Windows Server 2008 – новый уровень поддержания доступности файловой инфраструктуры

Обзор нововведений в Windows Server 2008, коснувшихся файловой структуры, файловых сервисов и управления данными в целом новой операционной системы, начало продаж которой планируется на осень 2008 г.

Введение

В конце февраля 2008 г. вышла на рынок новая серверная операционная система Windows Server 2008. Обсуждения функциональности нового продукта начались еще задолго до выхода RTM релиза, так как все ждали продолжения развития после выпуска Windows Server 2003 R2.

Статьи в большинстве своем касались нововведений в управлении сервером (появление core server, новой консоли управления Server Manager, Windows Powershell) и несомненно важных дополнений в Active Directory Domain Services (контроллеры – только-для-чтения RODC, детализированные политики паролей и моментальные снимки AD). Однако, помимо этих новшеств, изменения произошли в менее заметных областях работы сервера под управлением ОС Windows Server.

Windows Server 2008 – новый уровень управления файлами

Distributed File System – новый уровень доступности файлов в распределенной файловой инфраструктуре

Если говорить о нововведениях исключительно в области файловых сервисов, то следует отметить, что Майкрософт планомерно продолжает расширять функциональность распределенного файлового хранилища (Distributed File System, далее DFS).

Технологии DFS позволяют организовать для пользователей простой и надежный доступ к файлам, которые могут быть расположены на разных серверах и и в разных филиалах, организуя данные в единую древовидную структуру (DFS Namespaces, DFS-N), которая также может помочь оптимизировать трафик по дорогим каналам связи, перенаправляя запросы пользователей на ближайший сервер с необходимыми данными (используются данные Active Directory). Эффективно реплицировать копии необходимых данных по серверам позволяет новая технология DFS Replication (DFS-R). Эта технология появилась еще в версии Windows Server 2003 R2 и основана на использовании удаленного разностного сжатия, что значительно сокращает трафик репликации, так как она теперь реализована на синхронизации отдельных блоков целевых и исходных файлов.

Применение новой технологии репликации затрагивает не только область файловых сервисов, но и касается некоторым образом репликации Active Directory.

Несмотря на появление технологии DFS-R в Windows Server 2003 R2, для репликации SYSVOL между контроллерами домена по-прежнему использовалась служба репликации файлов (FRS). По этой причине репликация SYSVOL, особенно в распределенных территориально компаниях с большим количеством контроллеров домене, вызывает головную боль у администраторов Active Directory.

Если же домен работает на функциональном уровне Windows Server 2008, то появляется возможность выполнить репликацию SYSVOL с использованием технологии DFS-R, что повышает скорость и надежность репликации SYSVOL. Также не лишним может оказаться перенос объемных файлов в SYSVOL, чтобы они были доступны для всех контроллеров домена. Для подготовки к применению новой технологии репликации следует перенести данные из старого SYSVOL при помощи служебной программы DFSRMIG, которая помогает создать объекты в AD, которые необходимы для DFS-R, новую структуру SYSVOL на каждом контроллере домена, переключить все контроллеры домена на вновь созданный SYSVOL и удалить старый. Конечно, в зависимости от количества контроллеров домена и размера каталога SYSVOL такая операция может оказаться достаточно трудоемкой и займет определенное время, но в результате мы получим повышение производительности контроллеров домена, что не так уж и плохо.

Функциональный уровень Windows Server 2008 также позволяет снять “рекомендованное ограничение” для DFS в 5000 папок и настроить для пользователей видимость только тех ресурсов, к которым у них есть доступ (то же самое возможно и в случае stand-alone структуры – достаточно, чтобы DFS была организована на сервере WS 2008).

