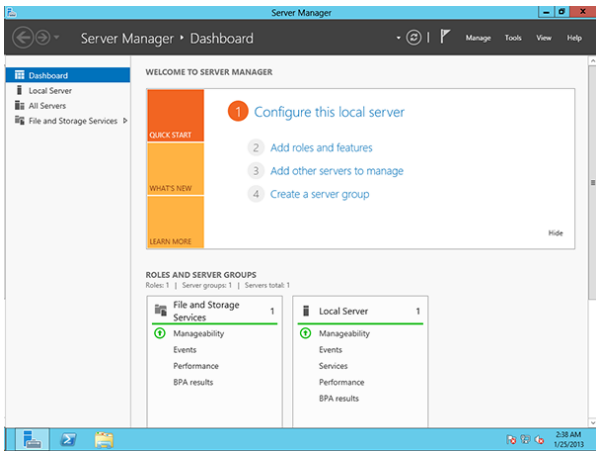
Тема занятия:

Windows Server 2012 с точки зрения системного администратора, обзор возможностей

Введение

По прошествии четырех лет разработки, 4 сентября 2012 года, Microsoft объявила о доступности новой версии Windows Server — Microsoft Windows Server 2012.



Исторически операционные системы линейки Windows Server — это ОС, предназначенные для управления аппаратным обеспечением серверов, обладающие требуемыми для этого функциональными особенностями. Также эти серверные ОС содержат специализированные службы (программные компоненты), предназначенные для организации, мониторинга и управления ИТ-инфраструктурой предприятия, начиная от управления адресным пространством протокола IP и учетными записями пользователей и заканчивая организацией отказоустойчивых сетевых сервисов.

Если мы посмотрим на ИТ-инфраструктуру предприятий образца 10-летней давности, то в большом количестве случаев увидим т. н. модель «on-premise», когда серверное аппаратное обеспечение приобреталось предприятиями в собственность, на каждом сервере разворачивался экземпляр операционной системы, настраивались ее комплектные службы, устанавливалось прочее программное обеспечение, реализующее дополнительную функциональность. В этой классической модели ИТ-инфраструктуры предприятия взаимодействие, как правило, строилось по схеме клиент—сервер, причем под клиентом в подавляющем большинстве случаев понимался ПК. То есть клиентский ПК, как устройство, на сетевом уровне взаимодействовал через локальную сеть с сервером, а на уровне приложений некое клиентское приложение взаимодействовало с соответствующим серверным.

В то же время, сейчас в индустрии мы видим трансформацию этой модели в модель «подключенных устройств и непрерывных сервисов». Всё большее количество пользователей работает со всё более и более возрастающим количеством разнообразнейших подключенных к интернету устройств: смартфонами, планшетами, ноутбуками, настольными ПК и даже «умными» телевизорами. На стороне «серверов» предприятия пользователи ожидают уже не просто серверных приложений, взаимодействующих с единственным их устройством, но непрерывно, 24×7×365, функционирующих сервисов: «облачных», умных, надежных, быстрых, соответствующим образом обрабатывающих и умеющих синхронизировать данные между всеми

устройствами. То есть нужна серверная операционная система, которая позволила бы строить такие сервисы. Растет и количество данных: в реляционных БД, текстовых документах и электронных таблицах накапливается все большее количество информации.

В условиях такой трансформации Microsoft поставила перед собой цель выпустить настоящую «облачную» операционную систему — платформу масштаба уже не единичного сервера, но центра обработки данных (ЦОД) с единообразными подходами и инструментами для управления и разработки приложений в частном, партнерском, глобальном облаке и гибридных вариантах. По аналогии с тем, как Microsoft перепридумала клиентскую ОС Windows, серьезному переосмыслению подверглась и парадигма серверной ОС Windows Server.

Ключевыми строительными блоками здесь являются Windows Server 2012, Windows Azure и System Center 2012 SP1.

Говоря «облачная операционная система», Microsoft понимает под этим четыре группы требований к серверной ОС:

1. Преобразование ЦОД. Необходимо иметь возможность взять все ресурсы ЦОД (хранение, сеть, вычислительные мощности), разделить их между облачными службами, обеспечить возможность высокой загрузки (эффективного использования) этих ресурсов. Нужно иметь возможность гибкого масштабирования, то есть для любой конкретной службы необходимо иметь возможность выделения ей дополнительных ресурсов, но только на то время, когда они ей нужны. Необходимо иметь возможность строить инфраструктуру, работающую в режимах always-up и always-on (всегда включено и всегда доступно). Необходимо иметь возможность автоматизирования задач по управлению ЦОД посредством API и порталов самообслуживания.
2. Необходимо иметь возможность размещения современных приложений поверх такой инфраструктуры. Нужно иметь большой набор работающих служб, позволяющих строить социальные, мобильные приложения и приложения для обработки сверхбольших массивов данных, т. е. поддержать все современные тренды. Предприятиям необходимо иметь гибкость в инструментарии, в среде разработки, чтобы быстро строить эти приложения. Необходимо иметь быстрый цикл разработки, который объединял бы разработчиков и управленцев.
3. Microsoft ставил перед собой задачу поддержать тенденцию BYOD (bring your own device = приноси свое собственное устройство) на предприятиях, в то же время обеспечивая необходимые контроль и управление со стороны ИТ-службы.
4. Необходимо было поддержать возможности по обработке и хранению любых массивов данных с любой парадигмой хранения: как SQL, так и NoSQL, совместно обрабатывать данные предприятия и данные из внешних структурированных источников, создавая новые возможности.

