Шифрование баз данных как основа безопасности

В статье дан обзор функциональных особенностей решений семейства SafeNet DataSecure на базе специализированных кластеризуемых устройств для полностью централизованного управления ключами и прозрачного шифрования данных на уровне серверов приложений, баз данных, систем хранения и оконечных устройств. Публикация – продолжение темы защиты данных в БД, начатой в SN № 3/32, 2007.

Вадим Калмыков – генеральный директор компании DS Technologies

Введение

В условиях возрастающего числа нормативных требований и регулирующих актов (отраслевых, федеральных, на уровне Евросоюза и регионов мира, включая PCI DSS, ФЗ 152 "О персональных данных" и стандарт Банка России СТО БР ИББС-1.2-2009), а также увеличения доли распределенных корпоративных инфраструктур с возможностью доступа к чувствительной информации за пределами охраняемого периметра защита информации на уровне корпоративных файловых серверов, баз данных и при ее передаче становится стандартной компонентой всех современных ЦОД.

В крупных компаниях для стратегического планирования и управления текущими бизнес-процессами используются ERP/CRM/BI-системы, которые основаны на сборе и анализе больших объемов данных, хранящихся в СУБД. Таким образом, СУБД являются ядром всей IT-инфраструктуры, а поддержание их защищенности и доступности – одна из основных функций ИБ. В то же время интеграция шифрования в БД является технологически сложной задачей, в процессе которой необходимо учесть вопросы сохранения производительности и совместимости решения с используемыми приложениями.

В настоящее время можно выделить 3 класса решений обеспечения корпоративной ИБ при хранении данных на базе: 1) программных разработок; 2) в основном, аппаратных решений на уровне SAN/СХД/ленточных приводов/библиотек/HDD; 3) программно-аппаратных решений.

Основной недостаток первой группы решений – накладные затраты процессорной мощности для серверов приложений, на основе которых строится решение по шифрованию данных. Примером второго класса решений может служить решение Brocade, поставляемое в виде блэйд-модулей – Encryption Switch, устанавливаемых в директора класса DCX Backbone. Каждый из модулей обеспечивает шифрование потока данных с общей скоростью 100 Гбит/с и со скоростью 50 Гбит/с – сжатых данных. Минус этого класса решений в том, что они требуют "достраивания" до уровня законченного решения с учетом всех компонент IT-инфраструктуры и использованием ПО от третьих фирм.

Третья группа предлагает решения, как правило, в виде специализированных устройств/appliance, основа которых – стандартный сервер с несколькими криптопроцессорами. Лучшие из данного класса разработок позволяют осуществлять полностью консолидированное централизованное управление как пользовательскими ключами, так и ключами приложений совместно с обеспечением функций шифрования/дешифрования данных в рамках всей IT-инфраструктуры.

Наиболее критичным недостатком данного решения является хранение криптоключей вне защищенных хранилищ, по сути на обычных жестких дисках, где они могут быть считаны злоумышленниками без обнаружения данного факта администратором безопасности. Основным ограничителем по производительности в подобных решениях выступает сервер, на основе которого строится решение. В ряде разработок оно снимается возможностью их кластеризации в единый пул с поддержанием самобалансировки, однако производительность таких решений не достигает производительности аппаратных решений той же конфигурации. Основное преимущество – полная законченность решений.

Функциональные особенности ИБ-решений на базе SafeNet DataSecure

Решения SafeNet DataSecure развиваются на основе технологии компании Ingrian Networks, которую SafeNet приобрела в апреле 2008 г. (сама компания SafeNet в марте 2007 г. за $634 млн перешла в собственность частной компании Vector Capital, США – *прим. ред.*).

В основе технологии Ingrian – программные решения, обеспечивающие перенос (с помощью библиотек для C и Java) и реализацию механизмов шифрования, ЭЦП и управление ключами с серверов приложений и баз данных на специальные криптоустройства. Данное решение, названное Ingrian Network Attached Encryption ("шифрование по сети"), позволяет прозрачно для приложений добавлять функции защиты данных, снимая при этом дополнительную нагрузку с прикладного сервера при вызове операций шифрования и ЭЦП из приложений.