SMB 2.0 – новый уровень производительности и целостности файловых операций

Еще одно нововведение – поддержка протокола SMB (Server Message Block) 2.0. Ранее использовался протокол SMB 1.0, который был разработан 15 лет назад и который по нынешним временам, когда наличие гигабитного Ethernet в компьютере является стандартом, уже устарел. При разработке SMB 2.0 Microsoft решила сделать его соответствующим современным реалиям. Среди преимуществ можно отметить возможность комбинирования нескольких запросов в одном пакете данных, то есть с меньшим числом пакетов можно отсылать больше запросов. Это снижает накладные расходы и улучшает пропускную способность. Кроме того, поддерживается больше соединений одновременно, что позволяет в одно время открывать больше файлов, улучшая качество соединения. Для получения описанных преимуществ и клиент, и сервер должны поддерживать новую версию протокола. Следует отметить, что Windows Vista уже поддерживает SMB 2.0, поэтому пользователь может сразу выиграть от более

высокой производительности, например, скачивая файл из общей папки к себе на ПК. Протокол выбирается автоматически при передаче файла, без каких-либо дополнительных настроек со стороны пользователя.

Также SMB 2.0 позволяет использовать так называемые символические ссылки (symbolic links) – некие объекты, которые могут ссылаться на другие подобные объекты, файлы или папки, даже находящиеся в сети. Подобная функциональность уже давно существовала в *nix системах и, думаю, будет полезна в некоторых случаях, например для обеспечения взаимодействия с *nix системами или для упрощения доступа к ресурсам на удаленном или локальном компьютере.

Еще одно, косвенно связанное с использованием SMB 2.0 новшество, – транзакционная файловая система. Транзакционная файловая система (Transactional NTFS, TxF) – это расширение файловой системы NTFS, позволяющее выполнять файловые операции над томом файловой системы NTFS в рамках транзакций. Это стало возможным благодаря новой транзакционной инфраструктуре, реализованной на уровне ядра операционной системы и позволяющей сервисам операционной системы участвовать в транзакциях, используя новый компонент – менеджер транзакций Kernel Transaction Manager (KTM). Помимо этого, в обеспечении функционирования транзакционной файловой системы задействована подсистема протоколирования – Common Log File System (CLFS), впервые реализованная в Microsoft Windows Server 2003 R2. Проще говоря, это означает, что некая последовательность файловых операций может быть выполнена в рамках единой транзакции, и в случае неуспеха одного из "атомов" транзакции все ранее произведенные изменения применены не будут, то есть либо вся транзакция выполняется корректно, либо не выполняется вовсе, и изменения откатываются. Это может быть интересно тем специалистам, которые нуждаются в четком контроле корректного прохождения файловых операций. Причем, благодаря тому, что TxF способна полноценно взаимодействовать с MS Distributed Transaction Coordinator (DTC), она может участвовать в транзакциях, использующих не только менеджеры ресурсов, предоставляемые Kernel Transaction Manager, но и другие, поддерживаемые на уровне DTC. Например, система документооборота может воспользоваться этой возможностью для работы как с файловой системой, так и с базой данных – и все в рамках одной транзакции. Другой пример применения транзакционной файловой системы – обновление файлов на группе компьютеров. А за счет расширений в протоколе SMB 2.0 появилась возможность использования в транзакциях распределенных файловых операций, например при работе с клиентами под управлением Windows Vista.

Однако необходимо отметить, что TxF не поддерживает операции над зашифрованной файловой системой (Encrypted File System, EFS), за исключением операций чтения.

Онлайновая проверка и коррекция ошибок в томах NTFS

Развивая концепцию по повышению надежности и доступности файловых сервисов, Microsoft включила в новую версию функциональность онлайн-проверки и коррекции ошибок в томах NTFS (Self-healing NTFS). Ранее, для того чтобы запустить утилиту проверки дисков chkdsk приходилось дожидаться перезагрузки сервера, теперь же этого делать не придется в подавляющем большинстве случаев – Self-healing NTFS включается по умолчанию при инсталляции нового сервера и позволяет в журнале видеть все действия по устранению ошибок, которые проводятся утилитой коррекции.