Результатом явилось построение облачной операционной системы и платформы. Новая ОС может быть развернута в своем ЦОД, можно использовать ее как услугу из партнерского ЦОД или из глобальной Windows Azure; при этом обеспечивается единый подход к виртуализации, инфраструктуре управления, инфраструктуре разработки приложений, управлению данными и сервисами идентификации.

Однако новая ОС несет множество новаций и усовершенствований и для тех, кто не планирует переселяться в облака ;)

Редакции и лицензирование в линейке Windows Server 2012

Обычно вопросы лицензирования, редакций и их ограничений у всех производителей — одни из самых непростых. В линейке Windows Server 2012 структура упрощена и унифицирована по сравнению с предыдущим поколением.

В линейке Windows Server 2012 доступны 4 редакции.

Редакция	Основное предназначение	Основные особенности	Модель лицензирования	Цена на условиях «Open No Level (NL) ERP»
Datacenter (Датацентр)	Частные и гибридные виртуализованные среды высокой плотности	Полнофункциональный Windows Server. В цену входит возможность запускать неограниченное количество виртуализованных экземпляров на одном физическом сервере	Цена устанавливается за физические процессоры + лицензии клиентского доступа (приобретаются отдельно)	$4,809 за два физических процессора (количество ядер и потоков не ограничено). При использовании на более чем двухпроцессорных серверах требуется приобретение дополнительных лицензий
Standard (Стандарт)	Невиртуализованные или виртуализованные среды низкой плотности	Полнофункциональный Windows Server. В цену входит возможность запускать два виртуализованных экземпляра на одном физическом сервере	Цена устанавливается за физические процессоры + лицензии клиентского доступа (приобретаются отдельно)	$882 за два физических процессора (количество ядер и потоков не ограничено). При использовании на более чем двухпроцессорных серверах и/или более чем двух виртуализованных экземпляров требуется приобретение дополнительных лицензий
Essentials	Для малого бизнеса	Ограниченная	Цена	$501

		функциональность Windows Server. В цену не входит возможность запускать дополнительные виртуализованные экземпляры. Максимально 25 пользователей. Максимально два физических процессора (количество ядер и потоков не ограничено)	устанавливается за редакцию сервера, дополнительные пользовательские лицензии оплачивать не нужно	
Foundation	Экономичная редакция	Ограниченная функциональность Windows Server. В цену не входит возможность запускать дополнительные виртуализованные экземпляры. Максимально 15 пользователей. Максимально один физический процессор (количество ядер и потоков не ограничено)	Цена устанавливается за редакцию сервера, дополнительные пользовательские лицензии оплачивать не нужно	Распространяется только с оборудованием

Ранее входившие в линейку редакции Windows Small Business Server (SBS), Windows Home Server более развиваться не будут, так как, по наблюдениям Microsoft, целевые аудитории этих продуктов (домашние пользователи, малый бизнес) все чаще выбирают облачные службы для решения своих задач, например таких, как организация электронной почты и совместной работы и резервного копирования, вместо развертывания собственной инфраструктуры.

Также ранее входившие в линейку редакции Enterprise, High-Performance Computing (HPC) и Web Server в новом поколении недоступны.

Важным изменением является то, что функционально редакции Datacenter и Standard не отличаются — теперь можно строить кластеры высокой доступности и отказоустойчивые кластеры, имея лицензию на Standard.

Платформа виртуализации (Hyper-V)

Поскольку виртуализация — краеугольный камень облачных сред, много нового появилось именно в этой области.

Принята во внимание необходимость больших компаний и облачных провайдеров лучше управлять их ЦОДами, учитывая потребление ресурсов: вычислительных, хранения, сети.

Масштабируемость

Если предприятию было недостаточно мощности решений виртуализации предыдущего поколения, то Windows Server 2012 может быть выходом, так как Hyper-V 3-й версии поддерживает:

- до 320 логических процессоров на физический сервер и до 64 процессоров в виртуальной машине;
- до 4 ТБ оперативной памяти на физический сервер и до 1 ТБ памяти в виртуальной машине;
- в виртуальной машине поддерживается жесткий диск объемом до 64 ТБ;
- кластеры Hyper-V с количеством узлов до 64 и до 8000 виртуальных машин на кластер до 1024 машин на узел.

Мне представляется, что лишь очень небольшая часть всех возможных нагрузок, исполняющихся на серверах архитектуры x86-64, не может быть виртуализована, учитывая эти ограничения.

Live Migration

Live Migration (живая миграция) — возможность переноса виртуальных машин между физическими серверами без перерыва в предоставлении сервисов клиентам — с появлением Windows Server 2012 стала возможна более чем для одной виртуальной машины одновременно. Фактически количество виртуальных машин, одновременно вживую мигрирующих между хостами, зависит от мощности оборудования. При использовании новой версии протокола SMB, SMB3 (см. ниже), и агрегировании высокопроизводительных сетевых интерфейсов (NIC teaming) можно одновременно переносить 120 виртуальных машин.

Также, благодаря поддержке размещения виртуальных жестких дисков на общих папках по протоколу SMB3, стало возможным выполнять Live Migration без использования разделяемого кластерного хранилища (CSV = clustered shared volume).