В настоящее время уникальность разработки SafeNet определяется тем, что это единственное решение своего рода, предельно упрощающее процесс интеграции в СУБД: внедрение решения сводится к установке агента и первоначальному шифрованию существующих данных. Бонусом к простоте установки является поддержка всех ведущих промышленных СУБД: Microsoft SQL Server 2000 и 2005, Oracle 8i, 9i, 10g и IBM DB2 v8, Teradata. Поддержка Oracle 11 будет добавлена в ноябре–декабре текущего года.

Законченные ИБ-решения SafeNet строятся на базе четырех основных продуктов:

- DataSecure i430/i116 – специализированного устройства для шифрования/дешифрования данных на уровне СУБД-сервера или сервера приложений, а также файловых систем;
- EdgeSecure i10 – специализированного устройства для шифрования/дешифрования данных в удаленных офисах и филиалах;
- SafeNet KeySecure – специализированного устройства для консолидированного хранения и управления ключами;
- программных агентов ("коннекторов").

Поддерживаемые алгоритмы шифрования Ingrian DataSecure представлены в табл. 1.

Производительность DataSecure модели i430 при шифровании строки в 35 символов алгоритмом AES с 256-битным ключом:

- до 100 000 оп/сек с использованием двух устройств и утилиты пакетной вставки;
- до 40 000 оп/сек при использовании одного устройства и утилиты пакетной вставки;

Табл. 1. Поддерживаемые алгоритмы шифрования Ingrian DataSecure

Алгоритм	Поддерживаемые операции	Описание	Примечание
AES	Шифрование Расшифрование	Симметричный алгоритм	наиболее безопасный и быстрый
DES	Шифрование Расшифрование	Симметричный алгоритм	взломан, должен использоваться только при необходимости поддержки старых приложений
3DES (DESede)	Шифрование Расшифрование	Симметричный алгоритм	Менее безопасен чем AES
HMAC-SHA1	Генерация MAC Проверка MAC	Имитовставка (код аутентичности сообщения)	MAC используется для проверки целостности и аутентичности. Только обладатель ключа может создать или проверить MAC.
RC4	Шифрование Расшифрование	Симметричный алгоритм	Очень медленный.
RSA	Шифрование Расшифррование ЭЦП Проверка ЭЦП	Асимметричный алогритм	Для шифрования с открытым ключом и ЭЦП. Более медленный, чем симметричные шифры.
SEED	Шифрование Расшифрование	Симметричный алгоритм	Национальный стандарт шифрования Кореи.

– до 10 000 оп/сек при миграции базы данных;

– до 3 500 одиночных оп/сек при вставке в БД (INSERT).

Основные функциональные возможности решений на базе DataSecure:

– криптографические операции (симметричное и асимметричное шифрование, ЭЦП, генерация MAC (Message Authentication Code), генерация случайных чисел);

– коммуникация между DataSecure и клиентами происходит по SSL/TLS с возможностью одно- или двусторонней аутентификации с помощью сертификатов и пар "логин–пароль";

– детальная спецификация прав для каждого пользователя и администратора, включая количество криптоопераций, дни недели и отрезки времени;

– соответствие стандартам PCI DSS, FIPS 140-2 Level 2 и Common Criteria Evaluation Assurance Level 2;

– опция авторизации ряда функций минимум двумя администраторами;

– функция резервного копирования, кластеризации и распределения нагрузки;

– выполнение до 100 000 криптоопераций в сек. (AES 256-битный ключ и др.);

