кнопку Далее. Доступны следующие варианты:
   - Назначить букву диска (Assign the following drive letter) — позволяет назначить букву диска, отметьте эту опцию и затем выберите доступную букву из предоставленного списка;
   - Подключить том как пустую NTFS-папку (Mount in the following empty ntfs folder) — используется для назначения пути диска, выберите эту опцию и затем введите путь к существующей папке на NTFS-диске, нажмите кнопку Обзор для поиска или создания папки;
   - Не назначать буквы диска или пути диска (Do not assign a drive letter or drive path) — выберите эту опцию для создания тома без назначения буквы диска или пути. Можно назначить букву диска или путь в любое время.
6. Укажите, должен ли том быть отформатированным. Если нужно отформатировать том, установите следующие опции форматирования:

- Файловая система (File system) — укажите тип файловой системы. В оснастке Управление дисками доступна только файловая система NTFS;
- Размер кластера (Allocation unit size) — устанавливает размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно установить размер кластера в определенное значение. Если есть много маленьких файлов, можно задать наименьший размер кластера, например, 512 или 1024 байта. Так маленькие файлы используют меньше дискового пространства;
- Метка тома (Volume label) — определяет текстовую метку для раздела. Эта метка — имя тома раздела;
- Быстрое форматирование (Perform a quick format) — указывает Windows Server 2012, что нужно отформатировать раздел без проверки ошибок. На больших разделах эта опция может сэкономить несколько минут. Однако обычно лучше производить проверку на ошибки, в результате которой оснастка Управление дисками пометит плохие секторы диска и заблокирует их;
- Применять сжатие файлов и папок (Enable file and folder compression) — включает сжатие для диска. Сжатие прозрачно для пользователей, и доступ к сжатым файлам осуществляется подобно доступу к обычным файлам. Если выбрать эту опцию, файлы и каталоги на этом диске будут сжиматься автоматически.

7. Нажмите кнопку Далее, а затем кнопку Готово.

Удаление томов и массивов томов

Тома всех типов (простые, составные, зеркальные, чередующиеся или RAID 5 (чередующиеся с контролем четности)) удаляются одним и тем же способом. Удаление массива томов удаляет связанные файловые системы и все данные на них. Перед удалением массива томов необходимо сделать резервную копию файлов и каталогов, хранящихся на этих массивах томов.

Нельзя удалить том, содержащий системные, загрузочные файлы или файлы подкачки Windows Server 2012.

Для удаления томов выполните действия:

- В оснастке Управление дисками щелкните правой кнопкой мыши по тому в массиве и выберите команду Удалить том (Delete Volume). Нельзя удалить часть составного тома без удаления всего тома.
- Нажмите кнопку Да для подтверждения удаления тома.

Управление томами

Управление томами происходит аналогично управлению разделами.

Повышение производительности и отказоустойчивости с помощью RAID

Часто нужно повысить защиту важных данных от отказов диска. Для этого используется технология RAID. С помощью RAID можно увеличить целостность данных и их доступность, создавая избыточные копии данных. Также можно использовать RAID, чтобы повы-сить производительность дисков.

Доступны различные реализации технологии RAID. Эти реализации описаны в терминах уровней. На данный момент определены уровни RAID от 0 до 5. Каждый уровень RAID отличается набором функций. Операционная система Windows Server 2012 поддерживает уровни RAID 0, 1 и 5. Можно использовать уровень RAID 0 для повышения производительности дисков. Уровни RAID 1 и RAID 5 применяются для повышения отказоустойчивости
данных. В табл. 11.2 предоставлен краткий обзор поддерживаемых уровней RAID. Поддержка осуществляется полностью программно.

Наиболее часто используемые на Windows-серверах уровни RAID — 1 (зеркалирование) и 5 (чередование с контролем четности). Зеркалирование диска — наименее дорогой способ повысить защиту данных с избыточностью. Здесь, для создания избыточного набора данных используются два тома одинакового размера на двух разных дисках. Если один из дисков откажет, можно восстановить данные с другого диска.

С другой стороны, чередование дисков с контролем четности требует большего числа дисков — как минимум три, зато предлагает отказоустойчивость с наименьшим числом издержек, чем зеркалирование дисков. Если произошел сбой диска, можно восстановить данные, комбинируя блоки данных на оставшихся дисках с записью четности. Четность — метод проверки ошибок, которая использует операцию "исключающее ИЛИ" для создания контрольной суммы для каждого блока данных, записанного на диск. Эта контрольная сумма используется для восстановления данных в случае отказа.

Таблица 2.2. Уровни RAID, поддерживаемые Windows Server 2012

Уровень RAID	Тип RAID	Описание	Основные преимущества
0	Чередование дисков	Два или более тома, каждый из которых находится на отдельном диске, настраиваются как чередующийся набор. Данные разбиваются на блоки — страйпы, а затем записываются последовательно на все диски в наборе.	Скорость и производительность

		Отказ одного диска приводит к неработоспособности массива	
1	Зеркалирование дисков	Два тома на двух дисках настраиваются идентично. Данные записываются на оба диска. Если один диск откажет, потерь данных не будет, поскольку другой диск содержит данные (этот уровень не поддерживает чередования)	Отказоустойчивость. Лучшая производительность записи по сравнению с чередованием с контролем четности
5	Чередование диска с контролем четности	Использует три или более тома, каждый на одном из дисков для создания чередования с контролем четности проверки ошибок. В случае сбоя данные могут быть восстановлены	Отказоустойчивость с меньшим количеством издержек, чем зеркалирование. Лучшая скорость чтения по сравнению с зеркалированием

Настоящие затраты для зеркалирования должны быть меньше, чем для чередования с четностью, но реальная стоимость гигабайта выше в случае с зеркалированием дисков. В случае с зеркалированием издержки составляют 50%. Например, если зеркалируются два диска по 750 Гбайт (общее пространство составляет 1500 Гбайт), то для хранения данных можно использовать только 750 Гбайт. Для чередования с контролем четности издержки составят примерно 33%. Например, если создается набор RAID 5, использующий три диска по 500 Гбайт (общее пространство — 1500 Гбайт), для хранения данных будет доступно 1000 Гбайт (издержки — одна треть).

Реализация RAID на Windows Server 2012

Операционная система Windows Server 2012 поддерживает зеркалирование диска, чередование диска и чередование с контролем четности. Реализация этих техник RAID описана в следующем разделе.

Некоторые операционные системы, например MS-DOS, не поддерживают RAID. Если нужна двойная загрузка одной из таких операционных систем, RAID-диски будут недоступны.

Реализация RAID 0: чередование диска

Уровень RAID 0 — это чередование диска. При чередовании диска два или более томов каждый на отдельном диске настраиваются как чередующийся набор. Данные, записываемые в чередующийся набор, называются страйпами. Эти страйпы записываются последовательно на все диски в наборе. Тома чередующегося набора могут быть размещены на 32 дисках, но более целесообразно использовать наборы из 2—5 томов для лучшей производительности. При большем числе дисков значительно снижается производительность.

Основное преимущество чередования дисков — это скорость. Поскольку данные находятся на нескольких дисках и для доступа к ним используется несколько головок, в результате повышается производительность. Однако этот прирост производительности стоит денег.

При работе с наборами томов, если один из дисков откажет, чередующийся набор больше нельзя будет использовать, т. е. все данные в этом наборе будут потеряны. Нужно воссоздать чередующийся набор и восстановить данные из резервной копии. Резервное копирование и восстановление данных обсуждается в главе 13.

Загрузочный и системный тома не могут быть частью чередующегося набора. Не используйте чередование диска с этими томами.

При создании чередующихся наборов нужно использовать тома приблизительно одинакового размера. Управление дисками вычисляет полный размер чередующегося набора по наименьшему размеру тома. Максимальный размер набора — количество дисков, умноженное на размер наименьшего тома. Например, если наименьший размер тома равен 20 Гбайт и нужен набор из трех дисков, максимальный размер набора — 60 Гбайт.

Максимизировать производительность чередующегося набора можно несколькими способами:

- используйте диски, размещенные на разных дисковых контроллерах. Это позволяет системе одновременно получать доступ к дискам;
- не используйте диски, входящие в состав чередующего набора, в других целях. Это позволяет диску выделить все свое время чередующемуся набору.

Создать чередующийся набор можно с помощью следующих действий:

1. В графическом представлении оснастки Управление дисками щелкните правой кнопкой мыши по нераспределенной области динамического диска и выберите команду Создать чередующийся том (New Striped Volume). Будет запущен мастер создания чередующихся томов (New Striped Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку Далее.
2. Создание томов было описано в разд. "Создание томов и массивов томов" ранее в этой главе. Основное отличие — нужны как минимум два динамических диска, чтобы создать чередующийся том.

После создания чередующегося тома можно использовать том, как том любого другого типа. Нельзя расширить чередующийся том, как только он будет создан. Поэтому к созданию томов отнеситесь со всей ответственностью.

Реализация RAID 1: зеркалирование диска

RAID 1 — это зеркалирование диска. При зеркалировании используются тома одинакового размера на двух разных дисках для создания избыточного набора данных. На диски записываются идентичные наборы информации, и если один из дисков откажет, информацию все еще можно будет получить со второго диска.

Зеркалирование дисков тоже предлагает отказоустойчивость, как и чередование дисков с четностью. Поскольку диски зеркала не должны записывать контроль четности, они обеспечивают лучшую производительность записи в большинстве случаев. Однако чередование с контролем четности обычно выигрывает в скорости чтения, поскольку операции чтения распределяются по нескольким дискам.

Основной недостаток зеркалирования — неэффективное использование дискового пространства. Например, для зеркалирования диска на 500 Гбайт нужен еще один такой диск на 500 Гбайт. Это означает, что фактически дисковое пространство в 1000 Гбайт будет использоваться для хранения 500 Гбайт информации.

Если возможно, нужно зеркально отразить системный и загрузочные тома. Это позволит загрузить сервер в случае выхода одного диска из строя.

Как и с чередованием дисков, зеркально отраженные диски должны быть на отдельных дисковых контроллерах. Это обеспечивает дополнительную защиту в случае отказа одного из дисковых контроллеров. Если один из контроллеров откажет, диск на втором контроллере будет все еще доступен. Технически при использовании двух отдельных контроллеров диска для дедупликации данных на самом деле используется метод, называемый дублированием дисков. На рис. 11.3 показана разница между этими двумя методами. Зеркалирование обычно использует единственный контроллер, дублирование — два контроллера. В противном случае оба метода — по существу, одно и то же.

Если один из дисков набора откажет, операции с диском могут быть продолжены. Здесь,

когда пользователи читают и записывают данные, данные будут записаны на работоспособный диск. Перед исправлением зеркала его нужно разбить. Чтобы узнать, как это сделать, см. разд. "Управление RAID-массивами и восстановление после сбоя" далее в этой главе.

Создание зеркального набора в оснастке Управление дисками

Создать зеркальный набор можно с помощью следующих действий:

1. В графическом представлении оснастки Управление дисками щелкните на нераспределенной области динамического диска и выберите команду Создать зеркальный том (New Mirrored Volume). Будет запущен мастер

создания образа (New Mirrored Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку Далее.

2. Создайте том, как было описано в разд. "Создание томов и массивов томов" ранее в этой главе. Основное отличие — нужно создать два тома одинакового размера, и эти тома должны быть расположены на разных динамических дисках. На странице Выбор диска (Select Disks) нельзя продолжить, пока не выберете два диска, с которыми будете работать.

Подобно другим техникам RAID, зеркалирование прозрачно для пользователей. Пользователи будут видеть зеркальный набор как единственный диск, доступ к которому может быть получен как к любому другому диску.

Нормальное состояние зеркала — Исправен. Во время создания зеркала можно увидеть состояние Ресинхронизация, говорящее о том, что оснастка Управление дисками создает зеркало.

Зеркалирование существующего тома

Вместо создания нового зеркального тома можно использовать существующий том для создания зеркального набора. Для этого том, который нужно зеркалировать, должен быть простым томом и на втором диске нужно иметь нераспределенную область равного или большего размера (чем существующий том).

Чтобы в оснастке Управление дисками зеркально отразить существующий том, выполните следующие действия:

1. Щелкните правой кнопкой мыши по простому тому, который нужно зеркально отразить, а затем выберите команду Добавить зеркало (Add Mirror). Появится окно Добавить зеркальный том (Add Mirror).
2. В списке Диски (Disks) выберите расположение для зеркала, а затем нажмите кнопку Добавить зеркальный том (Add Mirror). ОС Windows Server 2012 начнет процесс создания зеркала, а в оснастке Управление дисками будет установлено состояние Ресинхронизация на обоих томах. У диска, на котором создается зеркальный том, будет значок предупреждения.

Реализация RAID 5: чередование диска с контролем четности

Уровень RAID 5 — это чередование диска с контролем четности. Эта техника требует как минимум трех жестких дисков для настройки отказоустойчивости. Размеры томов на всех трех дисках должны быть одинаковыми. RAID 5, по сути, является улучшенной версией RAID-1 с ключевым добавлением отказоустойчивости. Отказоустойчивость гарантирует, что отказ одного диска не приведет к отказу всего набора. Вместо отказа набор продолжает функционировать с оставшимися томами в наборе.

Для обеспечения отказоустойчивости RAID 5 записывает контрольные суммы четности с блоками данных. Если любой из дисков набора откажет, можно использовать информацию четности для восстановления данных (этот процесс называется регенерацией чередующегося набора и будет описан в разд. "Управление RAID-массивами и восстановление после сбоя" далее в этой

главе). Если откажут два диска, информации четности будет недостаточно для восстановления данных и нужно будет восстановить набор из резервной копии.

Создание чередующегося набора с четностью в оснастке Управление дисками

В оснастке Управление дисками можно создать чередующийся набор с четностью с помощью следующих действий:

1. В графическом представлении оснастки Управление дисками щелкните правой кнопкой мыши на нераспределенном пространстве динамического диска и выберите команду Создать том RAID 5 (New RAID 5 Volume). Будет запущен мастер создания томов RAID 5 (New RAID 5 Volume Wizard). Прочитайте страницу приветствия и нажмите кнопку Далее.
2. Создайте том, как было описано в разд. "Создание томов и массивов томов" ранее в этой главе. Основное отличие — нужно выбрать три нераспределенных области на трех разных динамических дисках.

После создания чередующегося набора с контролем четности (RAID 5) пользователи могут
использовать том, как обычный диск. Помните, что нельзя расширить чередующийся раздел после его создания. Поэтому отнеситесь к созданию набора со всей ответственностью.

Управление RAID-массивами и восстановление после сбоя

Управление зеркальными дисками и чередующимися массивами иногда отличается от управления другими томами, особенно когда речь идет о восстановлении после сбоя. Техники, используемые для управления RAID-массивами и восстановления после сбоя, описаны в этом разделе.

Разделение зеркального набора

Разделить зеркальный набор необходимо по одной из двух причин.

- Если один из зеркальных дисков откажет, дисковые операции могут быть продолжены. Когда пользователи будут читать и записывать данные, эти операции будут произведены с оставшимся диском. Однако нужно исправить зеркало, для этого необходимо сначала разбить зеркало, заменить отказавший диск и затем переустановить зеркало.
- Если больше не нужно зеркально отражать диск, тогда тоже необходимо разбить зеркало. Это позволит использовать дисковое пространство для других целей.

"Разбить зеркало" не означает удаление всех данных в наборе, однако перед этим лучше всего выполнить резервное копирование данных. Это гарантирует, что в случае сбоя можно восстановить данные.

В оснастке Управление дисками можно разбить зеркальный набор с помощью следующих действий:

1. Щелкните по одному из томов зеркального набора и выберите команду Разделить зеркальный том (Break Mirrored Volume).

2. Подтвердите действие, нажав кнопку Да. Если том используется, будет отображено другое предупреждение. Опять подтвердите свое намерение, нажав кнопку Да.

Операционная система Windows Server 2012 разобьет зеркало, создав два независимых тома.

Ресинхронизация и восстановление зеркального набора

Операционная система Windows Server 2012 автоматически синхронизирует зеркальные тома на динамических дисках. Однако данные на зеркальных дисках могут оказаться рассинхронизированными. Например, если один из дисков перешел в состояние Вне сети, а данные были записаны только на диск, находящийся в состоянии В сети.

Можно ресинхронизировать и восстановить зеркальные наборы, но перед этим нужно сначала восстановить набор, используя диски с тем же стилем разделов — либо с главной загрузочной записью (MBR), либо с таблицей GUID (GPT). Необходимо получить оба диска в зеркальном наборе в состоянии В сети. Состояние зеркального набора должно быть Отказавшая избыточность. Меры по ликвидации последствий, которые можно предпринять, зависят от состояния отказавшего тома:

1. Если активно состояние Отсутствует или Вне сети, убедитесь, что к диску подключено питание и он правильно подключен. Затем запустите оснастку Управление дисками, щелкните правой кнопкой мыши по отказавшему тому и выберите команду Реактивировать том (Reactivate Volume). Состояние диска должно измениться на Регенерация, а затем — на Исправен. Если том не возвращается в состояние Исправен, щелкните по этому тому и выберите действие Ресинхронизация зеркала (Resynchronize Mirror).
2. Если активно состояние В сети (Ошибки), щелкните правой кнопкой мыши по отказавшему тому и выберите команду Реактивировать том. Состояние диска должно измениться на Регенерация, а затем — на Исправен. Если том не возвращается в состояние Исправен, щелкните правой кнопкой на томе и выберите команду Ресинхронизация зеркала.
3. Если один из дисков находится в состоянии Не читается, нужно пересканировать диски системы, выбрав команду Действие | Повторить проверку дисков (Action | Rescan Disks). Если состояние диска изменится, нужно перезагрузить компьютер.
4. Если один из дисков не возвращается в состояние В сети, щелкните правой кнопкой мыши на отказавшем томе и выберите команду Удалить зеркало (Remove Mirror).

Теперь нужно создать зеркало тома на нераспределенной области свободного пространства. Если нет свободного места, его нужно создать, удалив другие тома или заменив отказавший диск.

Восстановление зеркального системного тома

для включения загрузки Отказ зеркально отраженного диска может препятствовать загрузке системы. Как правило, это происходит, когда зеркалируется системный или загрузочный том (или оба) и основной зеркальный диск отказал. В предыдущих версиях Windows нужно выполнить несколько процедур, чтобы заставить систему снова работать. В Windows Server 2012 отказ зеркала разрешить намного проще.

При зеркалировании системного тома операционная система должна добавить запись в диспетчер начальной загрузки системы, которая позволяет загружаться со вторичного зеркала.

Восстановление первичного зеркала с этой записью в файле диспетчера загрузки намного

проще, потому что все, что нужно сделать для загрузки со вторичного зеркала — это выбрать данную запись при загрузке. Если зеркалируется загрузочный том и эта запись не была создана, можно отредактировать записи диспетчера загрузки и создать ее с помощью редактора BCD (Bcdedit.exe).

Если не получается загрузиться с основного системного тома, перезагрузите систему и в меню загрузчика выберите пункт Windows Server 2012 — Secondary Plex для операционной системы, которую нужно загрузить. Система должна запуститься без проблем. После успешной загрузки со вторичного диска можно приступить к восстановлению зеркала. Нужно выполнить следующие действия:

1. Завершите работу системы и замените отказавший том или добавьте жесткий диск. Затем перезагрузите систему.
2. Разделите зеркало и заново создайте зеркало на диске, который был заменен (обычно это диск 0). Щелкните правой кнопкой мыши на оставшемся от исходного зеркала томе и выберите команду Добавить зеркало. Далее следуйте указаниям из разд. "Зеркалирование существующего тома" ранее в этой главе.
3. Если нужно, чтобы основное зеркало было на диске, который был добавлен или заменен, используйте оснастку Управление дисками, чтобы снова разделить зеркало. Убедитесь, что основному диску в исходном зеркале назначена буква диска, которая была ранее присвоена полному зеркалу. Если это не так, назначьте надлежащую букву диска.
4. Щелкните правой кнопкой мыши по исходному системному тому и выберите команду Добавить зеркало. Заново создайте зеркало.
5. Проверьте загрузочные записи в диспетчере загрузки и с помощью редактора BCD убедитесь, что для запуска системы используется исходный системный том.

Удаление зеркального набора

Используя оснастку Управление дисками, можно удалить один из томов из зеркального набора. После этого все данные на удаляемом зеркале будут удалены, а используемое пространство будет помечено как нераспределенное.

Чтобы удалить зеркальный набор, выполните следующие действия:

1. В оснастке Управление дисками щелкните правой кнопкой мыши по одному из томов зеркального набора и выберите команду Удалить зеркало (Remove Mirror). Откроется одноименное окно.
2. В окне Удалить зеркало выберите диск, с которого нужно удалить зеркало.
3. Подтвердите действие, когда появится соответствующий запрос. Все данные на удаляемом зеркале будут уничтожены.

Восстановление чередующегося массива с контролем четности

Чередующийся массив без контроля четности не отказоустойчивый. Если один из дисков набора откажет, весь массив станет неиспользуемым. Перед попыткой восстановить чередующийся массив нужно восстановить или заменить отказавший диск. Затем необходимо заново создать чередующийся набор и восстановить данные из резервной копии.

Регенерация чередующегося массива с четностью

При использовании RAID 5 можно восстановить чередующийся массив с контролем четности, если один из дисков выйдет из строя. Какой именно из дисков вышел из строя, можно понять по его состоянию: состояние массива будет изменено на Отказавшая избыточность, а состояние отдельного тома должно быть изменено на Отсутствует, Вне сети или В сети (Ошибки).

Можно восстановить диски RAID 5, но нужно перестроить массив с использованием того же стиля разделов — либо MBR, либо GPT. Необходимо, чтобы все диски в наборе RAID 5 были в состоянии В сети. Состояние массива должно быть Отказавшая избыточность.

Предпринимаемые меры зависят от состояния отказавшего диска.

- Если активно состояние Отсутствует или Вне сети, убедитесь, что к диску подключено питание и он правильно подключен. Затем запустите оснастку Управление дисками, щелкните правой кнопкой мыши по отказавшему тому и выберите команду Реактивировать том. Состояние диска должно измениться на Регенерация, а затем на Исправен.
- Если состояние диска не вернулось на Исправен, щелкните правой кнопкой мыши по тому и выберите команду Регенерация четности (Regenerate Parity).
- Если активно состояние В сети (Ошибки), щелкните правой кнопкой мыши по отказавшему тому и выберите команду Реактивировать том. Состояние диска должно быть изменено на Регенерация, а затем на Исправен. Если состояние диска не вернулось на Исправен, щелкните правой кнопкой по тому и выберите команду Регенерация четности.
- Если состояние одного из дисков — Не читается, нужно пересканировать диски, используя команду Действие | Повторить проверку дисков (Action | Rescan Disks). Если состояние диска не изменится, перезагрузите компьютер.

– Если после этого один из дисков все еще Вне сети, нужно восстановить отказавший регион массива RAID 5. Щелкните правой кнопкой мыши на отказавшем томе и выберите команду Удалить том (Remove Volume). Теперь нужно выбрать нераспределенное пространство на другом динамическом диске для использования в массиве RAID 5. Это пространство должно быть больше, чем область, которую нужно восстановить, и не может быть на диске, который уже используется в массиве RAID 5. Если недостаточно места, команда Восстановить том (Repair Volume) будет недоступна и необходимо получить свободное пространство путем удаления других томов или замены отказавшего диска.

Если возможно, сделайте резервную копию перед выполнением этой процедуры. Это гарантия, что в случае проблем можно будет восстановить данные.