Microsoft говорит о появлении возможности миграции типа «shared-nothing», т. е. при наличии только Ethernet-кабеля.

Сетевые возможности

Выполнены существенные усовершенствования и в сетевой инфраструктуре Hyper-V. Если в физическом хосте виртуализации будут установлены серьезные сетевые адаптеры, с большим количеством возможностей на аппаратном уровне, например IPSec Offload, то с большой вероятностью, применив Hyper-V 3, все эти «вкусности» удастся получить и внутри виртуальных машин.

Виртуальный коммутатор, управляющий работой сетевых адаптеров виртуальных машин, серьезным образом переработан. Основным усовершенствованием является новая открытая архитектура, которая позволяет сторонним производителям использовать документированные API для написания своих расширений, реализующих функциональность инспекции и фильтрации пакетов, проприетарных протоколов свитчинга, фаерволла и систем определения вторжений.

В настоящее время уже выпущено одно решение, использующее упомянутую архитектуру — виртуальный свитч Cisco Nexus 1000V.

Вместе с тем, даже без применения сторонних решений виртуальный свитч стал мощнее — например, появилась возможность управлять полосой пропускания отдельных виртуальных машин.

Другие механизмы Hyper-V

Также усовершенствованы многие другие механизмы: Hyper-V стал лучше поддерживать NUMA; появился новый формат виртуальных жестких дисков VHDX, поддерживающий жесткие диски формата native 4K и диски большого размера; улучшен механизм Dynamic Memory — добавлена опция Minimum Memory, позволяющая гипервизору забирать память у виртуальных машин, если для запуска нужной ее недостаточно. Стало возможным делать инкрементальные резервные копии работающих виртуальных машин.

Сетевая подсистема

IPv6

В ОС Windows Server 2012 переписана реализация стека протоколов TCP/IP. Основным протоколом сейчас считается IPv6, в то время как IPv4 на внутреннем программном уровне обрабатывается как подмножество IPv6.

На приоритетное использование IPv6 нацелена и реализация многих протоколов более высокого уровня и сервисов — не стоит удивляться, когда при наличии возможности работы и IPv6, и IPv4 будет выбран именно IPv6. Например, служба разрешения доменных имен DNS в первую очередь пытается получить именно IPv6-адрес узла.

Остановимся на некоторых особенностях IPv6:

- первое, что упоминается всеми — большее адресное пространство, что позволит наделить собственным уникальным во вселенной IPv6-адресом $\approx 3{,}4 \cdot 10^{38}$ узлов. Вместе с тем, существующие правила выделения IPv6-адресов, учитывающие их структуру, предписывают выделять каждому обратившемуся за собственным блоком IPv6-адресов предприятию подсеть /64, т. е. предприятие получает возможность выдать своим серверам, клиентским ПК и устройствам 2^{64} уникальных глобально маршрутизируемых IPv6-адресов — в 2^{32} раза больше, чем было во всем вместе взятом IPv4-адресном пространстве Интернета;
- возможность выдать каждому узлу сети (каждому устройству) собственный глобально маршрутизируемый IPv6-адрес сделает гораздо более простой работу сервисов, которые должны из Интернета инициативно доставлять сообщения адресатам внутри корпоративных (да и домашних) сетей — в основном это различные приложения сегмента

унифицированных коммуникаций: мессенджеры, коммуникаторы и т. п. Культурный шок: PAT (NAT) — больше нет! Для клиентских же приложений отпадет необходимость постоянно поддерживать открытую через PAT (NAT) TCP-сессию, а для сервера, соответственно, держать их тысячи/десятки тысяч;

- IPv6 позволяет снизить нагрузку и, соответственно, требования к сетевому оборудованию, особенно это будет заметно на высоконагруженном провайдерском оборудовании: из стандарта убрана фрагментация, не нужно считать контрольные суммы, длина заголовков — фиксирована;
- в IPv6 включена обязательная поддержка узлами технологии IPSec. В настоящее время существует большое количество протоколов, разработанных на заре Интернета, к каждому из которых пришлось позже разрабатывать и стандартизовать безопасные аналоги — некие уникальные для каждого протокола «обертки» (HTTP/HTTP**S**, FTP/**S**FTP и т. п.). IPv6 позволит уйти от этого «зоопарка» и унифицированно защищать соединение двух узлов на 3-м уровне сетевой модели для любого протокола;
- IPv6 потенциально создает возможность роуминга мобильных устройств между беспроводными сетями различных операторов (Wi-Fi, 3G, 4G и т. д.) без разрыва сессий клиентского ПО, например голосового трафика SIP-клиентов.

В частности, такая входящая в Windows Server технология, как DirectAccess, позволяет организовать защищенный удаленный доступ клиентского компьютера в корпоративную локальную сеть прозрачно для пользователя. Со стороны пользователя нет необходимости использовать какие-либо VPN-клиенты или подключения. DirectAccess, будучи единственный раз настроен, в дальнейшем работает прозрачно для пользователя.

С технологической стороны, DirectAccess — это реализация IPSec VPN на базе IPv6 компании Microsoft. (Это не значит, что он не будет работать поверх транспортных сетей IPv4.)

Кстати, в Windows Server 2012 стало возможным не развертывать PKI, если клиенты DirectAccess — Windows 8.