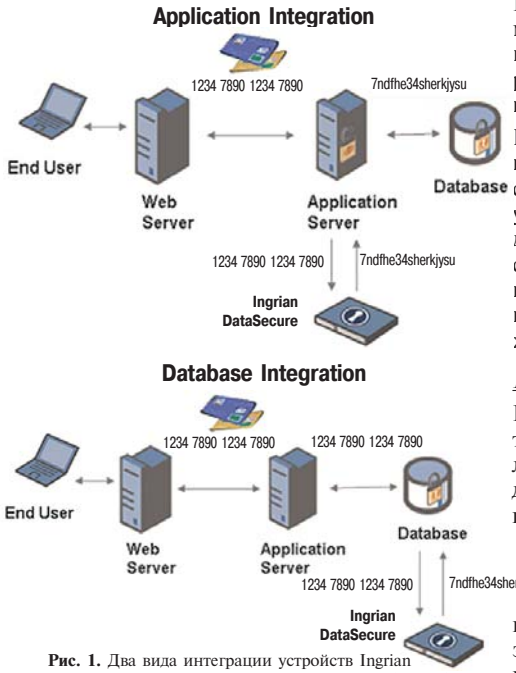


Рис. 1. Два вида интеграции устройств Ingrian DataSecure: на уровне приложений (вверху) и баз данных (внизу).

– шифрование за физическими пределами организации;

– автоматизированная ротация ключей;

– ведение подробных аудиторских логов и активное оповещение о возможных атаках;

– защита от физического доступа к ключам и критичным параметрам безопасности: при вскрытии нарушаются пломбы, расположенные на корпусе и дверцах устройства, что позволяет визуально идентифицировать взлом.

Физически DataSecure состоит из модифицированной серверной платформы Dell с интегрированным криптомодулем, непосредственно производящим операции шифрования, подписи и генерации случайных чисел, защищенным хранилищем, содержащим ключи и важные настройки безопасности, а также усиленным корпусом с двумя замками, защищающими переднюю панель.

Возможны три вида интеграции устройства Ingrian DataSecure в IT-инфраструктуру: на уровне приложения, БД или файловой системы (рис. 1).

Преимущество интегрирования на уровне приложений в том, что время, в течение которого защищаемые данные находятся в открытом виде, – минимально, что создает более безопасную среду. К тому времени, когда данные покидают сервер приложений, они уже зашифрованы.

Преимущество интегрирования на уровне баз данных состоит в автоматизации шифрования с минимальными изменениями для приложений, либо вообще без таких изменений. В этом случае для повышенной безопасности данные могут передаваться от приложения к БД по каналу SSL/TLS.

Интеграция на уровне файловой системы позволяет защитить файлы и папки пользователей незаметным для них образом, что актуально при использовании в корпорации ноутбуков.

При интеграции DataSecure на уровне БД в некоторых случаях требуется изменить существующие индексы, а интеграции на уровне приложения сводятся к добавлению двух-трех строк кода, устанавливающих соединение с устройством и выполняющих операцию шифрования (дешифровывания), при этом соединение также может быть защищено с помощью SSL/TLS.

Интеграция на уровне приложения

Криптооперации на уровне приложения требуют изменений в исходном коде приложения и используют библиотеки Ingrian для C или Java (доступны ICAPI, MSCAPI, и PKCS#11, а также z/OS и Java Cryptography Extension), которые устанавливаются на сервере приложения.

Интеграция на уровне приложения позволяет достичь набольшего уровня защищенности, поскольку данные расшифровываются непосредственно перед их использованием в приложении. При интеграции на уровне БД данные передаются от БД к серверу приложений в открытом виде (если соединение не защищено SSL/TLS).

На уровне приложений доступны большинство функций DataSecure, в том числе шифрование файлов, генерация новых ключей и предоставление разрешений на работу с ключами другим пользователям и группам.

Интеграция на уровне БД

С помощью библиотеки Ingrian, а также создаваемых в БД триггеров, процедур и пользовательских функций (все вместе называется "коннектор") DataSecure позволяет шифровать данные непосредственно перед их вставкой в БД и расшифровывать перед выдачей авторизованным пользователям. Таким образом, для приложений данный способ является наиболее прозрачным и в большинстве случаев не требует дополнительных изменений.