Стандартизированное управление хранилищами

Стандартизированное управление хранилищами фокусируется на самих томах хранилища, а не на физической разметке, полагаясь на аппаратные средства для обработки особенностей архитектуры для избыточности данных и частей диска, которые представлены, как используемые диски. Это означает, что расположением физических дисков управляет подсистема внешней памяти, а не операционная система.

Знакомство со стандартизированным управлением хранилищами

При работе со стандартизированным хранилищем физическое расположение дисков абстрагировано. Здесь "диск" может быть логическим указателем на часть подсистемы внешней памяти (виртуальный диск) или физический диск. Это означает, что диск просто становится модулем хранилища, а тома создаются для выделения места на дисках для файловых систем.

Можно поместить в пул все свободное место на дисках так, чтобы модули хранилища (виртуальные диски) могли быть выделены из этого пула по мере необходимости. В свою очередь, эти модули хранилища распределяются на тома для выделения пространства и создания файловых систем, доступных для использования.

Технически, такое хранилище называется пулом носителей, а виртуальные диски в пределах пула — пространствами хранилища. Этот массив "дисков" можно использовать для создания единственного пула хранения данных, помещая все диски в пул, или же создать несколько пулов, распределив имеющиеся диски между пулами.

Когда мы говорим о подсистеме внешней памяти, на самом деле мы имеем дело с трехуровневой архитектурой. На уровне 1 расположением физических дисков управляет подсистема внешней памяти. Система хранения, вероятно, будет использовать некоторую форму RAID для обеспечения избыточности и отказоустойчивости. На уровне 2 созданные массивами виртуальные диски доступны для серверов. Серверы рассматривают диски как хранилище, которое

может быть выделено. ОС Windows Server может применить какой-то из уровней программного RAID или другие способы избыточности для отказоустойчивости. На уровне 3 сервер создает тома на виртуальных дисках, а на них уже создаются файловые системы для хранения файлов и данных.

Работа со стандартизированным хранилищем

Для использования стандартизированного хранилища нужно добавить компонент Стандартизированное управление хранилищами Windows (Windows Standards-Based Storage Management) на серверы. Если сервер настроен с ролью Файловые службы и службы хранилища (File Services And Storage), Стандартизированное управление хранилищами Windows добавляет компоненты и обновляет диспетчер серверов опциями для работы со стандартизированными томами. Возможно, также нужно сделать следующее:

- добавить службу роли Дедупликация данных (Data Deduplication), если необходимо включить дедупликацию данных;
- добавить службы ролей Сервер цели iSCSI (iSCSI Target Server) и Поставщик целевого хранилища iSCSI (iSCSI Target Storage Provider), если нужно размещать виртуальные диски iSCSI.

После настройки сервера надлежащим для производственной среды способом можно выбрать узел Файловые службы и службы хранилища (File And Storage Services) в диспетчере серверов для работы с томами хранилища — там находятся дополнительные функции.

Подузел Серверы (Servers) содержит файловые серверы, которые были настроены для стандартизированного управления хранилищами.

Подузел Тома (Volumes), предоставляющий информацию о выделенном хранилище на каждом сервере. Здесь выводится, как настроены тома и сколько свободного пространства есть на томе. Тома выводятся независимо от того, основаны ли они на физических или виртуальных дисках. Щелкните правой кнопкой мыши на томе для отображения опций управления.

- Настройка дедупликации данных (Configure Data Deduplication) — позволяет включить и настроить дедупликацию данных на NTFS-томах. Если эта опция доступна, можно также впоследствии использовать ее для отключения дедупликации.
- Удалить том (Delete Volume) — используется для удаления тома. Используемое пространство будет помечено как нераспределенное на соответствующем диске.
- Расширить том (Extend Volume) — позволяет расширить том на все нераспределенное пространство на соответствующем диске.
- Форматировать (Format) — позволяет создать новую файловую систему на томе, которая перезапишет существующий том.
- Управление буквой диска или путями доступа (Manage Drive Letter) — позволяет изменить букву диска или пути доступа, связанные с томом.

- Создать виртуальный диск iSCSI (New iSCSI Virtual Disk) — позволяет создать новый виртуальный диск iSCSI, который будет сохранен на томе.
- Новый общий ресурс (New Share) — позволяет создать общий ресурс SMB (Server Message Block) или NFS (Network File System) на томе.
- Свойства — отображает информацию о типе тома, файловой системе, исправности, емкости, используемом пространстве и свободном пространстве. Можно также использовать окно Свойства для установки метки тома.
- Исправить ошибки файловой системы (Repair File System) — позволяет исправить ошибки, обнаруженные во время оперативного (онлайн) сканирования файловой системы.
- Проверить файловую систему на наличие ошибок (Scan File System For Errors) — осуществляет оперативное сканирование файловой системы. Хотя Windows пытается восстановить любые найденные ошибки, некоторые ошибки могут быть исправлены только с помощью этой процедуры. Подузел Диски выводит диски, доступные на каждом сервере, при этом сообщается общая емкость, нераспределенное пространство, стиль раздела, подсистема и тип шины. Диспетчер серверов пытается различать физические и виртуальные диски, показывая метку виртуального диска и исходную подсистему хранения. Щелкните правой кнопкой мыши на диске, чтобы увидеть опции управления:
- Подключить (Bring Online) — перевести диск в состояние В сети, что сделает его доступным для использования;
- Отключить (Take Offline) — перевести диск в состояние Вне сети, что сделает его недоступным;
- Сбросить диск (Reset Disk) — полностью сбросить диск, что удалит все тома на диске и все доступные данные на нем;
- Создать том (New Volume) — создать новый том на диске.

Создание пулов носителей и распределение пространства

В диспетчере серверов можно работать с пулами носителей и распределить пространство на них. Для этого перейдите в узел Файловые службы и службы хранилища | Пулы носителей (File And Storage Services | Storage Pools). В подразделе Пулы носителей (Storage Pools) выводятся доступные пулы, виртуальные диски, созданные внутри пулов, и доступные физические диски. Помните: диски, представленные как физически, могут оказаться на самом деле виртуальными дисками LUN от подсистемы хранения.

Работа с пулами носителей — многоэтапный процесс:

1. Администратор создает пулы носителей, чтобы объединить доступное пространство на одном или более дисках.
2. Администратор создает пространство из этого пула для создания одного или более виртуальных дисков.

3. Администратор создает один или более томов на каждом виртуальном диске для распределения хранилища для файловых систем.

Следующие разделы подробно описывают каждый этап.

Создание пространства хранилища

Пулы носителей позволяют объединять свободное место на дисках так, чтобы модули хранения (виртуальные диски) могли быть распределены из этого пула. Чтобы создать пул носителей, в системе должен быть по крайней мере один неиспользуемый диск, а также подсистема хранилища для его управления. Эта подсистема может включать функцию Storage Spaces или подсистему, связанную с присоединенным хранилищем.

Каждый физический диск, выделенный пулу, может использоваться одним из трех способов:

- как хранилище данных, доступное для использования;
- как хранилище данных, которое может быть вручную выделено для использования;
- как горячая замена в случае, если диск в пуле откажет или будет удален из подсистемы.

Можно создать пул носителей, выполнив следующие действия:

1. В диспетчере серверов выберите узел Файловые службы и службы хранилища, а затем подузел Пулы носителей.
2. Выберите меню Задачи (Tasks) на панели Пулы носителей и затем выберите команду Создать пул носителей (New Storage Pool). Будет запущен мастер создания пула хранения (New Storage Pool Wizard). Если мастер отобразит страницу Перед началом работы (Before You Begin), просто нажмите кнопку Далее.
3. На странице Укажите имя и подсистему пула носителей (Specify A Storage Pool Name And Subsystem) введите имя и описание пула носителей. Затем выберите исходный пул, с которым нужно работать. Исходный пул (primordial pool) — это просто группа дисков, управляемая и доступная определенному серверу через подсистему хранения. Нажмите кнопку Далее. Выберите исходный пул для сервера, с которым нужно связать пул и для которого нужно распределить хранилище. Например, если настраиваете хранилище для CorpServer38, выберите исходный пул, доступный для CorpServer38.
4. На странице Выбор физических дисков для пула носителей (Select Physical Disks For The Storage Pool) выберите неиспользуемые физические диски, которые станут частью пула носителей, а затем укажите тип выделения каждого диска. Пул носителей должен иметь более одного диска для использования функций зеркалирования и четности, которые используются для защиты данных в случае ошибки или сбоя. Когда устанавливаете значение Выделение (Allocation), помните о следующем:
   - Автоматически (Data Store) — диск выделяется пулу и делается доступным для использования;

- Вручную (Manual) — диск выделяется пулу, но он будет недоступным, пока администратор явно этого не разрешит;
- Горячий резерв (Hot Spare) — диск будет выделен пулу как горячий резерв, он будет использоваться, если другой диск в пуле откажет или будет удален из подсистемы.

5. Как только будете готовы продолжить, нажмите кнопку Далее. После подтверждения установленных параметров нажмите кнопку Создать (Create). Мастер показывает ход выполнения создания пула. Когда мастер закончит создавать пул, будет отображена страница Просмотр результатов (View Results). Просмотрите ее, чтобы убедиться в успешном завершении всех фаз, а затем нажмите кнопку Закрыть. Если на каком-то этапе конфигурации произошел сбой, определите причину отказа и примите меры по ликвидации последствий, а затем заново повторите эту процедуру.

Создание виртуального диска в пространстве хранилища

После создания пула носителей можно выделить пространство из пула виртуальным дискам, которые будут доступны серверам. Каждый физический диск в пуле может использоваться одним из трех способов:

- как хранилище данных, доступное для использования;
- как хранилище данных, которое может быть вручную выделено для использования;
- как горячая замена в случае, если диск в пуле откажет или будет удален из подсистемы.

Если в пуле носителей только один диск, будет только одна опция выделения пространства на этом диске — создание виртуальных дисков с простой (Simple) разметкой. Простая разметка не защищает от отказа диска. Если в пуле носителей есть несколько дисков, можно использовать следующие опции.

- Mirror — при выборе разметки Mirror данные дедуплицируются на дисках с использованием техники зеркалирования, подобной той, которая была ранее рассмотрена в этой главе. Однако техника зеркалирования более сложна тем, что данные зеркалируются на два или три диска за один раз. У этого метода есть свои преимущества и недостатки. Здесь, если в пространстве хранилища есть два или три диска, гарантируется полная защита от сбоя одного диска, а если в пространстве находится пять или более дисков, гарантируется защита от одновременного отказа двух дисков. Недостаток заключается в том, что зеркалирование уменьшает полезную емкость на 50%. Например, если зеркально отражаются два диска по 1 Тбайт каждый, можно использовать только 1 Тбайт для хранения данных.
- Parity — при выборе этого типа разметки данные и информация четности чередуются по физическим дискам с использованием метода чередования с контролем четности, подобно тому, который был ранее рассмотрен в этой главе. Подобно стандартному чередованию с

контролем четности, у этого метода есть преимущества и недостатки. Нужны как минимум три диска, чтобы полностью защитить свою систему от сбоя одного диска. С чередованием тоже будут потери емкости, но не такие большие, как с зеркалированием.

Можно создать виртуальный диск в пуле носителей, выполнив следующие действия:

1. В диспетчере серверов выберите узел Файловые службы и службы хранилища, а затем подузел Пулы носителей.
2. На панели Виртуальные диски (Virtual Disks) выберите меню Задачи (Tasks), а из появившегося списка — команду Создать виртуальный диск (New Virtual Disk). Будет запущен мастер создания виртуальных дисков (New Virtual Disk Wizard).
3. На странице Выбор пула носителей (Storage Pool) выберите пул носителей, в котором нужно создать виртуальный диск, и нажмите кнопку Далее. Для каждого доступного пула выводится сервер, которым он управляется. Убедитесь, что пул содержит достаточно свободного пространства для создания виртуального диска. Выберите пул носителей для сервера, с которым нужно связать виртуальный диск. Например, если настраиваете хранилище для CorpServer38, нужно выбрать пул носителей, который доступен серверу CorpServer38.
4. На странице Назначение имени виртуального диска (Specify The Virtual Disk Name) введите имя и описание виртуального диска. Нажмите кнопку Далее.
5. На странице Выбор структуры хранилища (Select The Storage Layout) выберите разметку хранилища, соответствующую требованиям надежности и избыточности. Для пулов, состоящих из одного диска, доступна только простая разметка (Simple). Если есть несколько дисков в пуле, то можно выбрать разметку Simple, Mirror или Parity. Нажмите кнопку Далее.
6. На странице Указание типа подготовки (Specify The Provisioning Type) выберите тип подготовки. Можно выбрать Тонкая (Thin) или Фиксированный (Fixed). При тонкой подготовке том использует пространство пула по мере необходимости, в зависимости от размера тома. Если выбрать тип Фиксированный, у тома будет фиксированный размер и он будет использовать пространство из пула, равное размеру тома. Нажмите кнопку Далее.
7. На странице Указание размера виртуального диска (Specify The Size Of The Virtual Disk) используйте предоставленные опции для указания размера виртуального диска. Если выбрать флажок Создать максимально большой виртуальный диск в пределах указанного размера (Create The Largest Virtual Disk Possible), то созданный диск захватит все доступное пространство. Например, если создается фиксированный диск размером 2 Тбайт с простой разметкой и только 1,5 Тбайт дискового пространства доступно, будет создан фиксированный диск размером 1,5 Тбайт.

Помните, что если диск зеркалируется или чередуется, он может использовать больше свободного пространства, чем будет указано.

8. Когда будете готовы продолжить, нажмите кнопку Далее. После подтверждения установленных параметров нажмите кнопку Создать. Мастер окажет ход выполнения процесса создания диска. Как только мастер закончит создавать диск, будет отображена страница Просмотр результатов. Просмотрите подробности и убедитесь, что все этапы были успешно выполнены. Если на каком-то этапе конфигурации произошел сбой, определите причину отказа и примите меры по ликвидации последствий, а затем заново повторите эту процедуру.
9. Нажмите кнопку Закрыть, будет автоматически запущен мастер создания томов (New Volume Wizard). Используйте его для создания тома, как описано в разд. "Создание стандартного тома" далее в этой главе.

Создание стандартного тома

Стандартные тома могут быть созданы как на физических, так и на виртуальных дисках.

Для создания тома используется один и тот же способ, независимо от того, как диск представлен серверу. Это позволяет создавать стандартные тома на внутренних дисках сервера, на виртуальных дисках в подсистеме хранения, доступной на сервере, и на виртуальных дисках iSCSI, доступных на сервере. Если нужно добавить дедупликацию данных на сервер, можно включить дедупликацию для стандартных томов, созданных для того сервера.

Для создания стандартного тома выполните следующие действия:

1. Запустите мастер создания томов (New Volume Wizard). Этот мастер автоматически запускается после создания пространства хранилища. Запустить его вручную можно одним из двух способов:
   - в подузле Диски на панели диски выводятся все доступные диски. Выберите диск, с которым нужно работать, а затем из меню Задачи выберите команду Создать том;
   - в подузле Пулы носителей на панели виртуальные диски (Virtual disks) выводятся все доступные виртуальные диски. Выберите диск, с которым нужно работать, а затем из списка Задачи выберите команду Создать том.
2. На странице Выбор сервера или диска (Select the server and disk) выберите сервер, на котором находится хранилище, а затем — диск, на котором нужно создать том, и нажмите кнопку Далее. Если только что создали пространство хранения, мастер создания томов автоматически выберет нужный сервер и диск, поэтому нужно просто нажать кнопку Далее.
3. На странице Выбор размера тома (Specify the size of the volume) используйте предоставленные параметры для установки размера тома. По умолчанию размер тома равен максимальному доступному пространству на диске. Нажмите кнопку Далее.

4. На странице Назначение букве диска или папке (Assign to a drive letter or folder) укажите, что нужно назначить — букву диска или папку, и нажмите кнопку Далее. Можно использовать следующие параметры:
   - Буква диска (Drive letter) — для назначения буквы, выберите этот параметр и укажите доступную букву из предоставленного списка;
   - Следующая папка (Following folder) — для назначения пути, выберите этот параметр и введите путь к существующей папке на NTFS-диске или же используйте кнопку Обзор для поиска или создания папки;
   - Не назначать букве диска или папке (Don't assign to a drive letter or drive path) — том будет создан без назначения букве диска или папке. При необходимости можно назначить том букве диска или папке позже.
5. На странице Выбор параметров файловой системы (Select file system settings) укажите, как том должен быть отформатирован:
   - Файловая система — тип файловой системы, например NTFS или ReFS;
   - Размер кластера — размер кластера для файловой системы. Это базовая единица, с помощью которой распределяется дисковое пространство. Размер кластера по умолчанию основывается на размере тома и устанавливается динамически до форматирования. Чтобы переопределить эту функцию, можно установить размер кластера в определенное значение;
   - Метка тома — метка, т. е. название тома.
6. Если выбрана файловая система NTFS и добавлена дедупликация данных на сервер, можно включить и настроить дедупликацию данных. Как только будете готовы продолжить, нажмите кнопку Далее.
7. После подтверждения установленных параметров нажмите кнопку Создать. Мастер покажет ход выполнения создания тома. Когда мастер закончит создавать том, он отобразит страницу Просмотр результатов. Просмотрите ее, чтобы убедиться в успешном завершении всех этапов. Если на каком-то этапе произошел сбой, определите причину сбоя и устраните ее перед повторением этой процедуры.
8. Нажмите кнопку Закрыть.

Управление существующими разделами и дисками

Оснастка Управление дисками предоставляет множество способов управления существующими разделами и дисками. Можно назначать буквы дисками, удалять разделы, устанавливать активный раздел и т. д. Дополнительно ОС Windows Server 2012 предоставляет другие утилиты для выполнения общих задач, таких как форматирование тома в NTFS, проверка диска на наличие ошибок, очистка неиспользуемого пространства диска.

Windows Vista, как и все последующие версии Windows, поддерживает сменные носители, которые могут использовать NTFS-тома. Эта возможность позволяет форматировать в NTFS флешки (USB-диски) и другие подобные устройства. В

результате гарантируется защита от потери данных при извлечении сменного носителя, отформатированного в NTFS.

Назначение буквы диска или путей

Можно назначить диску одну букву или один или более путей диска, при условии, что пути диска смонтированы на дисках NTFS. Дискам может быть не назначена ни буква диска, ни путь. Такие диски рассматриваются как размонтированные, и их можно смонтировать позже, присвоив букву диска или путь. Перед перемещением диска на другой компьютер его нужно размонтировать.

ОС Windows не может изменить букву системного, загрузочного томов или тома, на котором находится файл подкачки. Для изменения буквы диска системного или загрузочного тома нужно редактировать реестр, как описано в статье Microsoft Knowledge Base 223188 (support.microsoft.com/kb/223188/). Перед изменением буквы диска тома, на котором находится файл подкачки, нужно переместить файл подкачки на другой том.

Для управления буквами дисков и путями щелкните на диске, который нужно настроить в оснастке Управление дисками, и выберите команду Изменить букву диска или путь к диску (Change Drive Letter And Paths). Откроется диалоговое окно. Теперь можно сделать следующее:

- добавить путь диска — нажмите кнопку Добавить, выберите переключатель Подключить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder) и введите путь к существующей папке или нажмите кнопку Обзор для поиска или создания папки;
- удалить путь диска — выберите путь диска, который нужно удалить, нажмите кнопку Удалить, а затем — кнопку Да;
- назначить букву диска — нажмите кнопку Добавить, установите переключатель Назначить букву диска (Assign The Following Drive Letter), а затем выберите доступную букву, чтобы назначить ее диску;
- изменить букву диска — выберите текущую букву, а затем нажмите кнопку Изменить (Change), установите переключатель Назначить букву диска и выберите другую букву из списка;
- удалить букву диска — выберите текущую букву диска и нажмите кнопку Удалить, а затем — кнопку Да.

Если попытаетесь изменить букву диска, который в данный момент используется, Windows Server 2012 отобразит предупреждение. Нужно закрыть программы, которые используют диск, и попытаться снова или же разрешить оснастке Управление дисками принудительно изменить букву, нажав кнопку Да в предупреждении.

Изменение или удаление метки диска

Метка тома — это текстовый дескриптор диска. При использовании FAT максимальный размер метки — 11 символов, разрешено использовать пробелы. В NTFS максимальный размер метки тома — 32 символа. Хотя FAT не

разрешает использовать некоторые специальные символы (* / \ [ ] : ; | = , . + " ? < >), в NTFS не будет никаких проблем с такими символами.
Поскольку метка тома отображается при доступе к диску в разных утилитах Windows Server 2012, в том числе в Проводнике, она может использоваться для предоставления информации о содержимом диска. Можно изменить или удалить метку тома, используя оснастку Управление дисками или Проводник.
Используя оснастку Управление дисками, можно изменить метку так:

1. Щелкните правой кнопкой мыши на разделе и затем выберите команду Свойства.
2. На вкладке Общие окна Свойства введите новую метку тома в предоставленное текстовое поле или удалите существующую метку. Нажмите кнопку OK.

Используя Проводник, можно изменить метку так:

1. Щелкните правой кнопкой мыши на значке диска и выберите команду Свойства.
2. На вкладке Общие окна Свойства введите новую метку тома в предоставленное текстовое поле или удалите существующую метку. Нажмите кнопку OK.

Удаление разделов и дисков

Для изменения конфигурации диска, дисковое пространство которого полностью распределено, нужно удалить существующие разделы и логические диски. Удаление раздела или диска удаляет связанную файловую систему, и все данные в файловой системе будут потеряны. Перед удалением раздела или диска нужно сделать резервную копию всех файлов и каталогов, содержащихся на этом разделе или диске.
Для защиты целостности системы нельзя удалить системный или загрузочный раздел. Однако Windows Server 2012 позволяет удалить активный раздел или том, если он не назначен как загрузочный или системный. Убедитесь, что удаляемый раздел или том не содержит важных данных или файлов.
Можно удалить первичный раздел, том или диск с помощью следующих действий:

1. В оснастке Управление дисками щелкните правой кнопкой мыши по разделу, тому или диску, который нужно удалить, а затем выберите команду Проводник (Explore). Используя Проводник, переместите все данные на другой том или проверьте существующие резервные копии, чтобы убедиться, что данные сохранены надлежащим образом.
2. В оснастке Управление дисками щелкните правой кнопкой мыши по разделу, тому или диску, а затем выберите команду Удалить раздел (Delete Partition), Удалить том (Delete Volume) или Удалить логический диск (Delete Logical Drive) соответственно.
3. Подтвердите удаление, нажав кнопку Да.

Действия по удалению расширенного раздела слегка отличаются от удаления первичного раздела или логического диска. Для удаления расширенного раздела выполните такие действия:

1. Удалите все логические диски, как было описано ранее.
2. Выберите область расширенного раздела и удалите ее.

Преобразование тома в NTFS

ОС Windows Server 2012 предоставляет утилиту для преобразования томов FAT в NTFS. Эта утилита называется Convert (Convert.exe) и расположена в папке %SystemRoot%. При конвертировании тома с использованием этой утилиты структура файлов и каталогов сохраняется, и данные не будут потеряны. Помните, однако, что в Windows Server 2012 нет утилиты для обратного преобразования из NTFS в FAT. Единственный способ преобразовать раздел с NTFS в FAT — удалить его и создать на его месте FAT-том.