SMB3

В сетях Microsoft для доступа к ресурсам файл-сервера применяются протоколы SMB (Server Message Block). Уже довольно давно мы работаем с протоколом версии 2, а в Windows Server 2012 вошла новая редакция — SMB 3.0.

На самом деле, протокол SMB 3.0 необходимо рассматривать не в контексте сетевой подсистемы, а в контексте подсистемы хранения данных — и позже мы увидим почему.

В контексте же сетевой подсистемы можно сказать, что SMB 3.0 заточен под современные быстрые локальные гигабитные сети — при его использовании оптимизировано управление протоколом транспортного уровня TCP в таких сетях, учитывается возможность применения т. н. jumbo-фреймов Ethernet. Заточен он также и для применения IPv6.

Подсистема хранения

На крупных предприятиях при построении ИТ-инфраструктур часто применяются специализированные решения для хранения данных, за счет чего достигается

определенный уровень гибкости: полка с дисками может использоваться одновременно несколькими серверами, емкость гибко по необходимости распределяется между ними.

В то же время, такие специализированные решения достаточно дороги и в приобретении, и в последующем обслуживании. Администрирование и поддержка этих устройств и интерфейсов (например, Fiber Channel) требуют от администраторов соответствующих знаний и навыков.

При проектировании Windows Server 2012 в Microsoft ставили перед собой задачу реализовать в серверной ОС функциональность, которая позволит предоставить приложениям, таким как SQL Server и Hyper-V, тот же уровень надежности подсистемы хранения, что и специализированные решения, используя относительно недорогие («неумные») дисковые массивы. Причем, для унификации задач администрирования, реализация даже не применяет блочные протоколы (такие как iSCSI), а работает в варианте с обычными файл-серверными протоколами, такими как SMB.

Достигнуто это было в основном двумя механизмами — применением Storage Spaces и протокола SMB3.

SMB3

Таким образом, SMB 3.0 научили:

- максимально использовать возможности «умных» полок, если таковые уже приобретены: использовать технологии Offloaded Data Transfer (ODX), когда сервер только отдает команду полке на перемещение файлов, а полка это сверхбыстро внутри себя делает и возвращает серверу результат выполнения;
- открывать более одной TCP-сессии для копирования файла на сетевых картах, поддерживающих RSS (receive side scaling);
- использовать более одной сетевой карты одновременно для увеличения производительности: если два сервера Windows Server 2012 (или Windows 8) имеют по две сетевые карты, то скорость копирования вырастет;
- использовать более одной сетевой карты одновременно для обеспечения отказоустойчивости: если два сервера Windows Server 2012 (или Windows 8) имеют по две сетевые карты и одна из них откажет, то процесс копирования не остановится, а завершится успешно;
- обеспечивать работу Continuously Available File Server — настоящего отказоустойчивого кластера файл-серверов*.

** Здесь необходимо сделать лирическое отступление. Термин Windows Server Failover Clustering достаточно давно неправильно перевели как «отказоустойчивый кластер». На самом деле это **высокодоступный** кластер. То есть сервис, оказываемый клиенту конкретным узлом кластера, в случае нештатного выхода этого узла из строя, прервется. Далее, без вмешательства администратора, сервис поднимется на другом узле кластера и продолжит обслуживать клиентов. Ущерб конкретному клиенту, получившему отказ в обслуживании на короткое время, зависит от используемого сервиса и стадии сессии, на которой произошел отказ.*

Так вот, новый Continuously Available File Server — это тот самый настоящий «отказоустойчивый файл-сервер», то есть такое устройство кластера, выполняющего роль файл-сервера, при котором отказ узла, обслуживающего конкретного клиента в

данный момент времени (например, клиент может копировать большой файл с сервера на локальный диск), не повлечет перерыва в обслуживании для этого клиента — файл на клиента продолжит отдавать другой узел кластера.

Storage Spaces

Storage Spaces — новый механизм, появившийся в Windows Server 2012.

Его ключевая «фишка» — дать возможность организовать высокодоступную и масштабируемую инфраструктуру хранения по значительно более низкой совокупной стоимости владения (TCO), чем специализированные сторадж-решения.

Идея, реализованная этим механизмом — следующая. Есть сервер под управлением Windows Server 2012. У него есть DAS (directly attached storage) — может быть, в форме дисков SATA или SAS, находящихся в корпусе, а может быть, в виде внешних дисковых полок, подключенных по интерфейсу SAS. Полкам не нужно обеспечивать никакой расширенной обработки, то есть не нужно реализовывать алгоритмы RAID, достаточно отдать JBOD — просто набор дисков, то есть полка в данном случае — это просто железка с блоком питания, салазками и интерфейсом SAS.

В механизме Storage Spaces определяются т. н. Storage Pools — базовые логические строительные блоки системы хранения. Они включают один или несколько физических дисков. На уровне Storage Pool один из дисков может быть назначен как диск, находящийся в горячем резерве — он будет автоматически задействован тогда, когда один из рабочих дисков, входящих в Storage Pool, выйдет из строя.

Далее, внутри Storage Pool, определяются виртуальные диски. Виртуальный диск может быть собран в одном из трех режимов:

1. Простой (Simple) — данные будут распределены между физическими дисками, увеличивая производительность, но уменьшая надежность (некий аналог RAID0);
2. Зеркало (Mirror) — данные будут продублированы на двух или трех дисках, увеличивая надежность, но неэффективно используя емкость (некий аналог RAID1);
3. Четность (Parity) — данные и блоки четности будут распределены по дискам, представляя компромиссное решение между первыми двумя режимами (некий аналог RAID5).