Перед использованием этого способа необходимо начальное шифрование ("миграция") данных, которые подлежат защите, для чего DataSecure необходим полный доступ к таблице на время миграции. Существует также он-лайн миграция, сводящая время пребывания БД в офф-лайне к 5 минутам. Данный способ миграции осуществляется с помощью специальной утилиты под прямым надзором специалистов SafeNet.

Шифрование выполняется на уровне столбцов таблиц, для каждого из которых можно задать свой алгоритм и режим шифрования, ключ и его длину, а также владельца. Для каждого шифруемого столбца DataSecure создает новый столбец с именем <имя_столбца>_NEW, куда помещаются зашифрованные данные. Также создается один служебный индексный столбец. Время миграции зависит от конфигурации и загруженности сервера БД, и составляет около 1 млн записей в минуту для серверов средней производительности.

Зашифрованные данные хранятся в виде двоичных строк в полях типа RAW (для Oracle) и VARBINARY (MSSQL). Поскольку данные типы могут быть использованы для индексации, для новых зашифрованных столбцов можно создать доменный индекс и это также будет прозрачно для приложений. Нужно только иметь в виду, что в связи с блочной природой симметричных шифров размер нового столбца будет предсказуемо больше оригинального – он будет увеличен до ближайшего числа, делящегося нацело на 8 или 16 (в зависимости от размера блока алгоритма).

Во время миграции оригинальная таблица переименовывается в <имя_таблицы>_NEW, и создаются два вида: <имя_таблицы>_IDV и <имя_таблицы>. Первый использует пользовательские функции для соединения с сервером шифрования NAE, проверкой привилегий пользователя и выполнения автоматического шифрования и расшифровывания данных при обращении к ним.

Второй вид построен на основе предыдущего и выглядит как оригинальная незашифрованная таблица. Он скрывает появление двух новых столбцов и использует триггеры для шифрования и расшифровывания данных (для INSERT, UPDATE и SELECT) и поэтому может использо-

ваться приложениями и пользователями для прозрачного доступа к этим данным.

После миграции в консоли управления DataSecure доступны следующие функции:

- просмотр истории изменений БД и откат последней операции;
- удаление временных таблиц;
- завершение или откат последней неудачной операции;
- создание доменного индекса (Oracle);
- ротация ключей;
- снятие шифрования данных;
- удаление старых незашифрованных данных;
- обновление таблицы до версии коннектора.

Контроль доступа к зашифрованным данным в БД

Для того чтобы зашифровать или расшифровать данные, пользователь БД должен быть поставлен в соответствие пользователю на устройстве DataSecure. Это соответствие задается в консоли управления и хранится в таблице ING_AUTHORIZED_USER в БД в виде зашифрованной и подписанной строки.

У соответствующего пользователя DataSecure должен быть доступ к нужному ключу. В консоли управления каждому пользователю можно задать частоту и временные промежутки доступа к ключу шифрования, и, следовательно, к данным (например, не более 60 считываний в час в рабочие дни с 9 до 18 часов).

Также на устройстве DataSecure можно задать пользователя по умолчанию, который будет использован, если не найдено прямого соответствия пользователя БД внутреннему пользователю устройства. Это наиболее оптимальный способ сообщить приложению, что у него нет прав на просмотр защищенных данных.

Интеграция на уровне файловой системы

DataSecure позволяет осуществлять прозрачное шифрование файлов: запросы к файловой системе перехватываются коннектором, нужный файл расшифровывается и затем передается пользователю, и наоборот. При этом данные на диске хранятся только в зашифрованном виде, но для авторизованных пользователей и приложений файловая система выглядит как обычно, и они могут не подозревать о существовании защиты DataSecure.

Коннектор для файловой системы в настоящий момент поддерживает Microsoft Windows 2003 Server и файловую систему NTFS и состоит из Windows-сервиса, работающего под пользовательским аккаунтом, и драйвер фильтра файловой системы, который выполняется в ядре Windows.