Синтаксис утилиты Convert

Утилита Convert запускается в командной строке. Если нужно конвертировать диск, используйте следующий синтаксис:
convert volume /FS:NTFS
Здесь volume — буква диска с двоеточием, путь диска или имя тома. Например, если нужно преобразовать диск D: в NTFS, используйте команду:
convert D: /FS:NTFS
Если у тома есть метка, программа попросит ее ввести. Программа не будет просить ввести метку, если она не установлена.
Полный синтаксис программы Convert следующий:
convert volume /FS:NTFS [/V] [/X] [/CvtArea:filename] [/NoSecurity]
Параметры программы следующие:

- volume — задает том, с которым нужно работать;
- /FS:NTFS — преобразование в NTFS;
- /V — включает подробный режим;
- /X — принудительное размонтирование тома перед преобразованием (если необходимо);
- /CvtArea:filename — устанавливает имя непрерывного файла в корневом каталоге для резервирования файла для системных файлов NTFS;
- /NoSecurity — к преобразуемым файлам будет разрешен доступ для всех пользователей.

Еще один пример вызова Convert:
convert C: /FS:NTFS /V

Использование утилиты Convert

Перед применением утилиты Convert определите, используется ли раздел в качестве активного загрузочного раздела или системного раздела, содержащего операционную систему. Можно преобразовать активный загрузочный раздел в NTFS. Выполнение этой операции требует, чтобы система получила эксклюзивный доступ к этому разделу, который может быть получен только во время запуска. Таким образом, если попытаетесь преобразовать активный загрузочный раздел в NTFS, ОС Windows Server 2012 отобразит подсказку,

позволяющую запланировать преобразование при следующем запуске системы. Если нажать кнопку Да, можно перезапустить систему, чтобы начать процесс преобразования.
Часто нужно перезагружать систему несколько раз, чтобы полностью завершить преобразование активного загрузочного раздела. Не паникуйте. Позвольте системе завершить преобразование.
Перед тем как утилита Convert преобразует диск в NTFS, она проверит, достаточно ли на диске свободного места для осуществления преобразования. Вообще говоря, Convert требует 25% свободного дискового пространства от общей емкости используемого пространства.
Например, если на диске хранится 200 Гбайт данных, утилите Convert нужно около 50 Гбайт свободного пространства. Если на диске не хватает свободного пространства, Convert прервет процесс преобразования и сообщит о том, что нужно освободить дополнительное место на диске. С другой стороны, если на диске достаточно места, Convert начнет процесс преобразования, который занимает несколько минут (или чуть больше для больших дисков). Будьте терпеливы. Не нужно открывать файлы или запускать приложения на диске, пока идет процесс преобразования.
Можно использовать параметр /CvtArea для улучшения производительности тома путем
резервирования пространства для главной файловой таблицы (Master File Table, MFT). Данная опция помогает предотвратить фрагментацию MFT. Как? Со временем объем MFT может превысить размер дискового пространства, выделенного для нее. В этом случае операционная система должна расширить MFT на другие области диски. Несмотря на то, что утилита оптимизации дисков может дефрагментировать MFT, она не способна переместить первый раздел MFT, и маловероятно, что после MFT будет существовать свободное пространство, поскольку оно будет заполнено данными файла.
Чтобы предотвратить фрагментацию в некоторых случаях, нужно зарезервировать больше свободного пространства, чем резервируется по умолчанию (12,5% размера раздела или тома). Например, можно увеличить размер MFT, если том будет содержать много маленьких файлов (или файлов среднего раздела), а не большие файлы. Чтобы указать резервируемое пространство, можно использовать утилиту FSUtil для создания специального файла-заполнителя, размер которого равен размеру требуемого резервируемого пространства для MFT. Конвертировать том в NTFS и указать имя файла-заполнителя можно опцией
/CvtArea.
В следующем примере утилита FSUtil используется для создания заполнителя размером около 1,5 Гбайт (1 500 000 000 байтов) с именем Temp.txt:
fsutil file createnew c:\temp.txt 1500000000
Чтобы использовать этот файл-заполнитель для MFT при преобразовании диска C: в NTFS, нужно ввести следующую команду:
convert c: /fs:ntfs /cvtarea:temp.txt

Заметьте, что файл-заполнитель создается на разделе или томе, который преобразуется. Во время процесса преобразования файл будет перезаписан метаданными NTFS, и любое неиспользуемое место в файле будет зарезервировано для будущего использования MFT.

Изменение размера раздела и тома

Операционная система Windows Server 2012 не использует загрузчик Ntldr и файл Boot.ini для загрузки операционной системы. Вместо этого у Windows Server 2012 есть предустановочная среда, в которой используется диспетчер начальной загрузки Windows (Windows Boot Manager) для управления запуском системы, загружающий выбранное загрузочное приложение. Диспетчер начальной загрузки наконец-то освобождает операционную систему от зависимости от MS-DOS, так что можно использовать диски по-новому. В Windows Server 2012 можно сжимать или расширять базовые или динамические диски. Для этого применяется либо оснастка Управление дисками, либо утилита DiskPart. Нельзя сжать или расширить чередуемые, зеркальные и чередуемые с контролем четности тома.

При расширении тома конвертируются области нераспределенного пространства и затем добавляются к существующему тому. Для составных томов на динамических дисках пространство можно взять с любого доступного динамического диска, не только с того, где том был создан. Поэтому можно комбинировать области свободного пространства на разных дисках и использовать их для увеличения размера существующего тома.

Перед расширением тома помните о нескольких ограничениях. Можно расширить простой и составной тома, только если они форматированы в NTFS. Нельзя расширить чередующиеся тома. Также нельзя расширить тома, если они не форматированы или отформатированы как FAT. Нельзя также расширить системный или загрузочный тома независимо от их конфигурации. Можно сжать простой или составной том так:

1. В оснастке Управление дисками щелкните правой кнопкой мыши по тому, который нужно сжать, и выберите команду Сжать том (Shrink Volume). Эта команда доступна, только если том соответствует описанным ранее критериям.
2. В окне Сжать (Shrink) (рис. 11.9) введите размер сжимаемого пространства. Это окно предоставляет следующую информацию:
   - Общий размер до сжатия (МБ) (Total size before shrink in MB) — общий размер тома в мегабайтах. Это размер форматированного тома;
   - Доступное для сжатия пространство (МБ) (Size of available shrink space in MB) — размер пространства, доступного для сжатия. Это не общее свободное пространство тома, а общее пространство, которое может быть удалено, исключая данные, зарезервированные для MFT, файлов подкачки, временных файлов и т. д.;
   - Размер сжимаемого пространства (МБ) (Enter the amount of space to shrink in MB) — пространство, которое может быть удалено из тома. Начальное значение по умолчанию равно предыдущему значению. Для

оптимальной производительности нужно убедиться, что на сжимаемом диске останется хотя бы 10% свободного пространства после операции сжатия; Общий размер после сжатия (МБ) (Total size after shrink in MB) — выводит, какой размер будет у тома после сжатия (в мегабайтах). Это и есть новый размер отформатированного тома.

3. Нажмите кнопку Сжать (Shrink) для сжатия тома.

Расширить простой или составной том можно так:

1. В оснастке Управление дисками щелкните правой кнопкой мыши на томе, который нужно расширить, и выберите команду Расширить том (Extend Volume). Эта команда будет доступна, только если том соответствует описанным ранее критериям, и на одном или нескольких динамических дисках доступно свободное пространство.
2. В окне приветствия мастера расширения тома (Extend Volume Wizard) нажмите кнопку Далее.
3. На странице Выбор дисков выберите диск или диски, с которых нужно взять свободное пространство. Будут автоматически выбраны все используемые тома дисков. По умолчанию будет выбрано все используемое пространство на тех дисках.
4. Для динамических дисков можно указать дополнительное пространство, которое нужно использовать на других дисках, так:
   - выберите диск из списка Доступно и нажмите кнопку Добавить для добавления диска в список Выбраны;
   - выберите каждый диск в списке Выбраны, а затем в списке Выберите размер выделяемого пространства (МБ) (Select The Amount Of Space In MB) укажите размер неиспользуемого пространства, которое нужно добавить к выбранному диску.
5. Нажмите кнопку Далее, после чего просмотрите параметры и нажмите кнопку Готово.

Автоматическое исправление ошибок диска

Операционная система Windows Server 2012 содержит дополнительные функции, сокращающие число ручных операций по обслуживанию дисков:

- транзакционная NTFS;
- самовосстанавливающаяся NTFS.

Транзакционная NTFS позволяет производить файловые операции на NTFS-томе при помощи транзакций. Это означает, что программы могут использовать транзакцию для группировки операций над файлами и реестром. Пока транзакция активна, изменения не видны вне транзакции. Изменения фиксируются и записываются на диск только, если транзакция успешно завершена. Если произошел сбой транзакции или она была выполнена не полностью, происходит откат работы транзакции для восстановления файловой системы в состояние, предшествующее транзакции.

Файловая система ReFS (Resilient File System) содержит еще более продвинутые транзакционные и самовосстанавливающиеся функции. В ReFS используется несколько фоновых процессов для автоматического поддержания

целостности диска. Процесс scrubber проверяет диск на наличие несогласованности и ошибок. Если обнаружена ошибка, процесс восстановления локализует проблемы и выполняет автоматическое исправление. В редком случае, когда на физическом диске есть поврежденные секторы, ReFS запускает процесс восстановления, чтобы отметить поврежденные секторы и удалить их из файловой системы — и все это без размонтирования тома.

Транзакции, охватывающие несколько томов, координируются диспетчером транзакций ядра (Kernel Transaction Manager, KTM). KTM поддерживает независимое восстановление томов, если произойдет сбой транзакции. Локальный диспетчер ресурсов для тома обслуживает отдельный журнал транзакций и отвечает за поддержку потоков транзакций, отдельных от потоков, осуществляющих работу с файлом.

Традиционно раньше нужно было использовать утилиту ChkDsk для исправления ошибок и противоречий в NTFS-томах на диске. Поскольку этот процесс может разрушить доступность Windows-систем, ОС Windows Server 2012 применяет самовосстанавливающуюся NTFS, чтобы защитить файловые системы, и не требует использования отдельных инструментов для исправления проблем. Поскольку большая часть процесса самовосстановления выполняется автоматически, нужно обслуживать том вручную лишь в том случае, если будет получено уведомление от операционной системы, что проблема не может быть исправлена автоматически. Если произойдет такая ошибка, Windows Server 2012 уведомит о проблеме и предоставит возможные решения.

У самовосстановления NTFS есть много преимуществ по сравнению с ChkDsk.

- ChkDsk требует эксклюзивный доступ к тому, следовательно, системные и загрузочные тома могут быть проверены только при запуске операционной системы. А с самовосстановлением NTFS файловая система всегда доступна, и в большинстве случаев не нужно переводить ее в автономный режим для коррекции ошибок.
- Самовосстановление NTFS пытается сохранить как можно больше данных с учетом типа обнаруженной проблемы. Также самовосстановление сокращает число отклоненных запросов подключения файловой системы из-за несоответствий во время перезапуска или несоответствий на томе, который работает в оперативном режиме. Во время перезапуска самовосстановление немедленно восстанавливает том так, что он может быть смонтирован.
- Самовосстановление файловой системы NTFS уведомляет об изменениях, внесенных в том в ходе восстановления, с помощью механизмов Chkdsk.exe, уведомлений каталогов и записей журнала USN. Эта функция также позволяет авторизованным пользователям и администраторам контролировать операции восстановления. В число этих возможностей входят инициирование проверки дисков, ожидание завершения восстановления и получение сведений о ходе восстановления.

– Функция самовосстановления NTFS может восстановить том, если загрузочный сектор читаем, но невозможно идентифицировать NTFS-том. В этом случае нужно запустить автономную утилиту, которая восстановит загрузочный сектор, и затем разрешить самовосстановление NTFS для начала восстановления.

Несмотря на то, что функция самовосстановления NTFS — потрясающее улучшение, время от времени придется вручную проверить целостность диска. В этих случаях можно использовать Chkdsk.exe для обнаружения проблем на томах FAT, FAT32, exFAT и NTFS и восстановления (в случае необходимости). Несмотря на то, что ChkDsk может проверить и исправить много типов ошибок, утилита прежде всего ищет несогласованности в файловой системе и в ее связанных метаданных. Один из способов, с помощью которых проверка диска обнаруживает ошибки, — это сравнение битового массива тома с секторами диска, назначенными файлам в файловой системе. Вне этого полноценность утилиты проверки диска ограничена. Например, утилита не может восстановить поврежденные данные в файлах, которые, возможно, структурно не повреждены.

Как часть автоматизированного обслуживания, Windows Server 2012 выполняет превентивное сканирование томов NTFS. Как и с другим автоматизированным обслуживанием, Windows сканирует диски, запуская утилиту Проверка диска в 3:00, если компьютер работает от сети питания и операционная система неактивна. В противном случае Windows сканирует диски в следующий раз, когда операционная система не активна и компьютер подключен к сети питания. Несмотря на то, что автоматизированное обслуживание инициировало проверку диска, процесс вызова и управления утилитой Проверка диска обрабатывается отдельной задачей. В Планировщике заданий находится задача ProactiveScan в библиотеке планировщика (Microsoft\Windows\Chkdsk), и можно получить подробную информацию о выполнении этой задачи на вкладке Журнал (History).

Автоматическое обслуживание основано на диагностике Windows. По умолчанию Windows периодически осуществляет регламентное обслуживание в 3:00, если компьютер работает от сети питания и операционная система неактивна. В противном случае Windows, обслуживание будет запущено в следующий раз, когда компьютер работает от сети питания и операционная система простаивает. Поскольку обслуживание запускается только когда операционная система простаивает, обслуживанию разрешено работать в фоновом режиме в течение максимум трех дней. Это позволяет Windows завершать сложные задачи по обслуживанию автоматически. Задачи обслуживания включают обновление программного обеспечения, проверку безопасности, диагностику системы, проверку и оптимизацию дисков.

Проверка дисков вручную

В Windows Server 2012 утилита Проверка диска осуществляет расширенное сканирование и восстановление диска автоматически, вместо проверки вручную, как в предыдущих версиях Windows. Здесь, при использовании

утилиты Проверка диска с NTFS-томами, утилита производит фоновую проверку и анализ ошибок диска. Утилита записывает любую информацию о каждом обнаруженном повреждении в системный файл $corrupt. Если том используется, обнаруженные повреждения могут быть восстановлены путем временного отключения тома. Однако размонтирование тома закрывает все открытые дескрипторы файлов. Восстановление загрузочного/системного тома происходит при следующем запуске компьютера.

Сохранение информации о повреждении и последующее восстановление тома после его размонтирования позволяют Windows быстро восстанавливать тома, а также использовать диск, пока выполняется сканирование. Как правило, оффлайн-восстановление занимает несколько секунд (сравните с устаревшими методами сканирования и восстановления, когда сканирование и восстановление больших томов длилось часами).

FAT, FAT32 и exFAT не поддерживают расширенные функции. При использовании ChkDsk с FAT, FAT32 или exFAT Windows Server 2012 применяет процесс традиционного сканирования и восстановления. Это означает, что для сканирования и восстановления нужно размонтировать том, из-за этого он не может быть использован во время сканирования.

Можно запустить утилиту Проверка диска из командной строки или из других утилит. В командной строке для проверки целостности диска E: можно ввести следующую команду:

chkdsk /scan E:

Утилита выполнит анализ диска и выведет результат проверки. Если дополнительные опции не указаны, ChkDsk не будет исправлять ошибки. Для исправления ошибок на диске E: нужно ввести эту команду:

chkdsk /spotfix E:

Исправление ошибок требует эксклюзивного доступа к тому. Как он будет осуществляться, зависит от типа тома.

- Для несистемных томов будет отображен запрос: можно ли размонтировать том для восстановления? В этом случае введите Y для продолжения или N, чтобы отменить размонтирование. Если отменить размонтирование, то будет отображен другой запрос: нужно ли запланировать восстановление тома при следующем запуске компьютера? Введите Y, чтобы запланировать восстановление, или N для отмены восстановления.
- Для системных томов программа спросит, нужно ли запланировать восстановление тома при следующем запуске компьютера. Введите Y, чтобы запланировать восстановление, или N для отмены восстановления.

Нельзя запустить ChkDsk с обоими параметрами — /scan и /spotfix. Причина в том, что сканирование и восстановление — независимые друг от друга задачи.

Полный синтаксис команды ChkDsk выглядит так:

chkdsk [volume[[path]filename]] [/F] [/V] [/R] [/X] [/I] [/C] [/B] [/L[:size]] [/scan] [/forceofflinefix] [/perf] [/spotfix] [/sdcleanup] [/offlinescanandfix]

Описание параметров ChkDsk:

- volume — задает том, который нужно проверить или восстановить;
- [path]filename — только для FAT. Указывает файлы для проверки на предмет фрагментации;
- /B — переоценивает поврежденные кластеры тома (только для NTFS; подразумевает /R);
- /C — только для NTFS. Пропускает проверку циклов в структуре папок;
- /F — исправляет ошибки на диске, используя устаревшие методы;
- /I — только для NTFS. Менее строгая проверка элементов индекса;
- /L:size — только для NTFS. Изменяет размер файла журнала;
- /R — определяет поврежденные секторы и восстанавливает читаемую информацию (требует /F);
- /V — в FAT отображает полное имя (путь и имя) каждого файла на диске. В NTFS выводит сообщения об очистке (если они имеются);
- /X — предварительное отключение (размонтирование) тома, если необходимо (подразумевает параметр /F).

Для NTFS-томов утилита поддерживает расширенные параметры:

- /forceofflinefix — должен использоваться со /scan. Все найденные неполадки добавляются в очередь для восстановления в автономном режиме;
- /offlinescanandfix — запускает автономную проверку и исправление тома;
- /perf — использует больше системных ресурсов для скорейшего выполнения сканирования;
- /scan — выполняет упреждающее сканирование тома (по умолчанию). Обнаруженные во время сканирования ошибки будут записаны в системный файл $corrupt;
- /sdcleanup — очищает ненужные данные дескриптора, применяется с /F;
- /spotfix — позволяет исправить некоторые типы ошибок онлайн.

Интерактивный запуск проверки дисков

Можно запустить утилиту Проверка диска интерактивно, используя Проводник или оснастку Управление дисками. Следуйте этим действиям:

1. Щелкните на диске и выберите команду Свойства.
2. На вкладке Сервис (Tools) нажмите кнопку Проверить (Check). Откроется окно Проверка ошибок (Check Disk).
3. Нажмите кнопку Проверить диск (Scan Drive) для начала сканирования. Если ошибки не будут найдены, Windows сообщит об этом. Если ошибки будут обнаружены, появятся дополнительные опции, а какие именно, зависит от типа тома, с которым производится работа — с системным или несистемным томом.

Для томов FAT, FAT32 и exFAT Windows использует традиционную проверку. Для начала сканирования нужно нажать кнопку Проверить и восстановить диск

(Scan And Repair Drive). Если при сканировании будут найдены ошибки, нужно перезапустить компьютер для их исправления.

Анализ и оптимизация дисков

При добавлении или удалении файлов данные на диске становятся фрагментированными. Когда диск фрагментирован, большие файлы не могут быть записаны в последовательную область на диске. В результате операционная система должна записать файл на несколько меньших областей диска, и значит, для чтения файла понадобится больше времени. Для сокращения фрагментации ОС Windows Server 2012 может вручную или автоматически анализировать и оптимизировать диски посредством утилиты Оптимизация дисков (Optimize Drives).

При ручной оптимизации утилита Оптимизация дисков проводит анализ тома и затем сообщает процент фрагментации. Если необходима дефрагментация, можно ее осуществить. Системные и загрузочные тома могут быть дефрагментированы в оперативном режиме (без размонтирования диска), а также утилита Оптимизация дисков может использоваться с томами FAT, FAT32, exFAT, NTFS и ReFS.

Запустить анализ и оптимизацию диска вручную можно с помощью следующих действий:

1. В оснастке Управление компьютером выберите узел Запоминающие устройства (Storage), а затем — узел Управление дисками. Щелкните правой кнопкой мыши на диске и выберите команду Свойства.
2. Перейдите на вкладку Сервис и нажмите кнопку Оптимизировать (Optimize). В окне Оптимизация дисков (Optimize Drives) выберите диск и нажмите кнопку Анализировать (Analyze). Утилита Оптимизация дисков (рис. 11.11) проанализирует диск, чтобы определить, нуждается ли он в дефрагментации. Если это так, программа порекомендует дефрагментировать диск.
3. Если диск нуждается в дефрагментации, выберите диск и нажмите кнопку Оптимизировать.

В зависимости от размера диска дефрагментация может занять несколько часов. Можно прервать дефрагментацию в любой момент, нажав кнопку Стоп (Stop).

Анализ и оптимизация дисков может происходить автоматически — когда компьютер подключен к сети питания (а не работает от аккумулятора — для ноутбуков) и когда операционная система запущена, но находится в состоянии простоя. По умолчанию оптимизация диска — это еженедельное задание, а не ежедневное, и для этого есть серьезное основание.

Обычно оптимизировать диски нужно только периодически, и оптимизация раз в неделю в большинстве случаев вполне достаточна. Отметьте, однако, что хотя несистемные диски занимает намного больше времени.

Можно управлять приблизительным временем начала анализа и оптимизации дисков, изменяя автоматизированное время начала обслуживания. Операционная Windows Server также уведомляет, если пропущены три последовательных попытки оптимизации. Все внутренние диски и

определенные внешние диски оптимизируются автоматически как часть регулярного расписания.

ОС Windows Server 2012 автоматически осуществляет циклическую дефрагментацию. Благодаря этой функции, когда запланированная дефрагментация остановлена и запущена заново, компьютер автоматически продолжает дефрагментацию с места, на котором она была прервана.

Автоматической дефрагментацией можно управлять с помощью следующих действий:

1. В оснастке Управление компьютером выберите узел Запоминающие устройства (Storage), а затем — узел Управление дисками. Щелкните правой кнопкой мыши на диске и выберите команду Свойства.
2. На вкладке Сервис нажмите кнопку Оптимизировать. Откроется окно Оптимизация дисков. Если нужно изменить параметры оптимизации, нажмите кнопку Изменить параметры (Change Settings). Откроется окно. Для отмены автоматической дефрагментации сбросьте флажок Выполнять по расписанию (рекомендуется) (Run On A Schedule). Для включения автоматической дефрагментации, наоборот, установите этот флажок.
3. Частота дефрагментации по умолчанию установлена.
4. В раскрывающемся списке Частота (Frequency) можно выбрать значения ежедневно (Daily), еженедельно (Weekly) и ежемесячно (Monthly). Если не нужно получать уведомления о пропущенных выполнениях по расписанию, установите флажок Уведомлять в случае пропуска трех выполнений по расписанию подряд (Notify Me if three consecutive scheduled runs are missed).
5. Если нужно указать, какие диски должны быть дефрагментированы, нажмите кнопку Выбрать (Choose) и укажите тома, которые следует дефрагментировать. По умолчанию все диски, установленные внутри компьютера или подключенные к компьютеру, дефрагментируются. Также автоматически дефрагментируется каждый новый диск, подключенный к компьютеру. Установите флажки дисков, которые должны быть дефрагментированы, а также флажки для дисков, которые не нужно автоматически дефрагментировать. Нажмите кнопку OK для сохранения параметров.
6. Нажмите кнопку OK, а затем кнопку Закрыть.

ГЛАВА 3

Общий доступ к данным, безопасность и аудит

Протокол SMB (Server Message Block) — основной протокол предоставления общего доступа к файлам, используемый компьютерами под управлением Microsoft Windows. Когда к папкам предоставляется общий доступ по сети, клиент SMB применяется для чтения/записи файлов и для запроса служб с компьютеров, на которых находятся общие папки.