Новый уровень безопасности данных

В рамках повышения безопасности данных на сервере можно отметить доступность в новой версии Windows Server 2008 средства шифрования BitLocker Drive Encryption, которое обеспечивает AES шифрование всех данных на разделах совместно с проверкой целостности данных процесса (boot process), используемого для загрузки ОС. Главная цель этих нововведений – защита данных, даже если атакующий попытается получить к ним доступ в обход ОС или просто вытащит жесткий диск для анализа на другом компьютере. Нужно отметить, что шифрование раздела не ново; на рынке присутствует ряд решений, обеспечивающих такие же возможности. Однако кое-что отличает BitLocker от других программ: использование Trusted Platform Module TPM 1.2. Кратко TPM может быть охарактеризован как микроконтроллер, надежно хранящий данные, используемые в криптографических и защитных процессах (например ключи шифрования, цифровые сертификаты и пароли) с целью повышения защиты определенных приложений и модулей системы. При использовании чипа TPM для повышения защищенности BitLocker может быть сконфигурирован на загрузку системы после успешной проверки целостности файлов, используемых при загрузке, или (по крайней мере, в теории) на требование ввода PIN-кода или USB-устройства, содержащего ключ для входа в систему. BitLocker может также работать без поддержки TPM, используя ключ из USB-устройства, подключенного во время загрузки системы. В любом случае исследователи должны знать, какая именно информация должна быть собрана о системе, использующей BitLocker, и на что нужно обращать особое внимание (материнская плата, USB-диск, ключ/пароль для восстановления системы и т.п.).

В серверной редакции операционной системы зашифровать можно все разделы, включая и раздел, на котором установлена ОС. Это может быть полезным при установке контроллеров домена в удаленных филиалах.

Новый уровень эффективности и администрирования операций резервного копирования

Необходимость регулярного резервного копирования (РК) данных на сервере будет существовать всегда. К счастью, в Windows Server 2008 механизм резервного копирования и восстановления был полностью пересмотрен.

Повышенная эффективность операций РК

Система архивации данных Windows Server 2008 позволяет создать резервную копию всего тома сразу, нескольких томов или всего сервера, или же только system state. Для осуществления архивации данных используется механизм Volume Shadow Copy Service (VSS). Существует возможность архивирования на оптические носители, также в данной версии есть поддержка ручного архивирования на общие сетевые ресурсы. Поддержка архивирования отдельных файлов была удалена, что, впрочем, не отменяет при особой необходимости архивирования именно файлов использования скриптов.

Однако при переходе со всем знакомого Ntbackup следует быть готовым к тому, что все настройки необходимо будет пересоздавать, и архивные копии должны находиться на отдельном выделенном диске (возможно использование ротации дисков, существуют возможности по автоматическому контролю доступного места для архивной копии). Еще одна неприятность – для восстановления старых архивов, сделанных с помощью Ntbackup, необходимо будет скачать специальную версию для новой операционной системы с сайта Microsoft, потому как новая система архивации данных старый формат архивов не поддерживает.

В качестве хорошей новости, по моему мнению, очень полезная новая особенность: образы резервных копий сохраняются в формате VHD (виртуальный жесткий диск). Этот же формат используется в Microsoft Virtual Server 2005 для хранения образов виртуальных дисков. Из этого следует, что образ резервной копии, созданный системой архивации, можно монтировать в качестве жесткого диска на виртуальную машину под управлением Microsoft Virtual Server. Содержимое резервной копии можно будет просмотреть, как будто это обычный жесткий диск.

Улучшенное администрирование операций РК

Однако по-прежнему бесплатный продукт не предоставляет всей той функциональности, которая зачастую требуется администратору, ответственному за сохранность данных. Если раньше ему приходилось выбирать исключительно среди продуктов третьих, хоть и хорошо зарекомендовавших себя фирм-производителей программного обеспечения резервного копирования, то сейчас есть возможность использовать программное обеспечение от Microsoft. Недавно вышедший Data Protection Manager 2007 является частью целого комплекса продуктов, призванных упростить и упорядочить работу администратора, который Microsoft называет System Center. Как

известно, туда уже входит: программное обеспечение для проактивного мониторинга серверов System Center Operations Manager 2007, программное обеспечение для управления и инвентаризации System Center Configuration Manager 2007, средство проактивного планирования System Center Capacity Planner.