В консоли DataSecure создатся 256-битный AES-ключ (File System Key, FSK), который затем отправляется на коннектор. Этот ключ используется для шифрования индивидуальных ключей. В зависимости от конфигурации на DataSecure на каждом коннекторе может быть один или несколько FSK-ключей. После остановки сервиса файлового коннектора ключи, находящиеся в памяти, безопасно затираются.

Шифрование и расшифровывание файлов производится локально на пользовательской системе, поэтому соединение с сервером необходимо только для начального получения FSK-ключа и политик доступа, а также их периодического обновления. После получения FSK коннектор создает индивидуальный 128-битный AES-ключ для каждого шифруемого файла (эти ключи называются File Encryption Keys). Такие индивидуальные ключи хранятся в заголовках файлов.

Для шифрования файл делится на части размером 512 байтов. Затем каждая часть шифруется отдельно в режиме CBC и с использованием уникального инициализационного вектора (вектор создается на основе порядкового номера данной части файла с использованием алгоритма ESSIV). Шифрование каждой части отдельно позволяет оптимизировать доступ к файлам с произвольного места.

При использовании этого вида интеграции снижение производительности будет зависеть от количества и общего размера файлов. Заметно производительность снизится в процессе начальной миграции незашифрованных файлов, тем не менее, все файлы будут доступны. Кроме того, поддерживается прозрачная демиграция файлов, т.е. их расшифровывание и снятие с них защиты.

DataSecure использует двухуровневую систему контроля доступа. Первый уровень разрешений определяется на самом Data-Secure и различает доступ на чтение и запись как к открытому содержимому, так и к шифртексту файла на уровне групп и пользователей. Пользователи, для которых не задана явная политика доступа, используют политику доступа по умолчанию. Второй уровень соответствует встроенной системе доступа Windows. Оба уровня должны разрешать доступ к файлу данному пользователю.

Если пользователь, запрашивающий файл, определен как выполняющий резервное копирование, то файловый коннектор дает доступ к зашифрованным данным, что позволяет безопасно создать резервную копию зашифрованных файлов.

Обеспечение ИБ в удаленных офисах

Во многих компаниях, особенно розничных организациях, есть потребность зашифровать важную информацию в отдаленных офисах, филиалах или точках продаж. Многие розничные продавцы должны шифровать номера кредитных карт в точке продажи и затем передать эти данные в центр их обработки и хранения. Для таких ситуаций Ingrian были разработаны Enterprise Manager и EdgeSecure.

Эти решения, первоначально разработанные специально для сети кофеен Starbucks, подразумевают установку устройства EdgeSecure в каждом удаленном местоположении компании (рис. 2) и управление данной сетью через Enterprise Manager в центре обработки и хранения данных. Номера кредитных карт шифруются EdgeSecure сразу же после их получения и хранятся локально до проведения ежедневной выгрузки в ЦОД для последующей обработки и хранения. Таким образом, при краже или взломе сервера, хранящего зашифрованные номера кредитных карт в удаленном офисе, никакой опасности не возникает. Даже если злоумышленник выкрадет EdgeSecure, то он не сможет получить доступ к ключу шифрования данных.

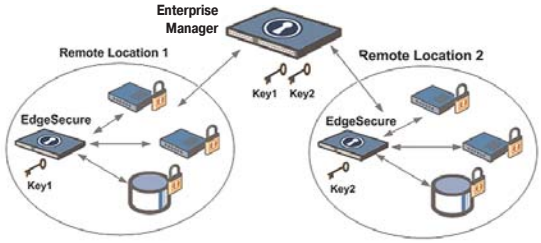


Рис. 2. Архитектура решения для безопасного хранения/передачи данных в удаленных офисах на безе решений SafeNet Enterprise Manager и EdgeSecure.