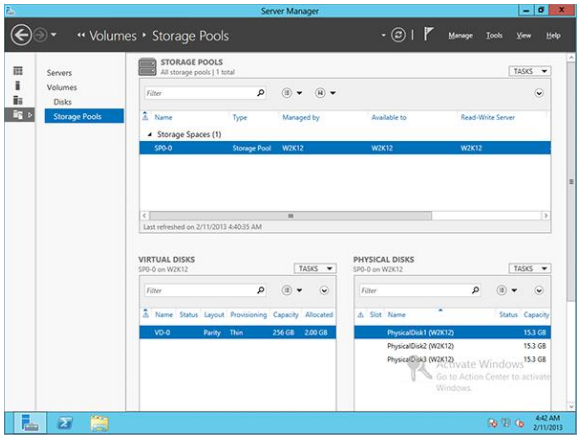
Виртуальные диски могут быть собраны с фиксированным размером на физическом диске либо потреблять место из Storage Pool по мере сохранения данных, до определенного для диска размера.

После создания виртуального диска ОС предлагает создать на нем раздел ОС, под который можно отвести все или часть пространства виртуального диска, отформатировать раздел и присвоить ему букву диска. То есть можно сказать, что механизм Storage Spaces формирует виртуальные жесткие диски, логически расположенные между «железом» и «Управлением дисками» (Disk Manager).

В чем же преимущество по сравнению со старым добрым софтовым RAID, работающим в Windows NT с незапамятных времен?

Неверное, самым большим отличием будет являться возможность создать виртуальные диски объемом больше, чем нижележащие диски с учетом режима.

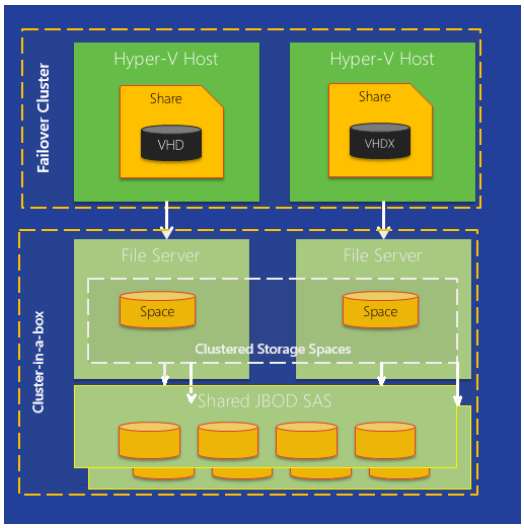
Например, определив Storage Pool, включающий три жестких диска по 16 ГБ, можно создать в нем виртуальный диск размером 120 ГБ. По мере того, как диск будет заполняться данными и доступная емкость физических жестких дисков будет заканчиваться, можно добавить в Storage Pool новые физические диски, не меняя ничего на уровне раздела и данных.



Отдельно хотелось бы сказать о производительности решения. Мы понимаем, что на определенном уровне архитектуры Storage Spaces представляют собой софтовую организацию RAID-массива. Софтовая — совсем не значит медленная или плохая. Например, реализация Intel Matrix RAID, несмотря на то что «снаружи» она выглядит как аппаратная, на самом деле для обсчета старших уровней RAID использует ресурсы ЦП. Необходимо полноценно тестировать производительность различных решений, и желательно не абстрактными синтетическими тестами, а тестами, имитирующими или представляющими собой реальную нагрузку.

Что же касается переносимости Storage Spaces между серверами — то она есть, без проблем. Если боевой сервер «упал», то можно подключить жесткие диски к новому и импортировать существующую конфигурацию Storage Spaces.

За счет новых технологий Storage Spaces и SMB3, в числе прочего, может быть собрана следующая архитектура:



Два Hyper-V-хоста обеспечивают режим высокой доступности для исполняющихся на них виртуальных машин. Виртуальные жесткие диски и конфигурация виртуальных

машин хранятся на выделенной в совместное использование по протоколу SMB3 папке. Папка, в свою очередь, выделена непрерывно доступным файл-сервером (отказоустойчивым кластером), состоящим из двух серверов, в каждом из которых расположены два SAS HBA (хост-адаптера), каждый из которых соединен с двумя идентичными коробками дисков). На файл-серверах настроены «зеркальные» Storage Spaces, а на соответствующих дисках организовано разделяемое кластерное хранилище (CSV). То есть подсистема хранения вообще не имеет единой точки отказа, и собрана она при этом исключительно средствами Microsoft Windows Server 2012.

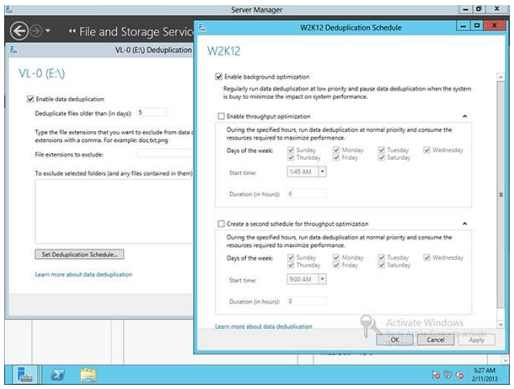
Дедупликация данных

Практически стандартной является ситуация, когда каждому сотруднику предприятия на файл-сервере выделена личная папка. Диск файл-сервера, как правило, организован на отказоустойчивом RAID-массиве, осуществляется регулярное резервное копирование, правами на доступ к личной папке обладает только сотрудник. Таким образом, и информация, и интересы предприятия эффективно защищены.