Операционные системы Windows 8 и Windows Server 2012 поддерживают SMB версии 3.0 и содержат SMB-клиента, совместимого с версией 3.0. SMB 3.0 содержит много улучшений, положительно влияющих на производительность, особенно при использовании кластеризируемых файловых серверов. Основное улучшение — сквозное шифрование данных SMB, которое избавляет от использования протокола IPsec, специальных аппаратных средств или акселераторов глобальной сети (WAN) для защиты данных от прослушивания. Шифрование SMB может быть включено индивидуально для каждого общего ресурса.

При использовании SMB Windows Server 2012 поддерживает две модели предоставления общего доступа к файлам: стандартный общий доступ и папка Общие (Public). Стандартный общий доступ позволяет удаленным пользователям получить доступ к сетевым ресурсам — файлам, папкам и дискам. При предоставлении общего доступа к папке или диску все их файлы и подпапки также станут доступными определенным пользователям. Не нужно перемещать файлы из их текущего местоположения для предоставления общего доступа к ним.

Включить стандартный общий доступ к файлам можно на дисках, отформатированных как FAT, FAT32, exFAT, NTFS и ReFS. К дискам exFAT, FAT или FAT32 применяется один набор разрешений — разрешения общего доступа. К дискам NTFS и ReFS применяются два набора разрешений — NTFS-разрешения (также называются разрешениями доступа) и разрешения общего доступа. Наличие двух наборов разрешений позволяет точно определять, кто получит доступ к общим файлам, а также уровень назначенного доступа. С NTFS-разрешениями или разрешениями общего доступа не нужно перемещать файлы, к которым предоставляется общий доступ.

При использовании папки Общие (Public) нужно просто скопировать или переместить файлы в папку Общие компьютера. Общие файлы доступны любому, кто входит в компьютер локально, независимо от того, есть ли у него стандартная учетная запись или учетная запись администратора. Также можно предоставить сетевой доступ к папке Общие. Если сделать это, возможности как-либо ограничить доступ не будет. Папка Общие и все ее содержимое открыты для всех, кто может получить доступ к компьютеру по локальной сети.

Использование и включение общего доступа к файлам

Параметры общего доступа на компьютере определяют способ предоставления общего доступа к файлам. Операционная система Windows Server 2012 поддерживает две модели предоставления общего доступа к файлам.

1. Стандартный общий доступ к файлам позволяет удаленным пользователям получать доступ к файлам, папкам и дискам по сети. При предоставлении общего доступа к папке или диску все файлы и подпапки в этой папке (на диске) станут доступными определенным пользователям. Разрешения общего доступа и разрешения доступа используются для определения, кто получит доступ к общим файлам и каким будет уровень

этого доступа. Не нужно перемещать файлы, к которым предоставляется общий доступ.

2. Папка Общие предоставляет локальным и удаленным (если установлено) пользователям доступ к любым файлам, помещенным в папку %SystemDrive%\Пользователи\ Общие (%SystemDrive%\Users\Public) компьютера. Разрешения доступа на папке Общие определяют, какие пользователи и группы могут получить доступ к общим файлам, и задают уровень этого доступа. При копировании или перемещении файлов в папку Общие разрешения доступа файлов изменяются так, чтобы они совпадали с разрешениями папки Общие. Также добавляются некоторые дополнительные разрешения. Когда компьютер — часть рабочей группы, можно добавить защиту паролем для папки Общие.

Отдельная защита паролем не нужна в домене. В домене только пользователи домена (группа Domain Users) имеют доступ к папке Общие.

Со стандартным общим доступом к файлам локальные пользователи автоматически не получают доступ к любым данным, сохраненным на компьютере. Администратор контролирует локальный доступ к файлам и папкам, используя параметры безопасности на локальном диске. При использовании папки Общие файлы, скопированные или перемещенные в эту папку, доступны любому пользователю, зарегистрировавшемуся локально. Также можно предоставить сетевой доступ к папке Общие. В результате, однако, папка Общие и все ее содержимое будет открыто каждому, кто может получить доступ к компьютеру по сети.

Операционная система Windows Server 2012 добавляет новые слои безопасности с помощью комплексной проверки подлинности, технологии идентификации на основе требований и политик централизованного доступа. В Windows 8 и Windows Server 2012 можно назначить идентификацию на основе требований к ресурсам файла и папки на томах NTFS и ReFS. В Windows Server 2012 пользователям доступ к ресурсам файла и папки предоставляется непосредственно с помощью разрешений доступа и разрешений общего доступа или косвенно с помощью идентификации на основе требований и политик централизованного доступа.

SMB 3.0 позволяет шифровать данные, передающиеся по сети. Можно включить SMB-шифрование для общих ресурсов на NTFS- и ReFS-томах. SMB-шифрование работает только тогда, когда компьютер, запрашивающий данные из SMB-ресурса (либо стандартный общий ресурс, либо DFS-ресурс), и сервер поддерживают SMB 3.0. Операционные системы Windows 8 и Windows Server 2012 поддерживают SMB 3.0 (они используют клиент SMB 3.0).

Хотя ReFS обеспечивает высоконадежную файловую систему, имейте в виду, что ReFS не поддерживает теневые копии. Поэтому, если создаете общие ресурсы на томах ReFS, пользователи не смогут вернуться к предыдущим версиям файлов и папок, сохраненных в этих общих ресурсах.

Папка Общие разработана для предоставления пользователям общего доступа к файлам и каталогам из одного расположения. В этом случае следует скопировать или переместить файлы, к которым нужно предоставить общий

доступ, в папку %SystemDrive%\ Пользователи\Общие (%SystemDrive%\Users\Public) компьютера. Доступ к общим файлам можно получить из Проводника. Дважды щелкните по системному диску, а затем перейдите в папку Пользователи\Общие (Users\Public).

В папке Общие есть несколько подпапок, которые можно использовать для организации общих файлов.

- Общий рабочий стол (Public Desktop) — используется для предоставления общего доступа к элементам рабочего стола. Любые файлы и ярлыки программ, помещенные в эту папку, появятся на рабочем столе всех пользователей, которые зайдут на этот компьютер (и всех сетевых пользователей, если к папке Общие был предоставлен сетевой доступ).
- Общие документы (Public Documents), Общая музыка (Public Music), Общие изображения (Public Pictures), Общие видео (Public Videos) — используются для предоставления общего доступа к документам и файлам мультимедиа. Все файлы, помещенные в одну из этих папок, доступны всем пользователям, которые зашли на этот компьютер (и всем сетевым пользователям, если к папке Общие был предоставлен сетевой доступ).
- Общие загруженные файлы (Public Downloads) — используются для предоставления общего доступа к загруженным файлам. Любые загрузки, помещенные в подпапку Общие загруженные файлы, станут доступны всем пользователям, которые зашли на этот компьютер (и всем сетевым пользователям, если к папке Общие был предоставлен сетевой доступ).

По умолчанию доступ к папке Общие есть у любого пользователя с учетной записью и паролем. При копировании или перемещении файлов в папку Общие разрешения доступа изменяются так, чтобы соответствовать папке Общие, а также добавляются некоторые дополнительные разрешения.

Можно изменить настройки общего доступа папки Общие двумя основными способами.

- Разрешить пользователям, которые зарегистрировались на компьютере, просматривать и управлять общими файлами, но запретить сетевым пользователям доступ к этим файлам. После настройки этой опции неявные группы Интерактивные (Interactive), Пакетные файлы (Batch) и Служба (Service) получат особые разрешения для публичных файлов и папок.
- Разрешить пользователям с сетевым доступом просматривать и управлять общими файлами. Это разрешит сетевым пользователям открывать, изменять, создавать и удалять публичные файлы. Неявной группе Все (Everyone) будут предоставлены полные права к публичным файлам и папкам.

Операционная система Windows Server 2012 может использовать одну или обе модели совместного использования в любое время. Однако стандартный общий

доступ к файлам более безопасен и предоставляет лучшую защиту, чем использование папки Общие, а улучшение безопасности очень важно для защиты данных организации. Со стандартным общим доступом к файлам, разрешения общего доступа используются только тогда, когда пользователь пытается получить доступ к файлу или папке с другого компьютера по сети. Права доступа (разрешения доступа) используются всегда, независимо от того, зарегистрировался ли пользователь локально или удаленно для получения доступа к файлу или папке по сети.

Если доступ к данным осуществляется удаленно, сначала применяются разрешения общего доступа, а затем — обычные разрешения доступа.

Можно настроить параметры базового общего доступа, используя опцию Дополнительные параметры общего доступа (Advanced Sharing Settings) в Центре управления сетями и общим доступом (Network and Sharing Center). Отдельные параметры предусмотрены для сетевого обнаружения, общего доступа к файлам и принтерам.

Можно управлять конфигурацией общего доступа компьютера так:

1. В Панели управления щелкните по ссылке Просмотр состояния сети и задач в (View network status and tasks) категории Сеть и Интернет (Network and Internet). В результате будет открыт Центр управления сетями и общим доступом.
2. В Центре управления сетями и общим доступом щелкните по ссылке Изменить дополнительные параметры общего доступа (Change advanced sharing settings) на панели слева. Выберите профиль сети, для которой нужно включить общий доступ к файлам и принтерам. Обычно, это профиль Доменный (Domain).
3. Стандартный общий доступ к файлам и принтерам управляет сетевым доступом к общим ресурсам. Для настройки стандартного общего доступа к файлам выберите одну из опций:
   - Включить общий доступ к файлам и принтерам (Turn on file and printer sharing) для включения общего доступа;
   - Отключить общий доступ к файлам и принтерам для отключения общего доступа (Turn off file and printer sharing).
4. Доступ к общедоступным папкам контролирует доступ к папке Общие компьютера. Для настройки этого доступа разверните панель Все сети (All Networks Public Folder Sharing), нажав соответствующую кнопку. Выберите одну из опций:
   - Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках (Turn on sharing so anyone with network access can read and write files in the public folders) — включает доступ к папке Общие и ко всем общим данным для всех, кто может получить доступ к компьютеру по сети. Настройки Брандмауэра Windows (Windows Firewall) могут предотвращать внешний доступ;
   - Отключить общий доступ (Turn off public folder sharing) — отключает общий доступ, предотвращая доступ локальной сети к

папке Общие. Любой пользователь, который зарегистрировался локально на компьютере, все еще сможет получить доступ к папке Общие и к ее файлам.

5. Нажмите кнопку Сохранить изменения (Save Changes).

Настройка стандартного общего доступа к файлам

Общие ресурсы используются для контроля доступа удаленных пользователей. Разрешения на общих папках не имеют никакого эффекта для пользователей, зарегистрировавшихся локально на сервере или рабочей станции, на которой размещены общие папки.

Просмотр существующих общих ресурсов

Для работы с общими ресурсами можно использовать и оснастку Управление компьютером и консоль Диспетчер серверов (Server Manager). Также можно просмотреть текущие общие ресурсы на компьютере с помощью команды net share, введенной в командной строке, или команды get-smbshare, введенной в приглашении PowerShell.

Командлет get-smbshare — один из многих командлетов, связанных с модулем smbshare.

Чтобы получить список других доступных для работы с SMB-ресурсами командлетов, введите команду get-command -module smbshare в приглашении Windows PowerShell.

Управление компьютером, net share и get-smbshare отображают информацию о SMB-ресурсах, включая стандартные SMB-папки, скрытые SMB-папки (которые заканчиваются суффиком $) и SMB-папки, предоставленные в общий доступ с использованием DFS (Distributed File System). Диспетчер серверов отображает информацию о стандартных SMB-папках, DFS-ресурсах и папках, предоставленных в общий доступ с использованием NFS. Диспетчер серверов не отображает скрытые SMB-папки.

В оснастке Управление компьютером можно просмотреть общие папки на локальном или удаленном компьютере так:

1. По умолчанию оснастка подключена к локальному компьютеру. Если нужно подключиться к удаленному компьютеру, щелкните по узлу Управление компьютером правой кнопкой мыши и выберите команду Подключиться к другому компьютеру (Connect to another computer). В появившемся окне выберите переключатель другим компьютером (Another Computer) и введите имя или IP-адрес компьютера, к которому нужно подключиться, а затем нажмите кнопку OK.
2. В дереве консоли перейдите к узлу Служебные программы\Общие папки (System Tools\Shared Folders), а затем выберите узел Общие ресурсы (Shares). Будет отображена информация о текущих общих ресурсах в системе
3. Колонки узла Общие ресурсы (Shares) предоставляют следующую информацию:
   - Общий ресурс (Share name) — имя общей папки;

- Путь к папке (Folder path complete) — полный путь к папке на локальной системе;
- Тип (Type) — тип компьютеров, которые могут использовать этот ресурс. Обычно здесь выводится Windows, поскольку SMB-ресурсы предназначены для Windows-компьютеров;
- Количество клиентских подключений (# Client Connections) — число клиентов, подключенных в данный момент к ресурсу;
- Описание (Description) — описание общего ресурса.

В диспетчере серверов можно просмотреть общие папки на локальном или удаленном компьютере с помощью следующих действий:

1. Выберите опцию Файловые службы и службы хранилища (File and Storage Services), а затем подузел Общие ресурсы.
2. Подузел Общие ресурсы предоставляет информацию о каждом ресурсе на каждом сервере, который был добавлен для управления (рис. 12.3). Колонки узла Общие ресурсы предоставляют следующую информацию:
   - Общий ресурс (Share) — имя общей папки;
   - Локальный путь (Local Path) — полный путь к папке на локальной системе;
   - Протокол (Protocol) — используемый протокол, SMB или NFS;
   - Тип доступности (Cluster Role) — если сервер, предоставляющий общий доступ к папке, часть кластера, здесь показан тип кластера. В противном случае, тип кластера — Некластерный (None).
3. Если щелкнуть по общему ресурсу на панели Общие ресурсы, на панели Том (Volume) (справа) будет отображена информация о соответствующем томе.

Сетевая файловая система (NFS, Network File System) — протокол общего доступа к файлам, используемый в UNIX-системах, в том числе и на компьютерах под управлением Mac OS X. Как будет сказано в разд. "Настройка общих ресурсов NFS" далее в этой главе, можно включить поддержку NFS, установив роль Сервер для NFS (Server For NFS), как часть настройки файлового сервера.

Создание общих папок в оснастке Управление компьютером

Операционная система Windows Server 2012 предлагает несколько способов предоставления общего доступа к папкам. Можно предоставить общий доступ к локальным папкам, используя Проводник, а общий доступ к локальным и удаленным папкам — в оснастке Управление компьютером или консоли Диспетчер серверов.

При создании общего ресурса в оснастке Управление компьютером можно настроить его разрешения общего доступа и автономные параметры. При создании общего ресурса в диспетчере серверов можно настроить все аспекты общего доступа, включая разрешения NTFS, шифрование данных, автономные параметры для кэширования и разрешения общего доступа. Обычно нужно

создавать общие ресурсы на NTFS-тома, поскольку NTFS предлагает самое устойчивое решение.

В оснастке Управление компьютером для предоставления общего доступа к папке выполните следующие действия:

1. Если необходимо, подключитесь к удаленному компьютеру. В дереве консоли перейдите в узел Служебные программы\Общие папки\Общие ресурсы. Будут отображены текущие общие ресурсы в системе.
2. Щелкните правой кнопкой мыши по подузлу Общие ресурсы и выберите команду Новый общий ресурс (New Share). Будет запущен мастер создания общих ресурсов (Create A Shared Folder Wizard). Нажмите кнопку Далее.
3. В поле Путь к папке (Folder Path) введите локальный путь к папке, к которой предоставляется общий доступ. Путь должен быть точным, например, C:\EntData\Documents. Если не знаете точный полный путь, нажмите кнопку Обзор и используйте окно Обзор папок для поиска папки, к которой нужно предоставить совместный доступ. Затем нажмите кнопку OK. Нажмите кнопку Далее. Если путь, указанный в поле Путь к папке, не существует, мастер создаст эту папку автоматически. Нажмите кнопку Да, когда появится запрос на создание папки.
4. В поле Общий ресурс (Share Name) введите имя общего ресурса. Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальны для каждой системы. Если нужно скрыть общий ресурс от пользователей (это означает, что они не увидят ресурс, когда они попытаются просмотреть список общих ресурсов в Проводнике или командной строке), введите знак доллара ($) в качестве последнего знака имени ресурса. Например, можно создать ресурс с именем PrivEngData$, который будет скрыт в Проводнике, в утилите net view и других подобных утилитах. Пользователи все еще могут подключиться к общему ресурсу и получить доступ к его данным, если им были предоставлены надлежащие разрешения доступа и они знают имя ресурса. Заметьте, что $ должен быть введен как часть имени общего ресурса, когда осуществляется подключение.
5. Можно ввести описание общего ресурса в поле Описание (Description). При просмотре общих ресурсов на определенном компьютере в оснастке Управление компьютером будет отображено описание ресурса.
6. По умолчанию общий ресурс настраивается так, что только файлы и программы, которые определяют пользователи, доступны в автономном режиме. Обычно эту опцию удобно использовать, поскольку она также позволяет пользователям получить преимущества новой функции Всегда вне сети (Always Offline). Если нужно использовать другие настройки автономного режима, нажмите кнопку Изменить и в окне Настройка автономного режима (Offline Settings) установите надлежащие параметры. Можно установить следующие параметры.
   – Вне сети доступны только указанные пользователем файлы и программы (Only the files and programs that users specify are available

offline) — выберите эту опцию, если нужно, чтобы клиентские компьютеры кэшировали только файлы и программы, которые укажут пользователи для автономного использования. Дополнительно, если служба роли BranchCache для сетевых файлов (BranchCache For Network Files) установлена на файловом сервере, установите флажок Включить BranchCache (Enable BranchCache), чтобы включить кэширование файлов компьютерами филиалов, которые были загружены из общего ресурса. Эти файлы также будут безопасно предоставлены в общий доступ другим компьютерам филиала.

- Файлы и программы в этой общей папке недоступны вне сети (No files or programs from the shared folder are available offline) — выберите эту опцию, если не нужно, чтобы кэшированные копии файлов и программ из общего ресурса были доступны на клиентских компьютерах в автономном режиме.
- Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы (All files and programs that users open from the share are automatically available offline) — выберите эту опцию, если нужно, чтобы клиентские компьютеры автоматически кэшировали все файлы и программы, которые пользователи открывали из общего ресурса. Дополнительно можно установить флажок Оптимизировать производительность (Optimize for performance) для запуска программных файлов из локального кэша, а не с общего ресурса на сервере.

7. Нажмите кнопку Далее и установите основные разрешения для общего ресурса. Доступны следующие параметры.
   - У всех пользователей доступ только для чтения (All users have read-only access) — предоставляет пользователям право просмотра файлов и чтения данных. Пользователи не могут создавать, изменять или удалять файлы и папки.
   - Администраторы имеют полный доступ, остальные — доступ только для чтения (Administrators have full access; other users have read-only access) — предоставляет администраторам полный доступ к общему ресурсу. Полный доступ позволяет администраторам создавать, изменять и удалять файлы и папки. На NTFS-томе или разделе администраторы также могут изменять разрешения доступа и владельцев файлов и папок. Другие пользователи могут только просматривать файлы и читать данные. Они не могут создавать, изменять или удалять файлы и папки.
   - Администраторы имеют полный доступ, остальные не имеют доступа (Administrators have full access; other users have no access) — предоставляет администраторам полный доступ к ресурсу, остальным пользователям доступ запрещен. • Настройка разрешений доступа (Customize permissions) — позволяет настроить доступ определенным пользователям и группам, обычно это лучший способ. Установка

разрешений доступа подробно рассматривается в разд. "Управление разрешениями общих ресурсов" далее в этой главе.

8. После нажатия кнопки Готово мастер создаст общий ресурс и отобразит состояние "Работа мастера создания общих ресурсов успешно завершена" (Sharing was successful).

Если вместо этого будет отображена ошибка, запомните ее, примите меры по ее ликвидации и повторите попытку создания общего ресурса. Нажмите кнопку Готово.

Отдельные папки могут иметь несколько общих ресурсов. У каждого ресурса собственное имя и собственный набор прав доступа. Для создания дополнительных общих ресурсов на уже существующем общем ресурсе просто следуйте предыдущей процедуре с этими изменениями:

- на этапе 4 при вводе имени общего ресурса убедитесь, что используете отличающееся имя;
- на этапе 5 при добавлении описания для общего ресурса используйте описание, объясняющее, какой это ресурс, для чего он используется и чем отличается от других ресурсов в этой же папке.

Создание общих папок в диспетчере серверов

В диспетчере серверов можно предоставить общий доступ к папке так:

1. Подузел Общие ресурсы в Файловые службы и хранилища показывает существующие общие ресурсы на всех файловых серверах, добавленных для управления.
2. На панели Общие ресурсы выберите меню Задачи, а затем команду Новый общий ресурс (New share wizard). Будет запущен мастер создания общих ресурсов (New share). Выберите один из профилей общего ресурса и нажмите кнопку Далее. Мастер предлагает несколько профилей:
   - Общий ресурс SMB — быстрый профиль (SMB share — quick) — основной профиль для создания общего ресурса SMB, который позволяет настраивать свои параметры и разрешения;
   - Общий ресурс SMB — дополнительные (SMB share — advanced) — дополнительный профиль для создания SMB-ресурса, позволяющий настроить параметры, разрешения, свойства управления и NTFS-квоты (если применимо);
   - Общий ресурс SMB — профиль приложений (SMB share — applications) — пользовательский профиль для создания SMB-ресурсов с параметрами, подходящими для Hyper-V, определенных СУБД и других серверных приложений. Это почти то же самое, что и быстрый профиль, но не позволяет включать перечисление на основе доступа — ABE (Access-based Enumeration) и автономное кэширование. Если используется служба роли Сервер для NFS (Server For NFS), также будут доступны профили для создания NFS-ресурсов. только файловые серверы, добавленные для управления. Как только будете готовы продолжить, нажмите кнопку Далее. По умолчанию консоль Диспетчер серверов создает общий ресурс как новую папку в каталоге

\Shares на выбранном томе. Чтобы переопределить это, выберите опцию Ввести пользовательский путь (Type a custom path) и затем введите нужный путь общего ресурса, например, C:\Data или нажмите кнопку Обзор и используйте окно Обзор папок для выбора пути общего ресурса.

3. На странице Выбор имени общего ресурса (Specify share name) введите имя общего ресурса (рис. 12.5). Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальными для каждой систем.SMB 3.0 содержит расширения для серверных приложений. Эти расширения повышают производительность небольших случайных чтений и записей, которые характерны для серверных приложений, например, Microsoft SQL Server OLTP. В SMB 3.0 пакеты используют наибольший размер передаваемых данных (Maximum Transmission Unit, MTU), что повышает производительность больших передач данных, которые характерны для развертывания и копирования виртуальных жестких дисков по сети, резервного копирования базы данных и восстановления по сети, транзакций хранилища данных SQL-сервера по сети.
4. На странице Укажите сервер и путь к этой общей папке (Select the server and path for this share) выберите сервер и том, на которых нужно создать общую папку. Доступны только файловые серверы, добавленные для управления. Как только будете готовы продолжить, нажмите кнопку Далее. По умолчанию консоль Диспетчер серверов создает общий ресурс как новую папку в каталоге \Shares на выбранном томе. Чтобы переопределить это, выберите опцию Ввести пользовательский путь (Type a custom path) и затем введите нужный путь общего ресурса, например, C:\Data или нажмите кнопку Обзор и используйте окно Обзор папок для выбора пути общего ресурса.
5. На странице Выбор имени общего ресурса (Specify share name) введите имя общего ресурса (рис. 12.5). Это имя папки, к которой будут подключаться пользователи. Имена общих ресурсов должны быть уникальными для каждой систем.
6. При необходимости введите описание общего ресурса в поле Описание общего ресурса. При просмотре списка общих ресурсов на определенном компьютере описание будет показано в оснастке Управление компьютером.
7. Запишите локальный и удаленный пути доступа к общему ресурсу. Эти пути установлены на основании расположения папки и указанного имени. Нажмите кнопку Далее для продолжения.
8. На странице Настройка параметров общего ресурса (Configure share settings) можно задать способ использования общего ресурса.
   – Включить перечисление на основе доступа (Enable access-based enumeration) — настраивает разрешения так, что при просмотре папки пользователями будут отображены только файлы и папки, которым как минимум предоставлено право чтения. Если у пользователя нет

права чтения (или эквивалентного) для файла или папки внутри общей папки, этот файл или папка будут скрыты. (Эта опция недоступна, если создается SMB-ресурс, оптимизированный для приложений.)