Кластеризация и балансировка нагрузки

Кластеризация позволяет нескольким устройствам DataSecure использовать одинаковые настройки пользователей, групп, ключей, политик доступа и т.д. Данные, зашифрованные на одном устройстве кластера, могут быть прозрачно расшифрованы другим, и наоборот. Аналогично, изменения конфигурации одного устройства, входящего в кластер, могут быть автоматически реплицированы на все остальные устройства (администратор может запретить реплицировать некоторые параметры).

Для того, чтобы устройство смогло присоединиться к кластеру, необходимы пароль и зашифрованный файл-ключ кластера. Такая двухуровневая система безопасности позволяет защититься от неавторизованных устройств, которым известен только пароль, но не файл-ключ. Кроме того, файл-ключ используется для авторизации членов кластера при репликации и синхронизации настроек. Если он украден или скомпрометирован, кластер должен быть разъединен и воссоздан заново.

Пароль используется администратором для управления кластером: добавления новых членов и восстановления резервной копии конфигурации.

Балансировка нагрузки выполняется на клиентской стороне. Эта функция позволяет задать несколько устройств первого, второго и третьего уровня. В штатном режиме клиент распределяет запросы между устройствами первого уровня. Если устройства первого уровня недоступны, клиент переключается на устройства второго уровня и т.д. Чтобы балансировка работала корректно, все устройства должны быть членами одного кластера.

Заключение

Когда организация сталкивается с проблемой соответствия законодательству в области ИБ или нуждается в защите больших объемов чувствительных данных, DataSecure является одним из наиболее привлекательных решений, удовлетворяющих потребности как администраторов баз данных, так и специалистов по информационной безопасности организации.

Это определяется, прежде всего, максимально простой интеграцией в существующую инфраструктуру организации, высокой производительностью и масштабируемостью, а также законченностью решения с точки зрения обеспечения ИБ для всей компании и компонент IT-инфраструктуры.

Вадим Калмыков,
генеральный директор
компании DS Technologies

HA/DR-решения – работоспособность в условиях постоянных изменений

Публикация – продолжение темы "Управление доступностью данных", начатой в SN №№ 2(35) 2008, 4(33) 2007.

Алексей Чеканов – генеральный директор, компания Almitech

Введение

Данная статья адресована в первую очередь тем компаниям, критические бизнес-процессы которых сильно зависят от ИТ-инфраструктуры, и, как следствие, последняя должна обладать высокой степенью отказоустойчивости.

Не вдаваясь в детали того, как были реализованы решения обеспечения высокой доступности (HA) и послеаварийного восстановления (DR), какие использовались системы хранения данных и механизмы репликации и кластеризации, давайте посмотрим, с какими проблемами сталкивается организация при эксплуатации и развитии ИТ-инфраструктуры.

Тестирование HA/DR-систем

Утверждение о том, что системы HA/DR необходимо тестировать, не подвергается никакому сомнению. Однако неумолимая статистика демонстрирует весьма неутешительные результаты. В среднем, один из четырех тестов дает сбой, и это при том, что тестирование проводится в контролируемой среде – с управляемым отключением элементов инфраструктуры, частичным сохранением элементов ядра и т.п.

Что же является причиной такого поведения для решений, использующих, казалось бы, достаточно зрелые технологии? В своем аналитическом отчете (по материалам "Symantec 2008 Disaster Recovery Research") за 2008 год (рис. 1) компания Symantec приводит результаты опроса 1000 сотрудников крупных компаний из 15 различных стран.

Как мы видим, причины сбоев можно разделить на три основных категории.

Первая связана с процессами послеаварийного восстановления и описывающими их планами. Основные проблемы здесь, как правило, кроются в несогласованности процессов и в неактуальности планов послеаварийного восстановления. Не вдаваясь глубоко в эту тему, которая достойна отдельной статьи, обозначим несколько направлений, позволяющих заметно улучшить ситуацию. Это формализация зависимостей между элементами инфраструктуры, проведение комплексного тестирования и использование средств автоматизации для разработки и поддержания в актуальном состоянии планов послеаварийного восстановления.