Иногда встречаются вариации схемы: средствами ОС Windows на файл-сервер перенаправлены папки «Мои документы» и «Рабочий стол». То есть сотрудник пользуется этими папками как обычно, а физически они расположены на файл-сервере.

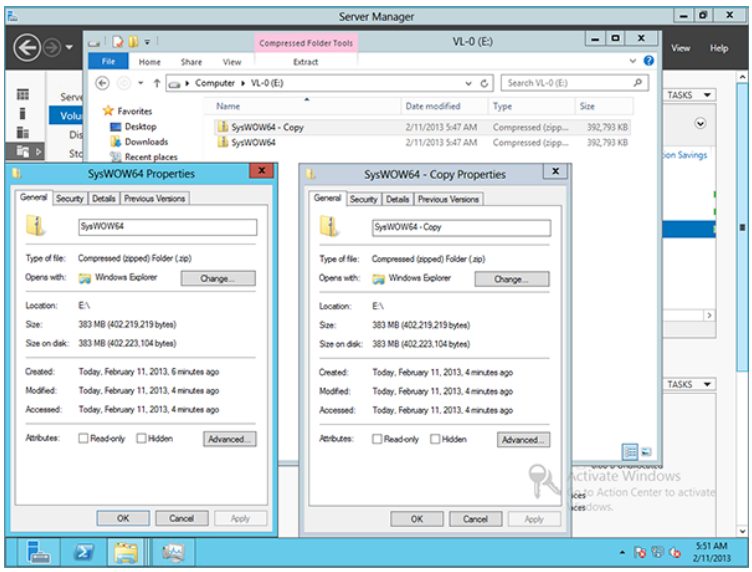
Теперь представим ситуацию, когда в общей папке появляется некий файл, представляющий интерес для нескольких сотрудников. Например, презентация нового продукта. Или фотографии с корпоративного мероприятия. Довольно скоро множественные копии этих файлов оказываются растащены по личным папкам. Конечно, на файл-сервере место занимает каждый экземпляр файла.

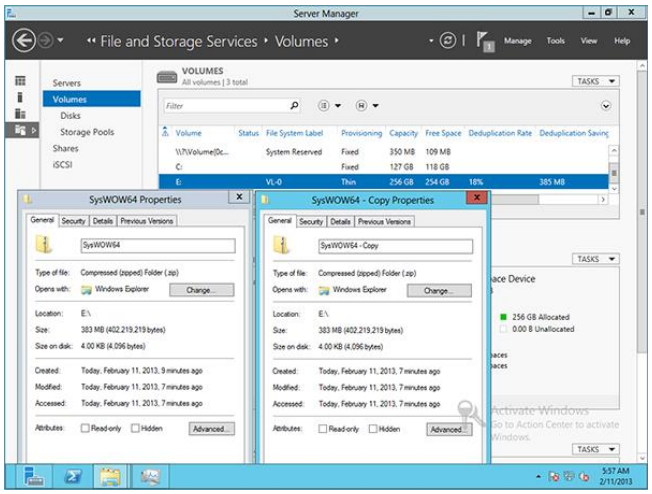
В такой ситуации может проявить себя новый механизм Windows Server 2012 — механизм дедупликации данных.



Будучи задействованным для конкретного тома, Windows Server 2012 начинает по определенному расписанию анализировать том на наличие блоков (не файлов, а блоков), содержащих идентичные данные, и обеспечивать их хранение в единственном экземпляре. Конечно, для пользователя это совершенно незаметно.

Расположив два идентичных по содержимому файла на диске, получаем следующую картину до и после дедупликации:





Механизм дедупликации не поддерживает ReFS и данные, защищенные EFS; не обрабатываются файлы менее 32 КБ и файлы с расширенными атрибутами (extended attributes), тома Cluster Shared Volumes и системные тома.

Новая файловая система — ReFS

Новая файловая система доступна только в Windows Server 2012. Хотя она остается совместимой с NTFS на уровне API, для нее действует целый ряд ограничений:

- не поддерживается шифрование NTFS;
- не поддерживается сжатие NTFS;
- не поддерживается на системных томах.

В ReFS для хранения информации о файлах используется структура т. н. «бинарного дерева», что позволяет быстро находить требуемую информацию. В ней не используется механизм «журналирования» NTFS, а реализован другой принцип транзакционности. ReFS хранит расширенную информацию о файлах, например контрольные суммы с возможностью коррекции считанных исходных данных файла, что помогает предотвратить ошибки типа «bit rotting».

CHKDSK

Утилита CHKDSK, отвечающая за проверку логической целостности файловой системы и ранее требовавшая эксклюзивного доступа к диску (отмонтирования тома), в Windows Server 2012 научилась работать в фоне. То есть, например, если большой диск с данными SQL Server требуется проверить CHKDSK, то после перезагрузки сервер запускается, SQL стартует и начинает обслуживать клиентов, а в фоне работает CHKDSK.