- Разрешить кэширование общего ресурса (Allow caching of share) — настраивает общий доступ для кэширования только файлов и программ, которые пользователи выберут для автономного использования. Хотя можно позже отредактировать свойства общего ресурса и изменить настройки автономного режима, обычно нужно выбрать эту опцию, поскольку она позволяет пользователям использовать преимущества новой функции Всегда не в сети (Always offline). Дополнительно, если служба роли BranchCache для сетевых файлов (BranchCache for network files) установлена на файловом сервере, отметьте флажок Включить BranchCache (Enable BranchCache) для общего файлового ресурса, чтобы включить кэширование файлов компьютерами филиалов, которые были загружены из общего ресурса. Эти файлы также будут безопасно предоставлены в общий доступ другим компьютерам филиала. (Эта опция недоступна при создании SMB-ресурса, оптимизированного для приложений.)
- Зашифровать доступ к данным (Encrypt data access) — включает SMB-шифрование, которое защищает данные файла от прослушивания при их передаче по сети. Опция полезна в ненадежных сетях.

9. На странице Определение разрешений для управления доступом (Specify permissions to control access) назначены разрешения по умолчанию. По умолчанию специальной группе Все предоставляется полный доступ, также перечислены разрешения папки. Для изменения разрешений ресурса, папки (или обоих типов разрешений) нажмите кнопку Настройка разрешений (Customize permissions) и затем используйте окно Дополнительные параметры безопасности (Advanced security settings) для настройки требуемых полномочий. Установка разрешений общего доступа полностью описана в разд. "Управление разрешениями общих ресурсов" далее в этой главе. Установка разрешений папки полностью описана в разд. "Разрешения файла и папки" далее в этой главе.
10. Если используется дополнительный профиль, можно установить свойства управления папки и затем нажать кнопку Далее. Эти свойства определяют назначение папки и тип данных, сохраненных в ней так, что политики управления данными, такие как правила классификации, могут использовать эти свойства.
11. Если используется расширенный профиль, дополнительно можно установить квоты папки по шаблону и затем нажать кнопку Далее. Можно выбрать только шаблон квоты, который уже создан. Подробно этот процесс будет описан в разд. "Управление шаблонами дисковых квот" далее в этой главе.
12. На странице Подтверждение выбора (Confirm Selections) просмотрите установленные параметры. После нажатия кнопки Создать мастер создаст общий ресурс, настроит его и установит разрешения. В случае успешного

создания ресурса будет установлено состояние "Общий ресурс успешно создан" (The share was successfully created). Если вместо этого будет отображено сообщение об ошибке, запишите его и примите меры по исправлению ошибки перед повторением этой процедуры. Нажмите кнопку Закрыть.

Изменение параметров общей папки

После создания общего ресурса можно настроить множество базовых и расширенных параметров, включая перечисление на основе доступа, зашифрованный доступ к данным, автономное кэширование и свойства управления. В диспетчере серверов можно модифицировать эти свойства так:

1. Подузел Общие ресурсы узла Файловые службы и службы хранилища (File And Storage Services) показывает существующие общие ресурсы для всех файловых серверов, добавленных для управления.
2. Щелкните правой кнопкой мыши на общем ресурсе, с которым нужно работать, и выберите команду Свойства.
3. В окне Свойства (рис. 12.6) есть несколько панелей с параметрами. Можно развернуть панели по одной или выбрать опцию Показать все (Show All), чтобы просмотреть все панели за один раз.Если общий ресурс будет использоваться для Hyper-V, нужно включить ограниченное делегирование для удаленного управления Hyper-V.
4. Используйте предоставленные параметры для изменения настроек (при необходимости), а затем нажмите кнопку OK. Доступны те же параметры, что и при создании ресурса, они зависят от используемого профиля.

Если создается ресурс для общего использования и общего доступа, можно опубликовать общий ресурс в Active Directory. Публикация ресурса в Active Directory делает доступ к нему проще для других пользователей. Однако эта опция не доступна в диспетчере серверов.

Для публикации общего ресурса в Active Directory щелкните на ресурсе в оснастке Управление компьютером и выберите команду Свойства. На вкладке Публикация (Publish) установите флажок Опубликовать этот общий ресурс в Active Directory (Publish this share in Active Directory), добавьте описание и информацию о владельце, а затем нажмите кнопку OK.

Управление разрешениями общих ресурсов

Разрешения доступа устанавливают максимальные допустимые действия с общим ресурсом. По умолчанию при создании общего ресурса каждый пользователь с доступом к сети имеет право чтения содержимого общего ресурса. Это очень важное изменение с точки зрения безопасности — в предыдущих версиях Windows Server разрешением по умолчанию был Полный доступ.

Для томов NTFS и ReFS можно использовать разрешения файла и папки, а также разрешения общего доступа для ограничения доступа к ресурсу. Для томов FAT можно устанавливать только разрешения общего доступа.

Различные разрешения общего ресурса

Список разрешений от самого строгого до наименее строгого таков:

1. Нет доступа (No Access) — ресурсу не предоставлены какие-либо разрешения;
2. Чтение (Read) — с этим разрешением пользователи могут:
   - просматривать имена файлов и подпапок;
   - получать доступ к подпапкам общей папки;
   - читать данные и атрибуты файла;
   - запускать программы;
3. Изменение (Change) — у пользователей есть разрешение Чтение и возможность выполнять следующие операции:
   - создавать файлы и подпапки;
   - изменять файлы;
   - изменять атрибуты файлов и подпапкок;
   - удалять файлы и подпапки;
4. Полный доступ (Full Control) — у пользователей есть разрешения Чтение и Изменение, а также дополнительные возможности на NTFS-томах:
   - изменение разрешений файлов и папок;
   - изменение владельца файлов и папок.

Можно назначить разрешения доступа пользователям и группам, в том числе даже неявным группам.

Просмотр и настройка разрешений общего доступа

Просмотреть и настроить разрешения общего доступа можно в оснастке Управление компьютером или в консоли Диспетчер серверов. Для просмотра и настройки разрешений общего доступа в оснастке Управление компьютером выполните следующие действия:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором создан общий ресурс. В дереве консоли разверните узел Служебные программы\Общие папки\Общие ресурсы.
2. Щелкните правой кнопкой мыши на ресурсе, настройки которого нужно изменить, и выберите команду Свойства.
3. В окне Свойства перейдите на вкладку Разрешения для общего ресурса (Share Permissions). Теперь можно просмотреть список пользователей и групп, у которых есть доступ к этому ресурсу, а также тип предоставленного им доступа.
4. Пользователи или группы, которым уже предоставлен доступ к общему ресурсу, отображаются в списке Группы или пользователи (Group or user names). Можно удалить разрешения для этих пользователей и групп, выбрав учетную запись пользователя или группу, разрешения для которых нужно удалить, и затем нажав кнопку Удалить (Remove). Изменить разрешения для этих пользователей и групп можно так:
   - выберите пользователя или группу;
   - измените разрешения в списке Разрешения для (Permissions for);

5. Для добавления разрешений для другой учетной записи пользователя или группы нажмите кнопку Добавить. Будет открыто окно Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"
6. Введите имя пользователя, компьютера или группы в текущем домене, а затем нажмите кнопку Проверить имена. У этой процедуры может быть один из следующих результатов:
   – если найдено одно совпадение, диалоговое окно будет автоматически обновлено и эта запись будет подчеркнута;
   – если совпадения не найдены, введено неправильное имя или выбрано неправильное место (домен), измените имя и попробуйте еще раз или же нажмите кнопку Размещение и выберите другое место;
   – если найдено несколько совпадений, выберите имя или имена, которые должны использоваться, и затем нажмите кнопку OK. Чтобы присвоить полномочия другим пользователям, компьютерам или группам, вводят точку с запятой (;) и затем повторяют этот процесс. Кнопка Размещение позволяет получить доступ к именам в других доменах. Нажмите эту кнопку, чтобы увидеть список доменов, к которым есть доступ. Благодаря транзитивным доверительным отношениям в Windows Server обычно можно получить доступ ко всем доменам в дереве доменов или лесу.
7. Нажмите кнопку OK. Пользователи и группы будут добавлены в список Группы или пользователи для ресурса.
8. Настройте разрешения доступа для каждого пользователя, компьютера и группы, выбрав имя учетной записи и затем разрешив или запретив разрешения доступа. Помните, что устанавливаются максимально допустимые разрешения для определенной учетной записи.
9. Нажмите кнопку OK. Как назначить дополнительные разрешения безопасности для NTFS.

Для просмотра и настройки разрешений общего доступа в диспетчере серверов выполните следующие действия:

1. Подузел Общие ресурсы узла Файловые службы и службы хранилища показывает существующие общие ресурсы для всех файловых серверов, добавленных для управления.
2. Щелкните правой кнопкой мыши на общем ресурсе, с которым нужно работать, и выберите команду Свойства.
3. В окне Свойства выберите опцию Разрешения (Permissions) на панели слева. Теперь можно просмотреть, кому и какие разрешения предоставлены.
4. Для изменения разрешений общего доступа или папки (или обоих типов разрешений) нажмите кнопку Настройка разрешений (Customize Permissions). Далее выберите вкладку Общая папка (Share) в окне Дополнительные параметры безопасности (Advanced Security Settings),
5. Пользователи и группы, которым предоставлен доступ к ресурсу, выводятся в списке Элементы разрешений (Permission entries). Можно удалить разрешения для пользователей и групп, выделив пользователя

или группу и нажав кнопку Удалить. Изменить разрешения для пользователя или группы можно так:

- выберите пользователя или группу и нажмите кнопку Изменить;
- разрешите или запретите разрешения доступа в списке Элементы разрешений и нажмите кнопку OK.

6. Чтобы добавить разрешения для другого пользователя или группы, нажмите кнопку Добавить. Откроется окно Элемент разрешения
7. Щелкните по ссылке Выберите субъект (Select a principal) для отображения окна Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы". Введите имя пользователя или группы. Убедитесь, что ссылаетесь на учетное имя пользователя, а не на полное имя пользователя. За один раз можно ввести только одно имя.
8. Нажмите кнопку Проверить имена. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова либо нажмите кнопку Размещение для выбора нового размещения. Если будет найдено несколько совпадений, в окне Найдено несколько имен (Multiple Names Found) выберите имя, которое нужно использовать, и нажмите кнопку OK.
10. Нажмите кнопку OK. Пользователь или группа будут добавлены как Субъект (Principal), а окно Элемент разрешения будет обновлено, чтобы отобразить это.
11. Используйте список Тип (Type), чтобы указать, что нужно сделать: разрешить или запретить разрешения. А затем выберите разрешения, которые нужно разрешить или запретить.
12. Нажмите кнопку OK, чтобы вернуться в окно Дополнительные параметры безопасности (Advanced Security Settings). Как назначить дополнительные разрешения безопасности для NTFS, см. в разд. "Разрешения файла и папки" далее в этой главе.

Управление существующими общими ресурсами

Администратору часто приходится управлять общими папками. В этом разделе мы рассмотрим общие административные задачи по управлению общими ресурсами.

Особые общие ресурсы

При установке Windows Server операционная система автоматически создает особые общие ресурсы, которые так же известны, как административные общие ресурсы (administrative shares) или скрытые общие ресурсы (hidden shares). Эти ресурсы разработаны с целью сделать системное администрирование проще. Нельзя установить разрешения доступа на автоматически созданных особых общих ресурсах. ОС Windows Server назначает разрешения доступом (можно

создать собственные скрытые ресурсы, добавив символ $ в качестве последнего символа общего ресурса).

Можно временно удалить особые общие ресурсы, если какие-то из них не нужны. Однако общие ресурсы будут созданы вновь при следующем запуске операционной системы. Для постоянного отключения административных общих ресурсов установите следующие значения реестра в 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer;

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks.

Какие особые ресурсы будут доступны, зависит от конфигурации системы. В табл. 2.1 перечислены специальные ресурсы и указано их использование.

Таблица 2.1. Особые общие ресурсы, используемые в Windows Server 2012

Имя ресурса	Описание	Использование
ADMIN$	время удаленного администрирования системы. Предоставляет доступ к папке %SystemRoot% операционной системы	На рабочих станциях и серверах администраторы и операторы архива могут получить доступ к этому ресурсу. На контроллерах домена доступ к этому ресурсу могут получить также операторы сервера
FAX$	Поддерживает сетевой факс	Используется факс-клиентами при отправке факсов
IPC$	Поддерживает именованные каналы во время межпроцессного взаимодействия	Используется программами при осуществлении удаленного администрирования и при просмотре общих ресурсов
NETLOGON	Поддерживает службу Net Logon	Используется службой Net Logon при обработке запросов входа в домен. Каждый пользователь имеет доступ Чтение к этому ресурсу
PRINT$	Поддерживает общие ресурсы принтера, предоставляя доступ к драйверам принтеров	Используется общими принтерами. У каждого пользователя есть доступ Чтение. Полный

		доступ к этому ресурсу имеют администраторы, операторы сервера и операторы печати
SYSVOL	Поддерживает Active Directory	Используется для хранения данных и объектов для Active Directory
Буква_диска$	Общий ресурс, позволяющий администраторам подключаться к корневой папке диска. Эти общие ресурсы показаны как C$, D$, E$ и т. д.	К этим ресурсам на рабочих станциях и серверах имеют доступ администраторы, операторы архива. На контроллерах домена также доступ к ресурсам есть и у операторов сервера

Подключение к особым ресурсам

Имена особых ресурсов заканчиваются символом $. Хотя эти ресурсы не отображаются в Проводнике, администраторы и определенные операторы могут подключаться к ним. Для подключения к специальному ресурсу выполните эти действия:

1. Откройте Проводник, перейдите на панель Компьютер (Computer).
2. Нажмите кнопку Подключить сетевой диск (Map Network Drive) на панели Компьютер. Откроется окно Подключение сетевого диска (Map Network Drive) (
3. В раскрывающемся списке Диск (Drive) выберите свободную букву диска. Она будет использоваться для доступа к особому ресурсу.
4. В поле Папка (Folder) введите UNC-путь к общему ресурсу. Например, для получения доступа к ресурсу C$ на сервере Twiddle введите \\TWIDDLE\C$.
5. Флажок Восстанавливать подключение при входе в систему (Reconnect At Sign-In) установлен автоматически, обеспечивая подключение сетевого диска при каждом входе пользователя в систему. Если нужно получить доступ к общему ресурсу только на время текущего сеанса, сбросьте этот флажок.
6. Если нужно подключиться к ресурсу с помощью других учетных данных, установите флажок Использовать другие учетные данные (Connect Using Different Credentials).
7. Нажмите кнопку Готово.

При попытке подключения посредством других учетных данных введите имя пользователя и пароль. Введите имя пользователя в формате домен\пользователь, например Cpandl\Williams. Перед нажатием кнопки OK установите флажок Запомнить учетные данные (Remember My Credentials),

если нужно сохранить учетные данные. В противном случае в будущем снова придется предоставить учетные данные.
После подключения к особому ресурсу с ним можно работать как с любым другим диском. Поскольку специальные ресурсы защищены, не нужно волноваться о доступе обычных пользователей к этим ресурсам. При первом подключении к ресурсу система может попросить ввести имя пользователя и пароль. Предоставьте эту информацию.

Просмотр сессий пользователя и компьютера

Оснастку Управление компьютером можно использовать для отслеживания всех соединений к общим ресурсам на системе Windows Server 2012. Независимо от того, кто подключился к ресурсу — пользователь или компьютер, Windows Server 2012 выводит соединение в узле Сеансы (Sessions).
Для просмотра соединений к общим ресурсам введите команду net session в командной строке или выполните следующие действия:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором был создан общий ресурс.
2. В дереве консоли разверните узел Служебные программы\Общие папки, а затем выберите узел Сеансы (Sessions). Теперь можно просмотреть соединения к общим ресурсам для пользователей и компьютеров.

Колонки в узле Сессии предоставляют следующую важную информацию о соединениях пользователей и компьютеров:

- Пользователь (User) — имя пользователя или компьютера, подключенного к общему ресурсу. Чтобы различать имена пользователей и компьютеров, к имени компьютера добавляется суффикс $;
- Компьютер (Computer) — имя используемого компьютера;
- Тип (Type) — тип используемого соединения;
- Количество открытых файлов (# Open Files) — число файлов, с которыми работает пользователь. Для более подробной информации (какие именно файлы открыты) перейдите в узел Открытые файлы (Open Files);
- Время подсоединения (Connected Time) — время, которое прошло с момента установки соединения;
- Время простоя (Idle Time) — время, прошедшее с момента последнего использования ресурса;
- Гость (Guest) — зарегистрирован ли пользователь как гость.

Управление сеансами и общими ресурсами

Управление сеансами и общими ресурсами — общая административная задача. Перед завершением работы сервера или приложения, запущенного на сервере, нужно отключить пользователей от общих ресурсов. Также нужно отключить пользователей, если планируется изменение прав доступа или удаление общего ресурса. Другая причина отключения пользователей — это избавление от

блокировок файлов. Отключить пользователей от общего ресурса можно путем завершения соответствующих сеансов пользователя.

Завершение отдельных сеансов

Для отключения отдельных пользователей от общего ресурса введите команду net session
\\computername /delete в командной строке или выполните эти действия:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел Служебные программы\Общие папки\Сеансы.
3. Щелкните правой кнопкой мыши на сеансе пользователя и выберите команду Закрыть сеанс (Close Session).
4. Нажмите кнопку Да для подтверждения действия.

Закрытие всех сеансов

Для отключения всех пользователей от общих ресурсов выполните эти действия:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором создан общий ресурс.
3. В дереве консоли разверните узел Служебные программы\Общие папки\Сеансы.
4. Выберите команду Отключить все сеансы (Disconnect All Sessions), а затем нажмите кнопку Да, чтобы подтвердить действие.

Помните, что пользователи отключаются от общих ресурсов, но не от домена. Чтобы заставить пользователей выйти из домена, можно использовать только часы входа и групповую политику. Отключение пользователей не означает отключение их от сети. Они просто отключаются от общего ресурса.

Управление открытыми ресурсами

Каждый раз, когда пользователи соединяются с общими ресурсами, открытые ими файлы и объекты ресурсов отображаются в узле Открытые файлы (Open Files). Узел Открытые файлы показывает файлы, открытые пользователем, но в данный момент не редактируемые.

Получить доступ к узлу Открытые файлы (Open Files) можно так:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел Служебные программы\Общие папки, а затем — Открытые файлы. Узел Открытые файлы предоставляет следующую информацию об использовании ресурса:
   – Открытый файл (Open File) — путь к файлу (или папке), который пользователь открыл на локальной системе. Путь также может быть именованным каналом, например \PIPE\spools, который используется для спула принтера;

- Пользователь (Accessed By) — имя пользователя, получающего доступ к файлу;
- Тип (Type) — тип используемого сетевого соединения;
- Блокир. (# Locks) — число блокировок ресурса;
- Режим открытия (Open Mode) — режим доступа, используемый при открытии ресурса, например, Чтение (read), Запись (write) или Чтение + Запись (read + write).

Закрытие открытого файла

Чтобы закрыть открытый на общем ресурсе файл, выполните следующие действия:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел Служебные программы\Общие папки\Открытые файлы.
3. Щелкните правой кнопкой мыши на файле, который нужно закрыть, а затем выберите команду Закрыть _____открытый файл (Close Open File).
4. Нажмите кнопку Да для подтверждения действия.

Закрытие всех открытых файлов

Для закрытия всех открытых файлов на общем ресурсе выполните эти действия:

1. В оснастке Управление компьютером подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли разверните узел Служебные программы\Общие папки\Открытые файлы. Щелкните правой кнопкой мыши по узлу Открытые файлы.
3. Выберите команду Отключить все открытые файлы (Disconnect All Open Files) и нажмите кнопку Да для подтверждения действия.

Прекращение общего доступа

Для прекращения доступа к папке:

1. Выполните одно из следующих действий:
   - в диспетчере серверов выберите общий ресурс в узле Файловые службы и службы хранилища\Общие ресурсы;
   - в оснастке Управление компьютеров подключитесь к компьютеру, на котором создан общий ресурс, и перейдите в раздел Общие ресурсы.
2. Щелкните правой кнопкой мыши на ресурсе, который нужно удалить, и выберите команду Прекратить общий доступ (Stop Sharing), а затем нажмите кнопку Да для подтверждения действия.

Никогда не удаляйте папку, содержащую общие ресурсы без предварительного прекращения общего доступа к ресурсам. Если не получилось прекратить общий доступ, ОС Windows Server 2012 попытается переустановить общие ресурсы при следующем запуске компьютера, и в результате вы получите ошибку, записанную в системный журнал событий.

Настройка общих ресурсов NFS

можно установить службу роли Сервер для NFS (Server for NFS) на файловый сервер. Служба предоставляет решение для совместного доступа к файлам на предприятии, где используются компьютеры под управлением Windows, OS X и UNIX, позволяя пользователям передавать файлы между операционными системами Windows Server 2012, OS X и UNIX с использованием протокола NFS (Network File System).

Можно настроить совместный доступ по протоколу NFS к локальным папкам на NTFStомах, используя Проводник. Также можно настроить общий NFS-доступ для локальных и удаленных папок на NTFS-томах посредством диспетчера серверов. В Проводнике для включения и настройки общего NFS-доступа выполните следующие действия:

1. Щелкните правой кнопкой мыши на общей папке и выберите команду Свойства. Будет показано окно Свойства для этой общей папки.
2. На вкладке Совместный доступ NFS (NFS Sharing) нажмите кнопку Управление доступом NFS (Manage NFS Sharing).
3. В окне Дополнительные параметры общего доступа NFS (NFS Advanced Sharing) установите флажок Открыть общий доступ к этой папке (Share This Folder),
4. В поле Общий ресурс (Share name) введите имя общего ресурса. Это имя папки, к которой будут подключаться UNIX-пользователи. Имена NFS-ресурсов должны быть уникальными для каждой системы и могут быть такими же, как и для стандартного общего доступа к файлам.
5. По умолчанию используется кодировка ANSI для отображения информации каталога и имен файлов. Если UNIX-компьютеры используют другую кодировку, можно выбрать ее из раскрывающегося списка Кодировка (Encoding).
6. UNIX-компьютеры по умолчанию используют аутентификацию Kerberos v5. Обычно также нужно разрешить целостность Kerberos и стандартную аутентификацию Kerberos. Установите флажки напротив механизмов аутентификации, которые нужно использовать. Снимите флажки тех методов, которые не планируется использовать.
7. Общий ресурс может быть настроен без проверки аутентификации серверов. Если не нужна аутентификация сервера, установите флажок Не использовать серверную проверку подлинности (No Server Authentication) и затем выберите дополнительные параметры. Доступ несопоставленным пользователям может быть разрешен и включен. Если нужно разрешить анонимным пользователям доступ к NFS-ресурсам, установите переключатель Разрешить анонимный доступ (Allow Anonymous Access) и укажите UID анонимного пользователя и GID анонимной группы.
8. Для UNIX-компьютеров доступ настраивается на основе имен компьютеров (они также называются именами хостов). По умолчанию ни один из UNIX-компьютеров не имеет доступ к NFS-ресурсу. Если нужно предоставить права чтения или чтения/записи, нажмите кнопку Разрешения, установите разрешения в окне Разрешения для общей

3. папки NFS (NFS Share Permissions) и нажмите кнопку OK. Можно настроить типы доступа Нет доступа (No Access), Только для чтения (Read-Only Access), Чтение и запись (Read/Write Access).
9. Нажмите кнопку OK дважды для закрытия открытых диалоговых окон и сохранения настроек.