Как мне кажется, выпуск Microsoft отдельного продукта для резервного копирования связан с изменениями на самом рынке решений для защиты данных. Постепенно стандартные решения на основе ленточных накопителей в связке с ежедневным ночным копированием отходят в прошлое. Это связано с тем, что увеличивается объем данных, которые надо резервировать, изменяется их структура (широко распространяются SAN-, NAS-решения), изменяются сами требования (быстрое восстановление, восстановление по запросу пользователя из архива), изменяются архитектуры систем (все большее применение находят системы поэтапного архивирования). Собственно поэтому на рынке начали появляться решения по созданию архивов на дисках, непрерывной защите данных (CDP – Continuous Data Protection). Некоторые из этих подходов стали возможны и даже необходимы в силу недавнего снижения стоимости дисковых накопителей, повышения производительности сетей и процессоров, а также новых нормативных требований.

Майкрософт давно занимается созданием решений в этой области, но до появления DPM делал это либо на уровне ОС (ntbackup), либо приложений (отдельные решения для Exchange & SQL). На рынке решений для защиты данных первым автономным программным средством производства Майкрософт стал продукт System Center Data Protection Manager (DPM) 2006. Это был один из первых программных продуктов, предлагавших защиту данных на основе дисков, и он остается одним из редких решений, с самого начала создававшихся с идеей использования архивов на дисках. В большинстве других предложений применялись и по-прежнему применяются адаптированные для случая дисков идеи, использовавшиеся для архивов на магнитных лентах.

System Center Data Protection Manager 2006 обеспечивает создание архивов на дисках для файловых серверов и серверов печати, а также создание дисковых архивов филиалов компании с использованием глобальной сети (WAN). Этот программный продукт был разработан с целью защиты файловых серверов в центре обработки данных и для удаления из филиала оборудования для локальных архивов на магнитных лентах. Но в нем отсутствует встроенная поддержка приложений Майкрософт, и для долговременных архивов на магнитных лентах используются программные продукты независимых поставщиков.

Новая версия DPM, System Center Data Protection Manager 2007, создана на этой основе и по-прежнему обеспечивает надежную защиту с использованием дисков для файловых серверов и серверов печати, а также филиалов компании. Но, помимо этого, добавлена поддержка для приложений Майкрософт, которые важны для работы предприятий, таких как Exchange, SQL Server и SharePoint®, а также встроенная поддержка для архивов на магнитных лентах. Поддержка Exchange & SQL позволяет эффективно архивировать данные и восстанавливать их, поддерживаются новейшие кластерные решения, а при восстановлении используются только стандартные средства Microsoft.

Поддержка операций РК для виртуальных серверов

Еще одним интересным нововведением в DPM 2007 является поддержка виртуальных серверов конкретных узлов. Хотя большинство программ архивирования в состоянии поддерживать виртуальные хосты сервера, немногие, если они вообще есть, в состоянии предоставить такую защиту на уровне виртуального хоста посредством одной установки лицензии и агента. В DPM преимущества рекурсивных модулей записи службы теневого копирования томов (VSS) используются для защиты всех хостов, размещенных на данном узле виртуального сервера, посредством одного развернутого на узле агента. Эти архивные образы конкретных узлов не обеспечивают восстановление с той же детальностью, как архивы, созданные посредством агента DPM, установленного на гостевом или изолированном сервере, но они предлагают другие эффективные возможности, включая удобное восстановление системы в виртуализированных средах.