Динамический контроль доступа

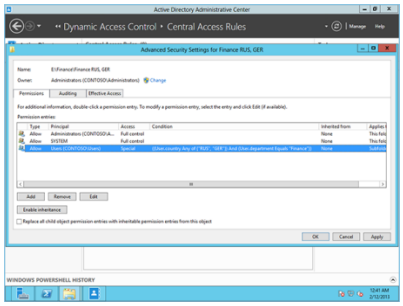
В предыдущих поколениях Windows Server разграничение на доступ к ресурсам файл-сервера строилось на механизме списков контроля доступа (ACL) на ресурсах и включении учетной записи пользователя в группы.

При наличии большого количества файл-серверов, ресурсов на них и обширного штата пользователей работа по администрированию доступа становилась трудоемкой. Представим ситуацию, когда есть:

1. несколько регионов продаж;
2. несколько уровней допуска к информации внутри подразделений продаж;
3. несколько типов документов по степени конфиденциальности;
4. предусматривается возможность доступа с нескольких категорий устройств: доверенных и недоверенных.

Дизайн становится непростым. Для пользовательских учеток возникают группы вида «G-Sales-RUS-High_Clearance-…». Учесть же требования п.4 вообще не представляется возможным. При этом отметим, что мы в какой-то части дублируем свою же работу: если для учетной записи пользователя в Active Directory мы уже исправно заполняем «Регион», то мы же сами потом и должны включить его учетку в группу «G-Sales-RUS-…».

В таких сценариях и появляется поле для деятельности динамического контроля доступа. Идея заключается в том, что файл-сервер при принятии решения о предоставлении доступа к ресурсу (файлу, папке) сможет учитывать определенные атрибуты пользователя и устройства, источником которых является Active Directory. Например, предоставлять доступ только в том случае, если Страна учетки пользователя = Россия или Германия, Департамент = Финансы, и Тип_Устройства, с которого пользователь пытается получить доступ = Управляемое. То есть для администраторов задача по сведению пользовательских учеток в группы в некоторых сценариях может быть значительно упрощена. Сам пользователь придет за доступом к ресурсу файл-сервера, уже имея набор определенных реквизитов, взятых из Active Directory. А на ресурсе значения этих реквизитов могут быть собраны в логические выражения.



Для развертывания, в числе прочего, требуется функциональный уровень леса не ниже Windows Server 2003 и хотя бы один домен-контроллер на Windows Server 2012, а также файл-сервер на Windows Server 2012. Клиентами могут быть Windows 7.

Особенно интересными могут быть сценарии, когда динамический контроль доступа работает в связке с инфраструктурой классификации файлов (FCI). В этом случае на файлы автоматически в зависимости от их содержимого могут быть установлены расширенные атрибуты типа «УровеньДоступа = КонфиденциальнаяИнформация», а доступ можно настроить, например, только группе «G_Managers» департамента «Управляющая компания».

RDP 8 / RemoteFX второго поколения

Интересные изменения произошли в протоколе удаленных рабочих столов — RDP — с выходом RDP 8.

Если посмотреть на историю вопроса, мы увидим, что на заре существования по протоколу RDP передавались команды GDI — графического интерфейса Windows, которые исполнялись (отрисовывались) на удаленном терминале.

Постепенно протокол эволюционировал, обрастал различными типами, способами и методами кодирования и передачи заданий на отрисовку.

В Windows Server 2008 R2 была представлена концепция RemoteFX, в которой идеология полностью поменялась. С RemoteFX RDP-сервер фактически отрисовывал все сам, брал готовый фрейм-буфер, кодировал одним кодеком и отдавал на клиента.

Теперь в RDP8 вошел RemoteFX, если так можно выразиться, второго поколения. Теперь фрейм-буфер анализируется, для различных участков экрана (графика, статичные изображения, анимация и видео) выбираются разные кодеки, участки кодируются и по отдельности отдаются на клиента. Для изображений применяется прогрессивный рендеринг, то есть изображение в низком разрешении клиент увидит мгновенно, а детали догрузятся так быстро, как это позволит пропускная способность канала.

RemoteFX первого поколения работал только в том случае, если RDP-хост был развернут в виде виртуальной машины Hyper-V и в системе работал совместимый видеоадаптер, реализующий DirectX 10-й версии. Сейчас эти требования ушли: и визуальная часть, и проброс USB-устройств будут работать на RDP-хосте, развернутом прямо на железе, без виртуализации, и не имеющем видеоадаптера с DirectX 10. (Проброс USB-устройств позволяет работать в терминальной сессии любым USB-устройствам, подключенным к клиентскому терминалу, например лицензионным USB-ключикам — проброс осуществляется на уровне передачи данных по протоколу USB.)

RDP8/RemoteFX2 научился подстраиваться под особенности канала связи, используя адаптивные кодеки. То есть при подключении по локальной сети видео будет воспроизводиться в отличном качестве, но и на тонком WAN-канале что-то да будет видно ;)

RDP8 поддерживает multi-touch и жесты, благодаря чему, например, на Microsoft Surface можно устанавливать RDP-соединение до сервера и использовать x86-приложения. В RDP-клиенте есть удаленный курсор, помогающий попадать пальцами по контролам Desktop-интерфейса.