В Проводнике можно отключить NFS-доступ так:

1. Щелкните правой кнопкой мыши на общей папке и выберите команду Свойства. Будет открыто одноименное окно для этой общей папки.
2. На вкладке Совместный доступ NFS нажмите кнопку Управление доступом NFS.
3. Сбросьте флажок Открыть общий доступ к этой папке и дважды нажмите кнопку OK.

В диспетчере серверов можно настроить NFS-разрешения как часть начальной конфигурации общего ресурса при его настройке. В подузле Общие ресурсы узла Файловые службы и службы хранилища можно создать NFS-ресурс так:

1. На панели Общие ресурсы выберите меню Задачи, а затем — Новый общий ресурс (New Share). Будет запущен мастер создания общих ресурсов (New Share Wizard). Выберите профиль Общий ресурс NFS — быстрый профиль или Общий ресурс NFS — дополнительные и нажмите кнопку Далее.
2. Укажите имя общего ресурса и расположение, как и в случае с SMB-ресурсом.
3. На странице Задайте способы проверки подлинности (Specify Authentication Methods) настройте аутентификацию Kerberos и аутентификацию без проверки подлинности сервера. Предоставленные опции подобны описанным ранее в этом разделе.
4. На странице Назначение разрешений для общей папки (Specify Share Permissions) настройте доступ для UNIX-узлов. Узлам (хостам) может быть предоставлен доступ на чтение или чтение/запись.
5. На странице Определение разрешений для управления доступом (Specify Permissions To Control Access) задайте NTFS-разрешения для общего ресурса.
6. На странице Подтверждение выбора (Confirm Selections) просмотрите все настройки. После нажатия кнопки Создать мастер создаст общий ресурс, настроит его и установит разрешения. В случае успешного создания ресурса будет отображено состояние "Общий ресурс успешно создан" (The share was successfully created). Если вместо этого появится ошибка, запишите ее и примите меры по ее исправлению перед повторением этой процедуры. Однако типичные ошибки касаются конфигурирования доступа хоста, и вероятно, не нужно повторять эту процедуру. Вместо этого следует изменить разрешения общего ресурса. Нажмите кнопку Закрыть.

Использование теневых копий

Если пользователи работают с общими папками, нужно рассмотреть создание теневых копий этих общих папок. Теневые копии (shadow copies) — резервные копии файлов данных, к которым пользователи могут получить доступ непосредственно в общих папках. Эти резервные копии могут сэкономить администраторам организации много времени, особенно если нужно получить потерянный, перезаписанный или поврежденный файл данных из резервной копии. Обычная процедура получения теневых копий — это использование Предыдущих версий (Previous Versions) или клиента Теневой копии. В Windows Server 2012, благодаря дополнительной функции, можно вернуть весь несистемный том в предыдущее состояние.

Что такое теневые копии

Теневые копии можно создать только на NTFS-томах и использовать для автоматического создания резервных копий файлов. Функция настраивается отдельно для каждого тома. Например, на файловом сервере есть три NTFS-тома, на каждом из них существуют общие папки, и нужно настроить эту функцию отдельно для каждого тома.

Если включить эту функцию в ее конфигурации по умолчанию, теневые копии будут создаваться дважды в неделю (в понедельник и пятницу) в 7 часов утра и в 12 часов вечера. Необходимо как минимум 100 Мбайт свободного пространства для создания первой теневой копии на томе. Общий объем дискового пространства зависит от объема данных, хранящихся в общих папках тома. Можно ограничить общий размер дискового пространства, используемый для хранения теневых копий, установив максимальный размер резервных копий.

Просмотреть и установить параметры теневых копий можно на вкладке Теневые копии (Shadow Copies) окна Свойства диска. В Проводнике или оснастке Управление компьютером щелкните на значке диска и выберите команду Свойства, а затем перейдите на вкладку Теневые копии1. Панель Выберите том (Select A Volume) показывает следующее:

- Том (Volume) — метка NTFS-тома на выбранном диске;
- Время следующего запуска (Next Run Time) — состояние теневой копии. Может быть указано либо значение Отключено (Disabled), либо время следующего создания теневой копии;
- Общие ресурсы — число общих папок на томе;
- Использовано (Used) — сколько дискового пространства заняла теневая копия.

Отдельные теневые копии выбранного в данный момент тома отображаются на панели Теневые копии выбранного тома (Shadow Copies Of Selected Volume) с сортировкой по дате и времени.

Создание теневых копий

Чтобы создать теневую копию на NTFS-томе с общими папками, выполните следующие действия:

1. Откройте оснастку Управление компьютером. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел Запоминающие устройства (Storage), а затем — Управление дисками. Будут показаны тома, сконфигурированные на выбранном компьютере.
3. Щелкните правой кнопкой мыши на узле Управление дисками и выберите команду меню Все задачи | Настроить теневые копии (All tasks | Configure shadow copies).
4. На вкладке Теневые копии (Shadow Copies) в списке Выберите том (Select a volume) выберите том, который нужно настроить.
5. Нажмите кнопку Параметры (Settings) для настройки максимального размера всех теневых копий для этого тома и изменения расписания по умолчанию. Нажмите кнопку OK.
6. После настройки параметров теневых копий тома нажмите кнопку Включить (Enable), если необходимо. Для подтверждения действия нажмите кнопку Да. Включение теневых копий создает первую теневую копию и устанавливает расписание для следующих теневых копий.

Если создается расписание путем настройки параметров теневой копии, теневое копирование будет автоматически включено после нажатия кнопки OK в окне Параметры. Однако первая теневая копия не будет создана до следующего запланированного раза. Если нужно создать теневую копию тома прямо сейчас, выберите том и нажмите кнопку Создать (Create).

Восстановление теневой копии

Пользователи, работающие на клиентских компьютерах, получают доступ к теневым копиям отдельных общих папок, используя функцию Предыдущие версии (Previous Versions) или Клиент теневых копий. Лучший способ получить доступ к теневым копиям клиентского компьютера — следовать этим рекомендациям:

1. В Проводнике щелкните правой кнопкой мыши по общему ресурсу, доступ к предыдущим версиям файлов которого нужно получить, и выберите команду Свойства, а затем перейдите на вкладку Предыдущие версии (Previous Versions).
2. На вкладке Предыдущие версии выберите папку, с которой нужно работать. Для каждой папки выводится дата изменения. Нажмите кнопку, соответствующую действию, которое необходимо выполнить:
   - нажмите кнопку Открыть (Open), чтобы открыть теневую копию в Проводнике;
   - нажмите кнопку Копировать (Copy) для отображения окна Копирование элементов (Copy Items), которое используется для копирования теневой копии папки в выбранное расположение;
   - нажмите кнопку Восстановить (Restore), чтобы сделать откат общей папки в ее состояние на момент создания выбранной версии.

Восстановление предыдущего состояния всего тома

Операционная система Windows Server 2012 содержит улучшение функции теневых копий, позволяющее возвращать целый том к состоянию, в котором он был на момент создания определенной теневой копии. Поскольку тома, содержащие файлы операционной системы, не могут быть восстановлены, восстанавливаемый том не должен быть системным. Это же касается и томов на общем кластерном диске.

Чтобы восстановить предыдущее состояние тома, выполните эти действия:

1. Откройте оснастку Управление компьютером. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел Запоминающие устройства (Storage), а затем выберите узел Управление дисками, щелкните на нем правой кнопкой мыши и выберите команду меню Все задачи | Настроить теневые копии (All tasks | Configure shadow copies).
3. На вкладке Теневые копии (Shadow copies) выберите том из списка Выберите том (Select a volume).
4. Отдельные теневые копии выбранного в данный момент тома отображаются на панели Теневые копии выбранного тома (Shadow copies of selected volume) с сортировкой по дате и времени. Выберите нужную теневую копию и нажмите кнопку Восстановить (Revert).
5. Чтобы подтвердить это действие, установите флажок Выполнить откат состояния этого тома (Check here if you want to revert this volume) и нажмите кнопку Откатить (Revert now). Нажмите кнопку OK, чтобы закрыть окно Теневые копии.

Удаление теневых копий

Каждая контрольная точка может обслуживаться отдельно. Можно удалить отдельные теневые копии тома при необходимости. Эта операция восстановит дисковое пространство, занятое теневыми копиями.

Для удаления теневой копии действия:

1. Откройте оснастку Управление компьютером. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел Запоминающие устройства, а затем щелкните правой кнопкой мыши по узлу Управление дисками. Выберите команду меню Все задачи | Настроить теневые копии.
3. На вкладке Теневые копии выберите том из списка Выберите том.
4. Отдельные теневые копии выбранного в данный момент тома отображаются на панели Теневые копии выбранного тома с сортировкой по дате и времени. Выберите нужную теневую копию, которую следует удалить, и нажмите кнопку Удалить. Нажмите кнопку Да для подтверждения действия.

Отключение теневых копий

Если больше не планируется использование теневых копий тома, можно отключить функцию Теневые копии. Отключение этой функции выключает

расписание автоматических резервных копий и удаляет существующие теневые копии.
Для отключения теневых копий тома выполните следующие действия:

1. Откройте оснастку Управление компьютером. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел Запоминающие устройства, а затем щелкните правой кнопкой мыши по узлу Управление дисками. Выберите команду меню Все задачи | Настроить теневые копии.
3. На вкладке Теневые копии выберите том из списка Выберите том, а затем нажмите кнопку Отключить (Disable).
4. Для подтверждения действия нажмите кнопку Да. Нажмите кнопку OK для закрытия окна Теневые копии.

Подключение к сетевым дискам

Пользователи могут подключаться к сетевым дискам и к общим ресурсам, доступным в сети. Это соединение будет показано значком сетевого диска, к которому пользователи могут получить доступ как к любому другому диску в своих системах.
Когда пользователи подключаются к сетевым дискам, проверяются не только разрешения общих ресурсов, но и разрешения файлов и папок Windows Server 2012. Различие в этих наборах разрешений — обычная причина отказа в доступе к определенному файлу или подпапке на сетевом диске.

Сопоставление сетевого диска

В ОС Windows Server 2012 подключение к сетевому диску осуществляется путем его сопоставления буквы диска общему ресурсу с использованием команды NET USE:
net use DeviceName \\ComputerName\ShareName
Здесь DeviceName определяет букву диска, можно указать символ * для использования следующей доступной буквы диска, а \\ComputerName\ShareName — UNC-путь к общему ресурсу, например:
net use g: \\ROMEO\DOCS
или
*net use * \\ROMEO\DOCS*
Чтобы убедиться, что сопоставленный диск будет доступен при следующем входе в систему, сделайте его постоянным, добавив опцию /Persistent:Yes.
Если клиентский компьютер работает под управлением Windows 8, можно сопоставить сетевые диски, выполнив следующие действия:

1. В Проводнике щелкните по крайнему левому переключателю в списке адресов, а затем выберите элемент Компьютер (Computer).
2. На панели Компьютер нажмите кнопку Подключить сетевой диск (Map Network Drive), а затем выберите команду Подключить сетевой диск (сначала нужно нажать на кнопку, а потом выбрать такую же команду из появившегося меню).

3. Используйте список Диск (Drive) для выбора свободной буквы диска, а затем нажмите кнопку Обзор справа от поля Папка (Folder). В окне Обзор папок разверните сетевые папки, чтобы можно выбрать имя рабочей группы или домена, с которым нужно работать.
4. Если развернуть имя компьютера в рабочей группе или домене, будет отображен список общих папок. Выберите необходимую общую папку и нажмите кнопку OK.
5. Установите флажок Восстанавливать подключение при входе в систему (Reconnect At Logon), если нужно, чтобы Windows автоматически подключалась к общей папке в начале каждого сеанса.
6. Нажмите кнопку Готово. Если у текущего пользователя нет надлежащих разрешений доступа для общего ресурса, выберите Использовать другие учетные данные (Connect Using Different Credentials) и затем нажмите кнопку Готово. После нажатия кнопки

Готово можно будет ввести имя пользователя и пароль, которые будут использоваться для подключения к общей папке. Введите имя пользователя в формате домен\пользователь, например, Cpandl\Williams. Перед нажатием кнопки OK отметьте флажок Запомнить учетные данные (Remember My Credentials), если нужно сохранить учетные данные. В противном случае в будущем вновь придется предоставить учетные данные.

Отключение сетевого диска

Для отключения сетевого диска выполните следующие действия:

1. В Проводнике щелкните по крайнему левому переключателю в списке адресов, а затем выберите элемент Компьютер.
2. В группе Сетевое расположение (Network location) щелкните правой кнопкой мыши по значку сетевого диска и выберите команду Отключить (Disconnect).

Управление объектами, владением и наследованием

Операционная система Windows Server 2012 использует объектно-ориентированный подход для описания ресурсов и управления разрешениями. Объекты, которые описывают ресурсы, определены на NTFS-томе и в Active Directory. В случае с NTFS-томами можно установить разрешения для файлов и папок. В Active Directory можно установить разрешения для других типов объектов, например, пользователей, компьютеров и групп. Эти разрешения могут использоваться для точного управления доступом.

Объекты и диспетчеры объектов

Независимо от того, где определены объекты, на NTFS-томе или в Active Directory, у каждого типа объектов есть диспетчер объектов и основные средства управления. Диспетчер объектов контролирует параметры и разрешения объекта. Основные средства управления — это средства для работы с объектом. Объекты, их диспетчеры и средства управления представлены в табл. 2.2.

Таблица 2.2. Объекты Windows Server 2012

Тип объекта	Диспетчер объекта	Средство управления
Файлы и папки	NTFS	Проводник
Принтеры	Диспетчер очереди печати	Принтеры в Панели управления
Ключи реестра	Реестр Windows	Редактор реестра
Службы	Контроллеры служб	Набор инструментов настройки безопасности
Общие ресурсы	Служба Сервер	Проводник, оснастка Управление компьютером, Управление общими ресурсами и хранилищами

Владение объектом и передача владения

Важно понимать концепцию владения объектом. В Windows Server 2012 владелец объекта не обязательно должен быть его создателем. Вместо этого, владелец объекта — это лицо, обладающее непосредственным контролем над объектом. Владельцы объектов могут назначить разрешения доступа и передать владение объектом другим пользователям.

Администратор может получить право владения объектов в сети. Это гарантирует, что для авторизированных администраторов не будет блокироваться доступ к файлам, папкам, принтерам и другим ресурсам. В большинстве случаев, как только администратор получит владение файлом, он не сможет вернуть его предыдущему владельцу. Это сделано специально, чтобы администраторы не могли получить доступ к файлам, а затем не пытались скрыть этот факт.

Способ назначения владения первоначально зависит от расположения создаваемого объекта. В большинстве случаев группа Администраторы является текущим владельцем, а фактический создатель указан как лицо, которое может получить владение объектом.

Передача владения может осуществляться несколькими способами:

- если группа Администраторы изначально назначена владельцем, создатель объекта получит владение при условии, что он сделает это раньше других;
- текущий владелец может предоставить разрешение Смена владельца (Take Ownership) другим пользователям, позволяя этим пользователям принять владение объектом;
- администратор может стать владельцем объекта при условии, что объект находится под его административным контролем.

Чтобы стать владельцем объекта, выполните эти действия:

1. Откройте программу управления объектом. Например, если нужно работать с файлами и папками, откройте Проводник.
2. Щелкните правой кнопкой мыши на объекте, владельцем которого нужно стать, а затем выберите команду Свойства. В окне Свойства перейдите на вкладку Безопасность.
3. На вкладке Безопасность нажмите кнопку Дополнительно, чтобы открыть окно Дополнительные параметры безопасности (Advanced Security Settings). В нем текущий владелец выводится под названием файла или папки.
4. Нажмите кнопку Изменить. Используйте окно Выбор: "Пользователь", "Компьютер", "Учетная запись службы" или "Группа" (Select Users, Computers, Service Accounts, or Groups) для выбора нового владельца.
5. Нажмите кнопку OK дважды, когда будете готовы.

При изменении владельца папки также можно изменить и владельца для всех вложенных объектов (подпапок и файлов), установив флажок Сменить владельца вложенных контейнеров и объектов (Replace Owner On Subcontainers And Objects). Эта опция работает не только с файлами, но и с другими объектами. Она изменяет владельца всех дочерних объектов.

Наследование объекта

Объекты определяются посредством родительско-дочерней структуры. Родительский объект — это объект верхнего уровня. Дочерний объект — это объект, определенный ниже родительского объекта в иерархии. Например, папка C:\ является родительской для папок C:\Data и C:\Backups. Любые папки, созданные в C:\Data и C:\Backups, являются дочерними для этих папок и "внуками" для C:\.

Дочерние объекты могут наследовать разрешения из родительских объектов. Фактически, все объекты Windows Server 2012 по умолчанию созданы с включенным наследованием. Это означает, что дочерние объекты автоматически наследуют разрешения родительского объекта. Поэтому разрешения родительского объекта контролируют доступ к дочернему объекту. Если нужно сменить разрешения дочернего объекта, необходимо сделать следующее:

1. Отредактируйте разрешения родительского объекта.
2. Остановите наследование разрешений из родительского объекта и затем назначьте разрешения дочернему объекту.
3. Выберите противоположное разрешение, чтобы переопределить наследованное разрешение. Например, если родитель разрешает какое-то право, необходимо его запретить на дочернем объекте.

Для остановки наследования разрешений из родительского объекта выполните эти действия:

1. Откройте утилиту управления объектом. Например, если нужно работать с файлами и папками, откройте Проводник.

2. Щелкните правой кнопкой мыши на объекте, владельцем которого нужно стать, а затем выберите команду Свойства. В окне Свойства перейдите на вкладку Безопасность.
3. Нажмите кнопку Дополнительно, чтобы отобразить окно Дополнительные параметры безопасности.
4. На вкладке Разрешения нажмите кнопку Изменить разрешения для отображения редактируемой версии вкладки Разрешения.
5. На вкладке Разрешения, если наследование в данный момент включено, будет отображена кнопка Отключение наследования (Disable Inheritance). Нажмите ее.
6. Теперь можно преобразовать наследованные разрешения в явные разрешения объекта или удалить все наследованные разрешения и применить только те, которые явно установлены на папке или файле.

Помните, что если удалить наследованные разрешения и не назначить никаких других разрешений, всем, кроме владельца, будет запрещен доступ к объекту.
Это эффективно блокирует доступ каждого, кроме владельца файла или папки. Однако администраторы все еще имеют право захватить владение объектом, независимо от установленных разрешений. Таким образом, если доступ к файлу или папке блокирован для администратора, он может стать владельцем файла и затем получить неограниченный доступ.
Для включения наследования выполните следующие действия:

1. Откройте утилиту управления объектом, например Проводник.
2. Щелкните правой кнопкой мыши на объекте, владельцем которого нужно стать, а затем выберите команду Свойства. В окне Свойства перейдите на вкладку Безопасность.
3. Нажмите кнопку Дополнительно, чтобы отобразить окно Дополнительные параметры безопасности.
4. На вкладке Разрешения нажмите кнопку Включение наследования, а затем кнопку OK. Обратите внимание, что кнопка Включение наследования доступна, только если наследование в данный момент выключено.

Разрешения файла и папки

Разрешения NTFS всегда обрабатываются, как только происходит доступ к файлу. На томах NTFS и ReFS можно установить права доступа к файлам и папкам. Эти разрешения предоставляют или запрещают доступ к файлам и папкам. Поскольку ОС Windows Server 2012 добавляет новые уровни безопасности, полномочия NTFS теперь охватывают следующие виды разрешений:

- базовые разрешения;
- разрешения на основе требований;
- особые разрешения.

Можно просмотреть NTFS-разрешения для папок и файлов так:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду Свойства. В окне Свойства перейдите на вкладку Безопасность.
2. В списке Группы или пользователи (Group or user names) выберите учетную запись пользователя, компьютера или группы, разрешения которой нужно просмотреть. Если разрешения недоступны, то они наследуются из родительского объекта.

Как было сказано ранее в этой главе, у общих папок есть и разрешения общего доступа, и разрешения NTFS. Можно просмотреть разрешения NTFS для общих папок так:

1. В диспетчере серверов перейдите в узел Общие ресурсы, показывающий существующие общие ресурсы серверов, добавленных для управления.
2. Щелкните правой кнопкой мыши на папке и выберите команду Свойства. Откроется окно Свойства.
3. Выберите Разрешения на панели слева, будут показаны разрешения общего ресурса и разрешения NTFS.
4. Чтобы получить больше информации, нажмите кнопку Настройка разрешений (Customize Permissions) для отображения окна Дополнительные параметры безопасности.

На файловых серверах под управлением Windows Server 2012 также можно использовать централизованные политики доступа для точного определения специальных атрибутов, которые должны иметь пользователи и устройства для доступа к ресурсам.

Подробности о разрешениях файлов и папок

Базовые разрешения, которые можно назначить файлам и папкам, представлены в табл. 2.3. Разрешения файла включают Полный доступ, Изменение, Чтение и выполнение, Чтение и Запись. Разрешения папок включают Полный доступ, Изменение, Чтение и выполнение, Список содержимого папки, Чтение и Запись.

Таблица 2.3. Разрешения файла и папки, используемые в Windows Server 2012

Разрешение	Значение для папок	Значение для файлов
Чтение (Read)	Разрешает обзор папок и просмотр списка файлов и подпапок	Разрешает просмотр или доступ к содержимому файла
Запись (Write)	Разрешает добавлять файлы и подпапки	Разрешает запись в файл
Чтение и выполнение (Read & Execute)	Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется файлами и папками	Разрешает просмотр и доступ к содержимому файла, а также запуск исполняемого файла (программы)
Список содержимого папки (List Folder Contents)	Разрешает обзор папок и просмотр списка файлов и подпапок;	--

	наследуется только папками	
Изменение (Modify)	Разрешает просмотр содержимого и создание файлов и подпапок; разрешает удаление папки	Разрешает чтение и запись данных в файл; разрешает удаление файла
Полный доступ (Full Control)	Разрешает просмотр содержимого, а также создание, изменение и удаление файлов и подпапок	Разрешает чтение и запись данных, а также изменение и удаление файла

При работе с разрешениями файла и папки нужно помнить о следующем:

- чтение — это единственное право, необходимое для запуска сценариев. Право выполнения здесь не имеет значения;
- для доступа к ярлыку и связанному объекту требуется разрешение на чтение;
- разрешение на запись в файл при отсутствии разрешения на удаление файла все еще позволяет пользователю удалять содержимое файла;
- если пользователь получит разрешение Полный доступ к папке, он может удалять любые файлы в такой папке, независимо от разрешений на доступ к этим файлам.