Улучшенная детализация и оптимизация операций РК

DPM 2007 также позволяет увеличить детализацию полных и добавочных архивов. Хотя DPM 2006 позволял выполнять даже ежечасную синхронизацию, новая версия DPM предоставляет возможность создавать добавочный архив каждые 15 минут, а полный архив – каждый час.

Также следует отметить, что из за специфической организации агента резервного копирования, помимо минимального влияния на производительность сервера, при полном архивировании не происходит перемещения полной копии данных с защищенного сервера на сервер DPM. Вместо этого перемещаются только измененные данные. Поэтому для группы хранения Exchange, имеющей объем 100 Гбайт и 10%-ную частоту изменений в течение дня, ежедневный полный архив будет иметь объем всего лишь 10 Гбайт. Если для создания точки восстановления делается мгновенный снимок, такое снижение объема полных архивов обеспечивает очень эффективное хранение на сервере DPM. Каждый мгновенный снимок состоит из измененных данных, образующих последний полный архив, и при выполнении полного архивирования он создается автоматически. При работе с приложениями эти мгновенные снимки содержат также результаты всех промежуточных добавочных архивирований. Добавочные архивы являются, в основном, архивами журналов DPM, поэтому при каждом полном архивировании приложения измененные данные перемещаются на сервер DPM и присоединяются к любому промежуточному архиву журналов с целью создания одного мгновенного снимка, содержащего несколько точек восстановления. Если взять случай 100-гигабайтной группы хранения Exchange с 10%-ной ежедневной частотой изменений, которая описывалась ранее, и считать, что полное копирование выполняется ежедневно с 15-минутным интервалом, то мгновенный снимок будет содержать 10 Гбайт измененных данных и примерно 5–10 Гбайт журналов приложений. Но важно осознавать, что в мгновенном снимке объемом от 15 до 20 Гбайт будет содержаться до 97 точек восстановления.

Непрерывная защита данных на основе мгновенных снимков

Одной из наиболее интересных возможностей является выполнение восстановления приложений Майкрософт после ошибок, которое не сопровождается потерями данных. Это стало возможным благодаря отслеживанию изменений на уровне блоков и архитектуре VSS, а также глубокой интеграции с журналами приложений, имеющимися на защищенном сервере.

Такое решение позволяет избежать недостатков решений по непрерывной репликации, которые также часто называют решениями по непрерывной защите данных (CDP – Continuous Data Protection). Защита данных с использованием репликации вызывает перемещение изменений, по мере их возникновения, с защищенного сервера на резервный сервер. Это решение на основе дисков, что означает возможность восстановления после ошибок в любой момент времени и без потерь данных. Однако зачастую в таком решении отсутствует понятие состояния приложения, что в итоге при восстановлении данных может не дать нам необходимого конечного результата – работоспособного приложения. Плюс к этому, решения на основе репликации зачастую связаны с высокой стоимостью, ведут к существенным перегрузкам сети и процессора и требуют больших объемов в хранилище, которое, вполне возможно, располагается на оборудовании, находящемся в частной собственности. Решения для защиты данных на основе репликации не слишком хороши в случае создания архивов или резервных копий на магнитных лентах, находящихся вне предприятия. А ведь большинству клиентов требуются обе эти возможности.

DPM 2007 развивает другой тип решений – подход к CDP на основе мгновенных снимков. Новая версия DPM делает мгновенные снимки каждые 15 минут, используя VSS и его технологию отслеживания изменений на уровне блоков с целью переноса из мгновенного снимка VSS на защищенный сервер

только измененных данных. В результате: отдельные мгновенные снимки на определенный момент времени имеют крайне небольшой размер, поскольку они содержат только изменения на уровне блоков. Учитывая то, что в новой версии существует поддержка на глубоком уровне и Exchange, и SQL, и Sharepoint, DPM имеет доступ к журналам приложений, и он в состоянии выполнить накат этих журналов в случае восстановления после ошибки. До тех пор, пока доступны журналы приложений (это обеспечивается при следовании оптимальным методикам и размещении журналов на отдельном носителе), DPM будет в состоянии выполнить их накат из последнего мгновенного снимка на определенный момент времени и обеспечить восстановление без потерь.