Появился и новый API, который позволяет приложениям использовать адаптирующиеся под пропускную способность канала кодеки. Например, в сценарии развертывания пользовательских ПК как виртуальных машин (т. н. VDI) клиент унифицированных коммуникаций, работающий в терминальной сессии и получающий аудио- и видеопотоки от RDP-клиента, может использовать преимущества RDP8. В настоящее время используется клиентом Lync 2013.

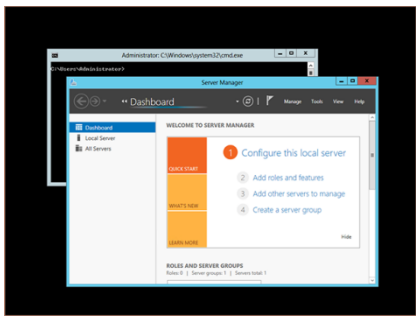
Клиент RDP8 с поддержкой всей новой функциональности уже сейчас доступен для Windows 7.

Режимы Server Core / Minimal Server Interface

Свершилось: режим Server Core в Windows Server 2012 является основным рекомендуемым режимом установки и использования Windows Server. Преимущества такого подхода известны давно: меньше размер на диске, меньше требования к ресурсам (что особенно важно при высокой плотности виртуальных машин на физическом хосте), меньшая поверхность атак и обслуживания (сервер начинает таскать на себя меньше патчей). Кстати, из Server Core можно удалить компонент WoW64, позволяющий исполняться 32-битному коду, превратив Windows Server в настоящую чистую на 100% 64-битную ОС ;)

Интересно, что между Server Core и Server with a GUI теперь находится некий промежуточный вариант, который нельзя выбрать при установке, но в который можно попасть при переходе от одного из двух основных вариантов к другому — т. н. «Minimal Server Interface», включающий Microsoft Management Console (MMC), Server Manager, и подмножество Control Panel.

Вместе с тем, в Windows Server 2012 можно переключаться между режимами Server Core, Minimal Server Interface и Server with a GUI в любое время после установки (в процессе эксплуатации), так что интересным представляется сценарий установки Server with a GUI, настройки сервера и последующего перехода к Server Core.



Для дополнительной экономии места на диске в Windows Server 2012 стало возможным после установки и настройки сервера полностью удалить бинарные файлы тех ролей и функциональности, которые остались незадействованными.

Администрирование

Новый Server Manager

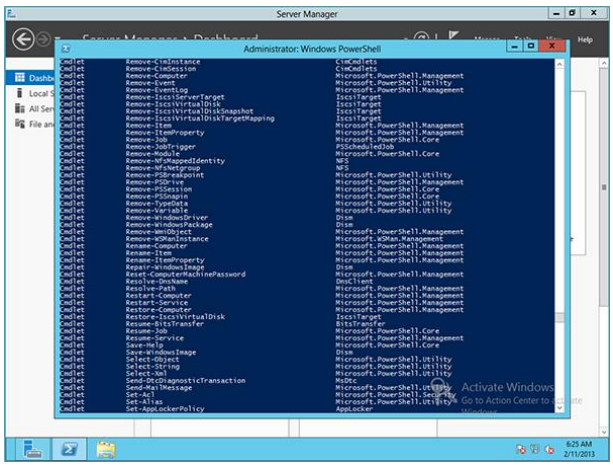
В Windows Server 2012 появился новый Server Manager. Из интересного: можно управлять сразу несколькими серверами, выполняя на них однотипную операцию.

В интерфейсе появился список задач администрирования. Например, после установки DHCP-сервера для администратора устанавливается задача его настройки — выделения диапазонов и пр.

Личные впечатления: приятная неожиданность — пожалуй, это первый Server Manager, который не был сразу же закрыт и у которого не выключалась опция автозагрузки.

PowerShell

PowerShell в Windows Server 2012 существенно расширен: добавились более 2400 (!) командлетов. PowerShell де-факто стал стандартом на управление из командной строки. Всей функциональностью — возможно, за крайне небольшим исключением — можно управлять через PowerShell.



Такой подход не может не радовать. Мы можем вспомнить зоопарк из комплектных утилит командной строки, Support Tools, Resource Kit, специальных утилит, которые техподдержка Microsoft писала сама для себя, и прочего, каждая со своим собственным синтаксисом и возможностью совместного использования только через разбор текстового вывода одной и подачей на вход другой.

Почувствуйте разницу: единообразный синтаксис, передача объектов между командлетами, удаленное управление через стандартизованный интерфейс WS-Management.

Интересно: некоторые утилиты, например netsh, предупреждают, что их функциональность в следующих версиях Windows Server может быть изъята, и советуют переходить на PowerShell для решения задач автоматизации управления.

Заключение

В Windows Server 2012 действительно много новой интересной функциональности. Основные изменения сосредоточены Моменты, показавшиеся автору наиболее интересными, затронуты в статье.

Вместе с тем, о чем-то мы даже не упомянули: например, о нововведениях в подсистеме печати, VDI, IIS, BranchCache, DHCP…

Закрепление материала:

1. Что такое операционные системы линейки Windows Server?
2. Перечислите строительные блоки клиентской ОС Windows.
3. Четыре группы требований с серверной ОС.
4. Перечислите доступные 4 редакции в линейке Windows Server 2012.
5. Функциональность Windows Server 2012
6. Изменения в областях виртуализации, подсистемы хранения, сетях, Windows Server 2012.

Задания выполнить в Word и направить на почту: ignat-80@mail.ru не позднее 28.03.2020