Базовые разрешения созданы при помощи объединения в логические группы особых разрешений. Особые разрешения, предусмотренные для создания базовых разрешений для файлов. Используя дополнительные параметры безопасности, можно индивидуально назначать эти особые разрешения, если необходимо. При изучении особых разрешений для файлов нужно учитывать следующее:

- по умолчанию, если пользователю явно не предоставлены права доступа, то доступ к файлу для него закрыт;
- действия, которые пользователи могут выполнять, основываются на сумме всех назначенных пользователю разрешений и разрешений всех групп, членом которых он является. Например, если пользователь GeorgeJ имеет доступ на чтение и в то же время входит в группу Techies, у которой есть доступ на изменение, то в результате у пользователя GeorgeJ тоже появляется доступ на изменение. Если группу Techies включить в группу Администраторы с полным доступом, то GeorgeJ будет полностью контролировать файл.

Особые разрешения, используются для создания базовых разрешений для папок. Здесь необходимо учитывать, что при создании файлов и папок они наследуют некоторые разрешения из родительских объектов. Эти разрешения показываются как разрешения по умолчанию.

Установка базовых разрешений файла и папки

Чтобы установить базовые NTFS-разрешения для файлов и папок, выполните следующие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду Свойства. В окне Свойства перейдите на вкладку Безопасность.
2. Нажмите кнопку Изменить для отображения редактируемой версии вкладки Безопасность
3. Пользователи или группы, которые уже имеют доступ к файлу или папке, выводятся в списке Группы или пользователи. Можно изменить разрешения для этих пользователей или групп так:
   - выберите пользователей или группы, которые нужно изменить;
   - разрешите или запретите разрешения в списке Разрешения для.

Наследованные разрешения отображаются серым (недоступны). Если нужно переопределить наследованные разрешения, выберите противоположные разрешения.

4. Для установки разрешений доступа для дополнительных пользователей, компьютеров или групп нажмите кнопку Добавить. Появится окно Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы".
5. Введите имя пользователя, компьютера или группы в текущем домене и нажмите кнопку Проверить имена. Далее возможен один из следующих сценариев:
   - если найдено одно совпадение, диалоговое окно будет обновлено и найденная запись будет подчеркнута;
   - если совпадения не были найдены, введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку Размещение для выбора нового размещения;
   - если найдено несколько совпадений, выберите имя или имена, которые нужно использовать, и нажмите кнопку OK. Для добавления нескольких пользователей, компьютеров или групп введите точку с запятой (;) и затем повторите этот шаг.

Кнопка Размещение позволяет получить доступ к именам учетных записей в других доменах. Нажмите кнопку Размещение, чтобы увидеть список из текущего домена, доверенных доменов и других ресурсов, к которым есть доступ. Благодаря транзитивным довериям в Windows Server 2012 обычно можно получить доступ ко всем доменам в доменном дереве или лесу.

6. В списке Группы или пользователи выберите учетную запись пользователя, компьютера, группы, которую нужно настроить, и установите разрешения в списке Разрешения для. Повторите этот процесс для других пользователей, компьютеров или групп.
7. Нажмите кнопку OK.

Поскольку у общих папок также есть NTFS-разрешения, может понадобиться установить базовые NTFS-разрешения с использованием диспетчера серверов. Чтобы сделать это, выполните следующие действия:

1. В консоли Диспетчер серверов щелкните правой кнопкой мыши на папке и выберите команду Свойства. Откроется одноименное окно.
2. Выберите на левой панели элемент Разрешения, будут отображены текущие разрешения общего ресурса и NTFS-разрешения на основной панели.
3. Нажмите кнопку Настройка разрешения для открытия окна Дополнительные параметры безопасности с активной вкладкой Разрешения.
4. Пользователи и группы, уже имеющие доступ к файлу или папке, перечислены в списке Элементы разрешений (Permission Entries). Используйте предоставленные параметры для просмотра, редактирования, добавления или удаления разрешений для пользователей или групп.

Установка особых разрешений для файлов и папок

Для установки особых NTFS-разрешений для файлов и папок выполните следующие действия:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите команду Свойства.
2. В окне Свойства перейдите на вкладку Безопасность и нажмите кнопку Дополнительно для отображения окна Дополнительные параметры безопасности. Перед изменением разрешений нужно нажать кнопку Изменить разрешения. Разрешения будут представлены в том порядке, в котором они находятся на вкладке Безопасность. Основные отличия — отображаются индивидуальные наборы разрешений, указано, наследованы ли разрешения и от кого, а также перечислены ресурсы, к которым применены разрешения.
3. Если для пользователя или группы уже установлены разрешения для папки или файла (и эти разрешения не наследуются), можно изменить специальные разрешения, выбрав пользователя или группу и нажав кнопку Изменить. Пропустите шаги 4—7 и следуйте оставшимся рекомендациям в этой процедуре.
4. Чтобы добавить особые разрешения для пользователя или группы, нажмите кнопку Добавить для отображения окна Элемент разрешения (Permission Entry). Щелкните по ссылке Выберите субъект (Select a principal) для отображения окна Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы".
5. Введите имя учетной записи пользователя или группы. Убедитесь, что ссылаетесь на имя учетной записи, а не на полное имя пользователя. Только одно имя может быть введено за один раз.
6. Нажмите кнопку Проверить имена. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В

противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку Размещение для выбора нового размещения. Если найдено несколько совпадений, в окне Найдено несколько имен (Multiple Names Found) выберите имя, которое нужно использовать, и нажмите кнопку OK.

8. Нажмите кнопку OK. Пользователь или группа будут добавлены как Субъект (Principal), и окно Элемент разрешения обновится для отображения этого факта.
9. По умолчанию отображаются только базовые разрешения. Щелкните по ссылке Отображение дополнительных разрешений (Show advanced permissions) для отображения особых разрешений
10. Используйте раскрывающийся список Тип, чтобы указать, что нужно сделать: разрешить или запретить особые разрешения. А затем выберите особые разрешения, которые нужно разрешить или запретить. Если разрешение недоступно, значит, оно наследуется от родительской папки. Можно разрешать и запрещать любые особые разрешения выборочно. Поэтому, если нужно и разрешить, и запретить особые разрешения, необходимо настроить разрешение, а потом повторить эту процедуру, начиная с шага 1, для запрещения.
11. Если доступен раскрывающийся список Применяется к (Applies to), выберите надлежащую опцию. Доступны следующие опции:
    - Только для этой папки (This folder only) — разрешения будут применены только для выбранной в данный момент папки;
    - Для этой папки, ее подпапок и файлов (This folder, subfolders and files) — разрешения применяются к этой папке, ко всем ее подпапкам и ко всем файлам в этих папках;
    - Для этой папки и ее подпапок (This folder and subfolders) — разрешения применяются к этой папке и к любой подпапке этой папки. Они не применяются к файлам в этих папках;
    - Для этой папки и ее файлов (This folder and files) — разрешения применяются к этой папке и к любому файлу в ней. Они не применяются к подпапкам этой папки;
    - Только для подпапок и файлов (Subfolders and files only) — разрешения применяются к любой подпапке этой папки и к любому файлу в этих папках. Но они не применяются к самой папке;
    - Только для подпапок (Subfolders only) — разрешения применяются только к подпапкам, но не затрагивают ни файлы, ни саму папку;
    - Только для файлов (Files only) — разрешения применяются к любым файлам в папке и в ее подпапках. Разрешения не применяются к самой папке и ее подпапкам.
12. Нажмите кнопку OK.

Поскольку у общих папок также есть NTFS-разрешения, можно задать особые NTFS-разрешения, используя консоль Диспетчер серверов:

1. В консоли Диспетчер серверов выберите узел Файловые службы и службы хранилища, а затем выберите Общие ресурсы. Щелкните правой кнопкой мыши по папке и выберите команду Свойства. Откроется одноименное окно.
2. В разделе Разрешения (на левой панели) отображаются текущие разрешения общего доступа и NTFS-разрешения.
3. Нажмите кнопку Настройка разрешений, чтобы открыть окно Дополнительные параметры безопасности с активной вкладкой Разрешения.
4. Пользователь и группы, для которых разрешения уже установлены, приведены в списке Элементы разрешений. Используйте предоставленные параметры для просмотра, редактирования, добавления или удаления разрешений для пользователей или групп. При редактировании выполните шаги 8—11 предыдущей процедуры для работы с особыми разрешениями.

Установка разрешений на основе требований

Средства управления доступом на основе требований используют комплексную проверку подлинности, включающую типы требований, которые являются утверждениями об объектах на базе атрибутов Active Directory, и свойства ресурса, классифицирующие объекты, и описывают их атрибуты. Когда доступ к ресурсам осуществляется удаленно, средства управления доступом на основе требований и центральные политики доступа полагаются на защиту Kerberos (Kerberos with Armoring) для аутентификации требований устройства. Защита Kerberos улучшает защиту домена, разрешая присоединенным к домену клиентам и контроллерам домена взаимодействовать по зашифрованным каналам.

Для тонкой настройки доступа используются разрешения на основе требований. Администратор определяет условия, ограничивающие доступ; это делается как часть установки дополнительных разрешений безопасности ресурса. Обычно эти условия добавляют требования устройств или требования пользователя к средствам управления доступом. Требования пользователя идентифицируют пользователей, а требования устройства — устройства. Например, можно определить типы требований на основе бизнес-категории или кода страны с помощью атрибутов Active Directory: businessCode и countryCode соответственно. Используя эти типы требований, можно гибко настроить доступ и гарантировать, что только пользователям, устройствам или обоим типам, принадлежащим определенной деловой категории или конкретной стране, будет предоставлен доступ к ресурсу. Также можно определить свойства ресурса Project для еще более тонкой настройки доступа.

С помощью централизованных политик доступа определяют централизованные правила доступа в Active Directory, эти правила применяются динамически по всему предприятию.

Централизованные правила доступа используют условные выражения, требующие определения свойств ресурса, типы требований и/или группы безопасности, необходимые для политики, а также серверы, где должна быть применена политика.

Перед определением и применением условий требований к файлам и папкам компьютера нужно включить политику на основе требований. Для компьютеров, не подсоединенных к домену, это можно сделать путем включения и настройки политики Поддержка KDC требований, комплексной проверки подлинности и защиты Kerberos (KDC Support For Claims, Compound Authentication And Kerberos Armoring) в разделе Конфигурация компьютера\Административные шаблоны\Система\Центр распространения ключей (Computer Configuration\Administrative Templates\System\KDC). Можно задать один из режимов работы политики:

- Поддерживается (Supported) — контроллеры домена поддерживают требования (утверждения), комплексную проверку подлинности и защиту Kerberos. Компьютеры клиентов, не поддерживающие защиту Kerberos, могут быть аутентифицированы;
- Всегда предоставлять утверждения (Always Provide Claims) — то же самое, что и режим Поддерживается, но контроллеры домена всегда поддерживают утверждения для учетных записей;
- Отклонять запросы проверки подлинности без защиты (Fail Unarmored Authentication) — защита Kerberos обязательна. Клиенты, не поддерживающие ее, не могут быть аутентифицированы.

Политика Поддержка KDC требований, комплексной проверки подлинности и защиты Kerberos контролирует, будут ли клиенты Kerberos, работающие под управлением Windows 8 и Windows Server 2012, запрашивать утверждения и комплексную аутентификацию.

Политика должна быть включена для Kerberos-совместимых клиентов для запроса утверждений и комплексной аутентификации. Данная политика называется Поддержка динамического контроля доступа и защиты Kerberos (Dynamic Access Control and Kerberos armoring) и находится в узле Конфигурация компьютера\Политики\Административные шаблоны\Система \Центр распространения ключей.

Нужно включить политику на основе требований для приложений по всему домену для всех контроллеров домена, чтобы гарантировать непротиворечивость приложения. Для этого она обычно включается и настраивается через объект групповой политики Default Domain Controllers или GPO самого высокого уровня, связанного с организационным подразделением контроллеров домена.

Как только основанная на требованиях политика включена и настроена, можно определить условия требования так:

1. В Проводнике щелкните правой кнопкой мыши на файле или папке и выберите Свойства. В открывшемся окне перейдите на вкладку Безопасность и нажмите кнопку Дополнительно, чтобы открыть окно Дополнительные параметры безопасности.

2. Если у пользователя или группы уже есть разрешения для файла или папки, можно отредактировать их существующие разрешения. Выберите пользователя, с которым нужно работать, и нажмите кнопку Изменить, а после пропустите шаги 3—6.
3. Нажмите кнопку Добавить для отображения окна Элемент разрешения (Permission Entry). Щелкните по ссылке Выберите субъект для отображения окна Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы".
4. Введите имя пользователя или группы. Убедитесь, что ссылаетесь на учетную запись пользователя, а не на его полное имя. За один раз можно добавить только одно имя.
5. Нажмите кнопку Проверить имена. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку Размещение для выбора нового размещения. Если будет найдено несколько совпадений, откроется окно Найдено несколько имен, выберите имя и нажмите кнопку OK.
6. Нажмите кнопку OK, и группа или пользователь будут добавлены как Субъект (Principal). Щелкните по ссылке Добавить условие (Add a condition).
7. Используйте предоставленные опции для определения условия или условий, при соответствии которым будет предоставлен доступ. Для пользователей и групп установите базовые требования на основе членства в группе и/или ранее определенных типов требований. Для устройств определите условия для правильных значений.
8. Нажмите кнопку OK.

Поскольку общие папки также имеют NTFS-разрешения, можно установить разрешения на основе требований с использованием диспетчера серверов. Чтобы сделать это, выполните следующие действия:

1. В консоли Диспетчер серверов щелкните правой кнопкой мыши на папке и выберите команду Свойства для отображения одноименного окна.
2. На панели слева выберите элемент Разрешения, на основной панели будут отображены разрешения общего ресурса и NTFS-разрешения.
3. Нажмите кнопку Настройка разрешений, чтобы открыть окно Дополнительные параметры безопасности с активной вкладкой Разрешения.
4. Пользователи и группы, у которых уже есть доступ к файлу или папке, перечислены в списке Элементы разрешений. Используйте предоставленные опции для просмотра, редактирования, добавления или удаления разрешений для пользователей или групп.

При редактировании или добавлении разрешений в окне Элемент разрешения можете добавить условия, как было показано в действиях 6—8 предыдущей процедуры.

Аудит системных ресурсов

Аудит — лучший способ для отслеживания событий в системах Windows Server 2012.

Аудит можно использовать для сбора информации, связанной с использованием какоголибо ресурса. Примерами событий для аудита могут являться доступ к файлу, вход в систему и изменение конфигурации системы. После включения аудита объекта в журнал безопасности системы заносятся записи при любой попытке доступа к этому объекту. Журнал безопасности можно просмотреть из оснастки Просмотр событий (Event Viewer).

Для изменения большинства настроек аудита необходимо войти в систему с учетной записью Администратор или члена группы Администраторы или иметь право Управление аудитом и журналом безопасности (Manage Auditing and Security Log) в групповой политике.

Установка политик аудита

Политики аудита существенно повышают безопасность и целостность систем. Практически каждая система в сети должна вести журналы безопасности. Можно настроить политики аудитов для отдельных компьютеров с помощью локальной групповой политики и для всех компьютеров в доменах с помощью групповой политики Active Directory. Посредством групповой политики можно установить политики аудита для целого сайта, домена или подразделения. Также возможно задать политики для персональных рабочих станций или серверов. Выберите GPO и выполните следующие действия для установки политик аудита:

1. В редакторе управления групповыми политиками перейдите к узлу Политика аудита (Audit Policy). Для этого разверните узел Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy).
2. Существуют следующие категории аудита:
   - Аудит событий входа в систему (Audit Account Logon Events) — отслеживает события, связанные с входом пользователя в систему и выходом из нее;
   - Аудит управления учетными записями (Audit Account Management Tracks) — отслеживает все события, связанные с управлением учетными записями средствами ос-настки Active Directory — пользователи и компьютеры. Записи аудита генерируются при создании, изменении или удалении учетных записей пользователя, компьютера или группы;
   - Аудит доступа к службе каталогов (Audit Directory Service Access) — отслеживает события доступа к каталогу Active Directory. Записи аудита генерируются каждый раз при доступе пользователей или компьютеров к каталогу;

- Аудит входа в систему (Audit Logon Events) — отслеживает события входа в систему или выхода из нее, а также удаленные сетевые подключения;
- Аудит доступа к объектам (Audit Object Access) — отслеживает использование системных ресурсов файлами, каталогами, общими ресурсами и объектами Active Directory;
- Аудит изменения политики (Audit Policy Change) — отслеживает изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений;
- Аудит использования привилегий (Audit Privilege) — отслеживает каждую попытку применения пользователем предоставленного ему права или привилегии. Например, права архивировать файлы и каталоги;
- Аудит отслеживания процессов (Audit Process Tracking) — отслеживает системные процессы и ресурсы, используемые ими;
- Аудит системных событий (Audit System Events) — отслеживает события запуска, перезагрузки или выключения компьютера, а также события, влияющие на системную безопасность или отражаемые в журнале безопасности.

3. Для настройки политики аудита дважды щелкните на нужной политике или щелкните правой кнопкой мыши на записи и выберите команду Свойства.
4. В появившемся окне установите флажок Определить следующие параметры политики (Define these policy settings), а затем установите либо флажок Успех (Success), либо флажок Отказ (Failure), либо оба флажка. Флажок Успех регистрирует успешные события, например успешные попытки входа. Флажок Отказ регистрирует неудачные события, например неудачные попытки входа в систему.
5. Нажмите кнопку OK.

Политика Аудит использования привилегий не отслеживает события, связанные с доступом к системе, такие как использование права на интерактивный вход в систему или на доступ к компьютеру из сети. Эти события отслеживаются с помощью политики аудита входа в систему.

Когда аудит включен, журнал безопасности будет отображать следующее:

- идентификаторы события 560 и 562 — аудит пользователя;
- идентификаторы события 592 и 593 — аудит процесса.

Аудит файлов и папок

Если GPO настроен для включения политики Аудит доступа к объектам, можно установить уровень аудита для отдельных файлов и папок. Это позволит точно отслеживать их использование. Данная возможность доступна только на томах с файловой системой NTFS.

Настроить аудит реестра можно с помощью следующих действий:

1. Откройте редактор реестра (regedit.exe). В командной строке или в поле поиска приложений введите regedit и нажмите клавишу <Enter>.
2. Перейдите к ключу реестра, который нужно отслеживать. Далее из меню Правка (Edit) выберите команду Разрешения (Permissions). В окне Разрешения нажмите кнопку Дополнительно. В окне Дополнительные параметры безопасности перейдите на вкладку Аудит.
3. Нажмите кнопку Добавить для отображения окна Элемент аудита. Щелкните по ссылке Выберите субъект для отображения окна Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы".
4. В этом окне введите Все (Everyone) и нажмите кнопку Проверить имена, а затем нажмите кнопку OK.
5. В окне Элемент аудита отображаются только базовые разрешения. Щелкните по ссылке Отображения дополнительных разрешений, чтобы отобразить особые разрешения.
6. Используйте список Применяется к, чтобы указать, как будет применяться элемент аудита.
7. Используйте раскрывающийся список Тип для уточнения, какие события (успешные, неудачные или оба типа) будут регистрироваться. Обычно нужно отслеживать следующие особые разрешения:
   - задание значения — успех и отказ;
   - создание подраздела — успех и отказ;
   - удаление — успех и отказ.
8. Нажмите кнопку OK три раза, чтобы закрыть все открытые диалоговые окна и применять настройки аудита.

Аудит объектов Active Directory

Если задействована политика Аудит доступа к службе каталогов, можно использовать аудит на уровне объектов службы каталогов Active Directory. Это позволит точно отслеживать их использование.

Для настройки аудита объекта проделайте следующее:

1. В оснастке Active Directory — пользователи и компьютеры убедитесь, что в меню Вид выбрана опция Дополнительные компоненты, а затем перейдите в контейнер, содержащий объект.
2. Дважды щелкните по объекту для аудита. Будет открыто окно Свойства.
3. Перейдите на вкладку Безопасность, затем нажмите кнопку Дополнительно.
4. В окне Дополнительные параметры безопасности перейдите на вкладку Аудит. Список Элементы аудита показывает пользователей, группы или компьютеры, действия которых уже отслеживаются. Для удаления учетной записи из этого списка выберите ее и нажмите кнопку Удалить.
5. Для добавления особых учетных записей нажмите кнопку Добавить, чтобы открыть окно Элемент аудита. Щелкните по ссылке Выберите субъект для отображения окна Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы".

6. Введите имя пользователя, компьютера или группы в текущем домене или нажмите кнопку Проверить имена. Если отыщется одно совпадение, диалоговое окно обновится, а найденная запись будет подчеркнута. В противном случае откроется дополнительное окно. Если совпадения не обнаружились, значит, было введено некорректное имя или выбрано некорректное размещение. Измените имя и попытайтесь снова или нажмите кнопку Размещение для выбора нового размещения. Если найдено несколько совпадений, в окне Найдено несколько имен выберите имя или имена и нажмите кнопку OK.
7. Нажмите кнопку OK для возврата в окно Элемент аудита. Используйте список Применяется к, чтобы определить, как элемент аудита будет применен.
8. Используйте раскрывающийся список Тип, чтобы указать, какие события (успех, отказ или оба типа) нужно регистрировать. Успех регистрирует успешные события, например успешную попытку модификации разрешений объекта. Отказ регистрирует неудачные события, например неудачную попытку изменения владельца объекта.
9. Нажмите кнопку OK. Повторите этот процесс для аудита других пользователей, групп или компьютеров. Использование, настройка и управление дисковых квот файловой системы NTFS

Операционная система Windows Server 2012 поддерживает два взаимоисключающих типа дисковых квот.

- Дисковые квоты файловой системы NTFS поддерживаются всеми выпусками Windows Server 2012 и позволяют администратору управлять использованием дискового пространства пользователями. Квоты настраиваются для каждого тома. Хотя пользователи, которые превысили лимиты, увидят предупреждения, администраторы будут уведомлены через журнал событий.
- Дисковые квоты диспетчера ресурсов поддерживаются всеми выпусками Windows Server 2012 и позволяют управлять использованием дискового пространства на уровне папки и тома. Пользователи, которые скоро превысят лимит или уже превысили его, могут быть автоматически уведомлены по электронной почте. Система уведомления также позволяет уведомлять по электронной почте администраторов, протоколировать соответствующие события и запускать команды. Далее мы рассмотрим дисковые квоты NTFS.

Независимо от того, какая система дисковых квот была выбрана, можно настроить квоты только на NTFS-тома. Нельзя создать квоты на FAT-, FAT32- или ReFS-томах.

Когда задаются дисковые квоты, нужно быть предельно внимательным при выборе способа их применения, особенно в отношении системных учетных записей, учетных записей служб или других учетных записей особого назначения. Неправильное применение дисковых квот к учетным записям этих типов может вызвать серьезные проблемы, которые трудно диагностировать и решить. Установив квоты на учетных записях System, NetworkService или

LocalService, можно препятствовать выполнению важных задач операционной системы. Например, если эти учетные записи достигнут определенного лимита квоты, нельзя будет применить изменения в групповой политике, поскольку клиент групповой политики работает окнах. А это означает, что нужно связываться с локальным диспетчером пользователя или с контроллером домена Active Directory в случае необходимости.
После того как операционная система Windows Server 2012 преобразует имена, она кэширует их в локальном файле, поэтому они будут моментально доступны в следующий раз, когда понадобятся. Кэш запроса нечасто обновляется — если заметите несоответствие между тем, что отображено, и тем, что настроено, нужно обновить информацию. Обычно следует выбрать команду Обновить (Refresh) из меню Вид (View) или просто нажать клавишу <F5> в текущем окне.