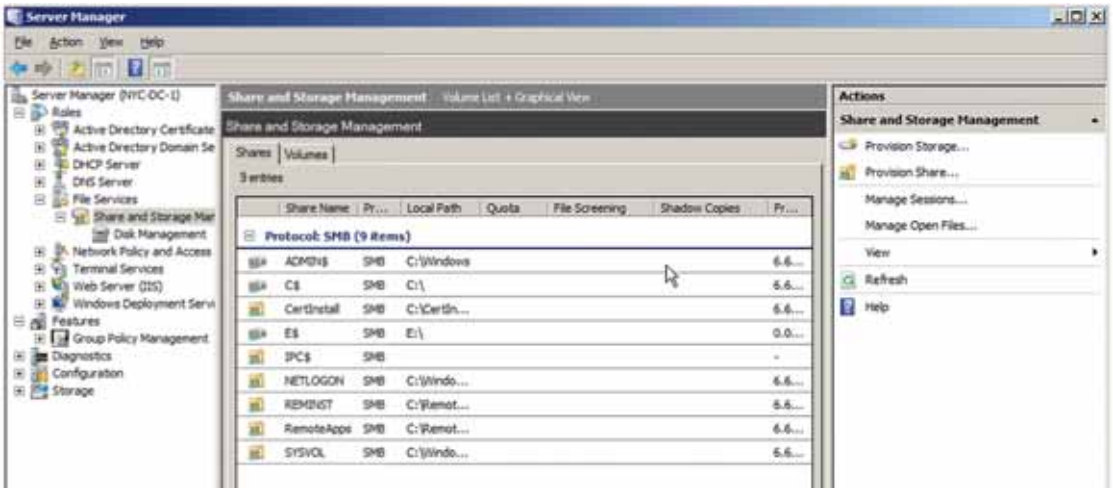

Рис. 1. Вид окна Server Manager.

Поддержка магнитных лент

Как говорилось ранее, в DPM 2007 была добавлена поддержка магнитных лент: данные можно перемещать с диска защищенного сервера на диск, подключенный к серверу DPM (D2D), на магнитную ленту, подключенную к серверу DPM (D2T), или защищенные данные можно разместить на диске сервера DPM перед их перемещением на магнитную ленту для длительного хранения (D2D2T).

Заключение

В заключение хотелось бы сказать несколько слов о лицензировании: оно останется таким же – по сокетам, что позволит, если нет особых требований (например, при создании кластеров), использовать самую дешевую версию – Standard. Что касается редакций, то аппаратные ограничения останутся такими же, как и в предыдущей версии (максимум 4 Гбайт памяти в 32-битном варианте, 32 Гбайт – для 64-битной версия для редакции Standard).

Если говорить о продукте в целом, сразу бросаются в глаза изменения интерфейса. Из особенностей можно отметить упрощение задач администрирования за счет использования нового Server Manager (рис. 1). Связанные задачи и службы сгруппированы вместе, что позволяет легко и быстро их находить. Кроме того, система указывает на проблемы в конфигурации в начале установки серверных задач, предотвращая многие грубые ошибки. Сервисы, запущенные случайно, легко определить и остановить, а фильтры Event Viewer позволяют выводить только относящуюся к проблеме информацию. Однако оснастка FTP-сервера, которая может понадобиться при настройке IIS, не включена в Server Manager.

В целом, можно признать новую версию, а также добавленные функции удачными. Удачны они потому, что в конечном результате выход новой версии призван был решить проблемы пользователей. И сейчас я знаю такие проекты, в которых применение новой версии поможет упростить жизнь администраторов заказчика. Естественно, внедрение должно проводиться постепенно, только после тестирования, но потенциал у продукта есть, и это не может не радовать.

Епищева Анна,
пресейл-инженер решений Microsoft, ДСИ ЛАНИТ