Установка политик дисковых квот файловой системы NTFS

Лучший способ настроить дисковые квоты NTFS — применить групповую политику. При настройке дисковых квот с помощью локальной политики или через политику организационного подразделения, домена или сайта определяется общая политика, которая будет установлена автоматически, как только будет включено управление квотами на отдельных томах. Таким образом, вместо настройки каждого отдельного тома можно использовать один и тот же набор правила и применять их поочередно к каждому тому, которым нужно управлять.
Политики, контролирующие дисковые квоты NTFS, применяются на уровне системы и находятся в разделе Конфигурация компьютера\Административные шаблоны\Система\Дисковые квоты (Computer Configuration\Administrative Templates\System\Disk Quotas).
При работе с пределами квоты нужно использовать стандартный набор политик на всех системах. Как правило, не нужно включать все политики. Вместо этого необходимо выборочно включить политики и затем использовать стандартные функции NTFS, чтобы управлять квотами на разных томах. Для включения квот выполните следующие действия:

1. Откройте групповую политику для системы (например, для файлового сервера). Перейдите к узлу Дисковые квоты (Disk Quotas), развернув узел Конфигурация компьютера\Административные шаблоны\Система (Computer Configuration\Administrative Templates\System).
2. Дважды щелкните по параметру политики Включить дисковые квоты (Enable disk quotas). Выберите Включено (Enabled) и нажмите кнопку OK.
3. Дважды щелкните по элементу Обеспечить соблюдение дисковой квоты (Enforce Disk Quota Limit). Если нужно обеспечить соблюдение дисковых квот на всех NTFS-томах этого компьютера, выберите значение Включено (Enabled), в противном случае выберите значение Выключено (Disabled) и затем установите квоты отдельно для каждого тома. Нажмите кнопку OK.

4. Дважды щелкните по параметру политики Определить квоту и порог предупреждений по умолчанию (Specify default quota limit and warning level). В диалоговом окне установите переключатель Включено.
5. В поле Квота по умолчанию (Default quota limit) установите лимит дискового пространства по умолчанию, который будет применен к пользователям, когда они впервые запишут данные на том с этими включенными квотами. Квота не применяется к текущим пользователям. Для корпоративного общего ресурса, например, используемого членами команды проекта, можно установить квоту от 5 до 10 Гбайт. Конечно, размер квоты зависит от размера файлов, с которыми работают пользователи, от числа пользователей и размера тома. Дизайнерам и инженерам данных может понадобиться больше дискового пространства.
6. Для установки порога предупреждений пролистайте вниз окно Параметры (Options). Хороший порог — 90% от квоты по умолчанию, это означает, что если установлена квота размером 10 Гбайт, порог предупреждения нужно установить в 9 Гбайт. Нажмите кнопку OK.
7. Дважды щелкните на параметре Записать в журнал событие при превышении квоты (Log event when quota limit exceeded). Установите переключатель Включено, чтобы при достижении пользователями предела квоты соответствующее событие записывалось в журнал приложений, и нажмите кнопку OK.
8. Дважды щелкните на параметре Записать в журнал событие при превышении порога предупреждения (Log event when quota warning level exceeded). Установите переключатель Включено, чтобы при достижении пользователями порога предупреждения соответствующее событие записывалось в журнал приложений, и нажмите кнопку OK.
9. Дважды щелкните на параметре Применить политику к съемным носителям (Apply policy to removable media). Установите переключатель Отключено — квоты не будут применяться к съемным томам компьютера. Затем нажмите кнопку OK.

Чтобы убедиться, что политики были применены немедленно, перейдите в узел Конфигурация компьютера\Административные шаблоны\Система\ Групповая политика (Computer Configuration\Administrative Templates\System \Group Policy) и дважды щелкните на политике Настройка обработки политики дисковых квот (Configure Disk Quota Policy Processing). Выберите переключатель Включено, а затем — Обрабатывать, даже если объекты групповой политики не изменились (Process Even If The Group Policy Objects Have Not Changed). Нажмите кнопку OK.

Включение дисковых квот на томах NTFS

Установить дисковые квоты NTFS можно отдельно для каждого тома. Дисковые квоты могут быть включены только для томов с файловой системой NTFS. После настройки надлежащих групповых политик можно использовать оснастку Управление компьютером для установки дисковых квот локальных и удаленных томов.

Если используется параметр политики Обеспечить соблюдение дисковой квоты (EnforceDisk Quota Limit), пользователи не смогут записать данные на диск, если они превысили квоту. Этот параметр перезаписывает параметр на вкладке Квота (Quota) тома NTFS.

Для включения дисковых квот на NTFS-томе выполните следующие действия:

1. Откройте оснастку Управление компьютером. Если необходимо, подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел Запоминающие устройства, а затем выберите Управление дисками. На основной панели будут отображены тома, настроенные на компьютере.
3. Используйте представление Список томов или Графическое представление, щелкните на томе и выберите команду Свойства.
4. На вкладке Квота установите флажок Включить управление квотами (Enable quota management). Если квоты уже включены через групповую политику, эти параметры будут недоступны, и их нельзя изменить. Вместо этого нужно модифицировать параметры через групповую политику.

При работе с вкладкой Квота обратите особое внимание на текст Состояние (Status) и значок светофора. Если квоты не настроены, светофор показывает красный свет, а состояние сообщит, что дисковые квоты отключены. Если операционная система обновляет квоты, светофор покажет желтый свет, а Состояние отобразит выполняемое действие. Если квоты настроены, светофор покажет зеленый свет, а текст состояния сообщит, что квоты активны.

5. Для установки квоты по умолчанию для всех пользователей выберите переключатель Выделять на диске не более (Limit disk space to). В текстовом поле введите лимит в килобайтах, мегабайтах, гигабайтах, терабайтах, петабайтах или эксабайтах. Затем установите параметр Порог выдачи предупреждений (Set warning level to). Обычно порог выдачи предупреждений соответствует 90—95% от дисковой квоты.Хотя квота и порог предупреждения по умолчанию применяются ко всем пользователям, можно настроить разные уровни для отдельных пользователей. Это можно сделать в окне Записи квот (Quota Entries). Если создано много уникальных записей квот и нет желания создавать их на томе с одинаковыми характеристиками и использованием, можно экспортировать записи квот и импортировать их на другой том.
6. Чтобы обеспечить соблюдение квоты и запретить пользователям запись данных на диск после превышения лимита, установите флажок Не выделять место на диске при превышении квоты (Deny disk space to users exceeding quota limit). Помните, что включение этого параметра создаст фактическое физическое ограничение для пользователей, но не для администраторов.
7. Для настройки протоколирования, когда пользователи превысят порог предупреждения или квоту, установите флажки Регистрация... (Log event...). Нажмите кнопку OK для сохранения изменений.

8. Если квоты системы в данный момент выключены, будет отображено окно, спрашивающее разрешения включить квоты. Нажмите кнопку OK для разрешения Windows Server 2012 пересканировать том и обновить статистику использования диска. Против пользователей, превышающих квоту или порог, могут быть предприняты меры. Эти меры могут включать предотвращение записи на том, уведомление и регистрацию событий в журнале приложений.

Просмотр записей квот

Дисковое пространство отслеживается отдельно для каждого пользователя. Если дисковые квоты включены, у каждого пользователя, записывающего данные на том, есть запись в файле дисковой квоты. Эта запись периодически обновляется, чтобы показать используемое в данный момент дисковое пространство, предельную квоту, порог предупреждения и процент допустимого использованного пространства. Администратор может изменить записи квот для установки разных квот и порогов предупреждения для определенных пользователей. Администратор также может создать записи квот для пользователей, у которых еще нет сохраненных данных на томе. Основная причина создания записи заключается в том, чтобы у пользователя, работающего с томом, была надлежащая квота и порог предупреждения.

Для просмотра текущих записей квот для тома выполните следующие действия:

1. Откройте оснастку Управление компьютером. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел Запоминающие устройства, а затем выберите Управление дисками. На основной панели будут отображены тома, настроенные на компьютере.
3. Используйте представление Список томов или Графическое представление, щелкните на томе и выберите команду Свойства.
4. На вкладке Квоты нажмите кнопку Записи квот. Откроется одноименное окно. Каждая запись приводится согласно состоянию. Состояние позволяет быстро узнать, превысил ли пользователь квоту. Состояние OK означает, что пользователь работает в пределах квоты. Любое другое состояние обычно означает, что пользователь достиг либо порога предупреждения, либо предела квоты.

Создание записей квоты

Администратор может создать записи квот для пользователей, которые еще не сохраняли данные на томе. Это позволяет установить квоту и порог предупреждения для конкретного пользователя. Обычно эта функция используется, когда пользователь часто сохраняет больше информации, чем другие пользователи, и надо разрешить ему использовать больше пространства, чем остальным пользователям, либо когда нужно установить определенный лимит для администраторов. Как было ранее отмечено, администраторы не являются субъектами дисковых квот, поэтому если нужно задать квоты для

отдельных администраторов, необходимо создать записи квот для каждого администратора, которого надо ограничить.
Нельзя создавать отдельные записи квот хаотически. Необходимо тщательно отслеживать отдельные записи. В идеале, можно хранить журнал, который детализирует любые отдельные записи так, чтобы другие администраторы поняли, какие политики используются и как они применены. При изменении основных правил томов на томе нужно повторно исследовать отдельные записи, чтобы увидеть, применимы ли они все еще или должны быть обновлены. Автор книги обнаружил, что определенные типы пользователей — чаще исключение, чем правило, и поэтому иногда лучше поместить отдельные классы пользователей на разные тома и затем применять дисковые квоты к каждому тому. Таким образом, у каждого класса пользователей будет квота, подходящая для типичных задач, выполняемых пользователями. Например, можно создать отдельные тома для руководителей, менеджеров иобычных пользователей или можно создать отдельные тома для управляющих, дизайнеров, инженеров и всех остальных пользователей.
Для создания записи квоты на томе выполните следующие действия:

1. Откройте окно Записи квот, как было описано ранее в этой главе. Окно содержит записи квот для всех пользователей. Для обновления окна нажмите клавишу <F5> или выберите команду Вид | Обновить.
2. Если у пользователя еще нет записи на этом томе, можно создать ее, выбрав команду Квота | Создать запись квоты (Quota | New quota entry). Откроется окно Выбор: "Пользователи".
3. В этом окне введите имя пользователя в поле Введите имя выбираемых объектов (Enter the object names to select), а затем нажмите кнопку Проверить имена. Если совпадение найдено, выберите учетную запись и нажмите кнопку OK. Если совпадений не будет, введите другое имя и повторите поиск снова. Повторите этот шаг при необходимости и затем нажмите кнопку OK.
4. После выбора пользователя появится окно Добавление новой квоты (Add New Quota Entry). Есть две опции. Мож но удалить все ограничения квот для этого поль-зователя, выбрав переключатель Не ограничивать выделение места на диске (Do notlimit disk usage), или установить определенную квоту и порог предупреждений, выбрав переключатель Выделять на диске не более (Limit disk space to) (после этого нужно ввести надлежащие значения). Нажмите кнопку OK.

Удаление записей квот

Если пользователю больше не нужно использовать том, а для него созданы записи квот, можно удалить соответствующие записи. При удалении записи квоты все файлы связанного с записью пользователя будут собраны и отображены в окне, и можно будет безвозвратно удалить эти файлы, сменить их владельца или переместить эти файлы в папку на другом томе.
Для удаления записи квоты для пользователя и управления оставшимися файлами пользователя выполните следующие действия:

1. Откройте окно Записи квот, как было описано ранее в этой главе. Окно содержит записи квот для всех пользователей. Для обновления окна нажмите клавишу <F5> или выберите команду Вид | Обновить.
2. Выберите запись дисковой квоты, которую нужно удалить, и нажмите клавишу <Delete>или выберите команду Удалить запись квоты (Delete Quota Entry) из меню Квота. Несколько записей можно выделить с помощью клавиш <Shift> и <Ctrl>.
3. Для подтверждения действия нажмите кнопку Да. Откроется окно Дисковая квота, содержащее список файлов, принадлежащих выбранному пользователю (пользователям).
4. В списке Файлы, которыми владеет (List files owned by) отображаются файлы для пользователя, чья запись квоты удаляется. Можно обработать каждый файл отдельно, выбрав отдельные файлы и надлежащее действие, а можно выбрать несколько файлов с помощью клавиш <Shift> и <Ctrl>. Доступны следующие опции:
   - Удалить (Permanently delete files) — выберите файлы для удаления и нажмите кнопку Удалить. Для подтверждения действия нажмите кнопку Да;
   - Сменить владельца (Take ownership of files) — выберите файлы, для которых нужно сменить владельца, и нажмите кнопку Сменить владельца;
   - Переместить (Move files to) — выберите файлы, которые нужно переместить, и затем введите путь к папке на другом томе. Если не знаете точный путь, используйте кнопку Обзор для отображения окна Обзор папок. Как только будет найдена надлежащая папка, нажмите кнопку Переместить (Move).
5. Нажмите кнопку Закрыть. Если надлежащим образом были обработаны все файлы пользователя, запись квоты будет удалена.

Экспорт и импорт дисковых квот NTFS

Вместо повторного создания пользовательских записей квот на отдельных томах можно экспортировать настройки с исходного тома и затем импортировать их на другой том. Оба тома должны быть отформатированы в NTFS. Для экспорта и последующего импорта записей квот выполните следующие действия:

1. Откройте окно Записи квот, как было описано ранее в этой главе. Окно содержит записи квот для всех пользователей. Для обновления окна нажмите клавишу <F5> или выберите команду Вид | Обновить.
2. Выберите запись квоты и команду Квота | Экспорт (Quota | Export). Будет отображено окно Параметры экспорта квоты (Export Quota Settings). Выберите размещение для файла квоты, введите его имя в поле Имя файла и нажмите кнопку Сохранить. В окне сохранения файла квоты можно просто ввести имя файла и нажать кнопку Сохранить. Так будет проще импортировать файл. Файлы квоты очень маленькие, поэтому не нужно беспокоиться об использовании дискового пространства.

3. Выберите команду Квота | Закрыть (Quota | Close) для закрытия окна Записи квот.
4. Щелкните правой кнопкой мыши на узле Управление компьютером и выберите команду Подключиться к другому компьютеру (Connect to another computer). В окне Выбор компьютера (Select Computer) выберите компьютер, содержащий целевой том. Целевой том — этот тот том, на который нужно импортировать экспортированные записи квот.
5. Как было описано ранее, откройте окно Свойства целевого тома. Перейдите на вкладку Квота и нажмите кнопку Записи квот. Откроется одноименное окно для целевого тома.
6. Выберите команду Квота | Импорт (Quota | Import). В окне Параметры импорта квоты (Import Quota Settings) выберите ранее сохраненный файл и нажмите кнопку Открыть.
7. Если том содержит предыдущие записи квот, можно либо заменить существующие записи, либо сохранить их. Нажмите кнопку Да для замены существующей записи или кнопку Нет для сохранения существующей записи. Для применения своего выбора ко всем записям квот установите флажок Применить ко всем записям квот (Do this for all quota entries), а затем нажмите кнопку Да или Нет.

Отключение дисковых квот NTFS

Отключить квоты можно для отдельных пользователей или для всех пользователей на томе. При отключении квоты для отдельного пользователя этот пользователь больше не является предметом ограничения квот, но дисковые квоты все еще отслеживаются для других пользователей. При отключении квот на томе отслеживание и управление квотами будут полностью удалены. Для отключения квот конкретного пользователя следуйте рекомендациям из разд. "Просмотр записей квот" ранее в этой главе. Для отключения отслеживания квот на всем томе выполните следующие действия:

1. Откройте оснастку Управление компьютером и при необходимости подключитесь к удаленному компьютеру.
2. Откройте окно Свойства для тома, на котором нужно отключить квоты NTFS.
3. На вкладке Квота установите флажок Включить управление квотами. Нажмите кнопку OK. Когда увидите запрос, еще раз нажмите кнопку OK.

Использование, настройка и управление квотами диспетчера ресурсов

Операционная система Windows Server 2012 поддерживает расширенную систему управления квотами, называемую дисковыми квотами диспетчера ресурсов (Resource Manager disk quotas). Используя эти квоты, администратор может управлять использованием дискового пространства папки и тома.

Поскольку управление дисковыми квотами диспетчера ресурсов осуществляется отдельно от дисковых квот NTFS, можно настроить один том на использование обоих систем квотирования. Однако рекомендуется применять какую-то одну систему. Альтернативно, если уже настроены

дисковые квоты NTFS, можно продолжить использовать их для ограничения дискового пространства на томах, а для важных папок использовать квоты диспетчера ресурсов.

Понимание дисковых квот диспетчера ресурсов

При работе с Windows Server 2012 можно использовать дисковые квоты диспетчера ресурсов — это еще один инструмент, который администратор может применять для управления использованием дискового пространства. Можно настроить квоты диспетчера ресурсов для ограничения дискового пространства тома или папки. Администратор устанавливает либо жесткий лимит — означает, что предел квоты не может быть превышен, либо мягкий лимит — предел квоты может быть превышен.

Вообще говоря, использовать жесткие лимиты необходимо, когда нужно запретить пользователям превышать определенное ограничение дискового пространства. Задавать мягкие лимиты нужно для простого контроля использования дискового пространства и предупреждения пользователей, которые превышают или собираются превысить квоты. У всех квот есть путь к основному файлу на томе или папке, к которому применена квота. Квота применяется к выбранному тому или папке и ко всем подпапкам выбранного тома или папки. В шаблоне квоты, определяющем свойства квоты, задается то, как квоты работают и как пользователи будут ограничены или предупреждены.

Используя утилиту Диспетчер ресурсов файлового сервера (File Server Resource Manager), можно легко определить дополнительные шаблоны, которые будут доступны при создании квот, или установить единожды свойства квот при определении квоты. Шаблоны квот определяют следующее:

- предел — предел использования дискового пространства;
- тип квоты — жесткая или мягкая;
- порог уведомления — тип уведомления, возникающего при процентном превышении заданного предела.

Несмотря на то, что у каждой квоты есть определенный предел и тип, возможно определение нескольких порогов предупреждений. Порог предупреждения — процентное соотношение от порога квоты, которое меньше 100%. Например, можно инициировать предупреждения на 85 и 95% квоты и окончательное уведомление, когда будет достигнуто все 100% квоты.

Пользователи, которые вот-вот превысят предел или уже превысили его, могут быть автоматически уведомлены по электронной почте. Система уведомления также поддерживает уведомление администраторов по электронной почте, инициирование создания отчетов, запуск команд и журналирование событий.

Управление шаблонами квот

Шаблоны квот используются для определения свойств квоты, в том числе предела, типа квоты и порогов уведомлений. В утилите Диспетчер ресурсов файлового сервера можно просмотреть определенные в данный момент шаблоны квот, развернув узел Управлениеквотами и выбрав узел Шаблоны квот.

Изменить существующие шаблоны квот можно так:

1. В утилите Диспетчер ресурсов файлового менеджера разверните узел Управление квотами, а затем выберите Шаблоны квот. Будут отображены определенные в данный момент шаблоны квот.
2. Чтобы модифицировать свойства шаблона квоты, дважды щелкните на нем. Откроется окно Свойства шаблона квоты
3. На вкладке Параметры (Settings) можно установить имя шаблона, предел и тип квоты. Также выводятся определенные в данный момент пороги уведомления. Для изменения существующего порога уведомления выделите его и нажмите кнопку Изменить. Для определения нового порога нажмите кнопку Добавить.
4. Когда закончите изменять параметры шаблона, нажмите кнопку OK для сохранения параметров.

Создать новый шаблон можно с помощью этих действий:

1. В утилите Диспетчер ресурсов файлового менеджера разверните узел Управление квотами, а затем выберите Шаблоны квот.
2. Из меню Действие или на панели Действия выберите команду Создать шаблон квот (Create Quota Template). Откроется окно Создание шаблона квоты (Create Quota Template).
3. На вкладке Параметры установите имя шаблона, предел и тип квоты. Сначала нужно установить порог используемого пространства, а затем задать дополнительные пороговые значения для уведомлений. В поле Порог (Limit) введите значение и укажите, в ка-ких единицах будет измеряться предел — в килобайтах, мегабайтах, гигабайтах или терабайтах.
4. Нажмите кнопку Добавить, чтобы добавить пороговое значение для уведомлений. В окне Добавление порога (Add Threshold) введите значение в поле Создавать уведомления, когда достигает (%) (Generate Notifications When Usage Reaches (%)). Процентное значение порога уведомления должно быть меньше 100. Предельный порог фиксируется, когда достигается 100% квоты. 5. На вкладке Сообщение электронной почты (E-Mail Message) можно настроить уведомления так.
   - Для уведомления администратора, что достигнут порог квоты, установите флажок Отправить сообщения следующим администраторам (Send E-Mail To The Following Administrators) и введите электронные адреса или адрес. Несколько адресов разделяются точкой с запятой. Используйте переменную [Admin Email] , чтобы указать администратора по умолчанию, ранее указанного в глобальных параметрах.
   - Для уведомления пользователей установите флажок Отправить сообщения пользователям, превысившим порог (Send e-mail to the user who exceeded the threshold) ивведите содержимое письма уведомления в поля Тема (Subject) и Текст сообщения (Message body).
5. На вкладке Журнал событий (Event Log) можно настроить журналирование событий. Установите флажок Записывать

предупреждения в журнал событий (Send Warning To Event Log) для включения журналирования и затем укажите текст записи журнала в поле Запись журнала (Log entry). В табл. 12.8 приведены доступные переменные и их значения.

6. На вкладке Отчет (Report) установите флажок Создать отчет (Generate reports) для включения отчета об инциденте и затем выберите типы отчетов для создания. Отчеты по умолчанию сохраняются в папке %SystemDrive%\StorageReports\Incident по умолчанию, и они могут также быть отправлены назначенным администраторам. Используйте переменную [Admin Email] , чтобы указать администраторов по умолчанию, ранее указанных в глобальных параметрах.
7. Повторите действия 5—7 для определения дополнительных порогов уведомлений.
8. Нажмите кнопку OK, когда закончите создавать шаблон.
9. Создание квот диспетчера ресурсов Чтобы просмотреть определенные в данный момент дисковые квоты, запустите утилиту Диспетчер ресурсов файлового сервера и разверните узел Управление квотами, а затем выберите узел Квоты. Перед определением дисковых квот нужно сначала определить группы файлов, к которым будут применяться квоты, и шаблоны квот, как было показано в разд. "Управление шаблонами квот" ранее в этой главе.

После определения необходимых групп файлов и шаблонов квот можно создать квоты так:

1. В утилите Диспетчер ресурсов файлового сервера разверните узел Управление квотами, а затем выберите узел Квоты.
2. Из меню Действие или из панели Действия выберите команду Создать квоту.
3. В окне Создание квоты укажите локальный путь для квоты, нажмите кнопку Обзор и затем, используя окно Обзор папок, укажите путь, например C:\Data. Нажмите кнопку OK.
4. В списке Наследовать свойства из следующего шаблона (Derive properties from this quota template) выберите шаблон квот, который будет использоваться.
5. Нажмите кнопку Создать.

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

Администрирование данных Windows Server 2012

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