Следующая категория проблем заключается в нехватке ресурсов, как материальных, так и человеческих. Если руководство организации не уделяет должного внимания задаче обеспечения непрерывности бизнеса, очевидно, что и финансирование будет осуществляться по остаточному принципу. В результате возникают проблемы недооснащенности резервных площадок, люди не проходят необходимого обучения, и, как следствие, в "час X" система срабатывает совсем не так, как это ожидается. Для решения этих проблем руководителям, ответственным за обеспечение работоспособности ИТ-инфраструктуры, необходимо активно взаимодействовать с высшим руководством организации, донося до них важность обеспечения непрерывности бизнеса и ИТ-сервисов и получая необходимую поддержку на высшем уровне.

И, наконец, последняя по порядку, но, пожалуй, наиболее затратная по ресурсам категория – это обеспечение работоспособности используемых технологий. К сожалению, сам факт инвестиций миллионов долларов в кластерные решения и распределенные системы хранения данных еще не означает того, что в случае чрезвычайной ситуации спроектированное и внедренное решение обеспечит требуемый уровень восстановления ИТ-сервисов. Даже полное тестирование системы в момент ее сдачи в эксплуатацию не гарантирует того, что в момент чрезвычайной ситуации через полгода будут достигнуты те же показатели восстановления (RTO и RPO[1]), что и в момент тестирования. Давайте проанализируем причины возникновения подобных ситуаций.

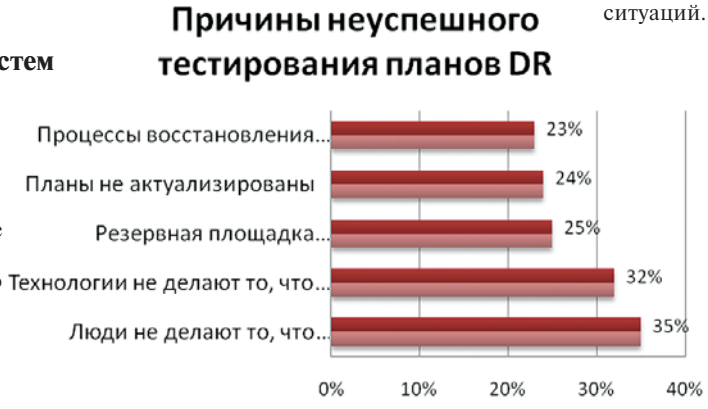


Рис. 1. Причины неуспешного тестирования планов послеаварийного восстановления

Основные причины неработоспособности DR-решений

На первом месте (до 75% причин сбоев при проведении тестирования) оказывается **расхождение основной и резервной конфигураций**. ИТ-инфраструктура является наиболее динамичным элементом инфраструктуры организации, подвергаемым, с одной стороны, прессингу бизнес-требований, а с другой – воздействию стремительно прогрессирую-

щих технологий. В результате в "боевые" системы постоянно вносятся различные изменения – расширяются вычислительные мощности, подключаются новые системы хранения данных и параллельно меняются версии установленного программного обеспечения, устанавливаются обновления и т.п. Несмотря на все усилия, предпринимаемые ИТ-персоналом организации, рано или поздно в резервной инфраструктуре начинают накапливаться отличия от основной. Какие-то из них могут быть непринципиальными и только незначительно влиять на производительность, а другие могут быть гораздо серьезнее и приводить к потере данных и необходимости ручного вмешательства при переходе на резервную площадку.

Следующий по серьезности риск – это **некорректное построение решений** обеспечения высокой доступности. Ошибки могут быть допущены как при проектировании архитектуры, так и при ее реализации с использованием конкретных систем. Результатом таких ошибок могут быть как неполная работоспособность решения (хотя это чаще всего выявляется при первоначальном тестировании), так и проблемы с производительностью, и необходимость ручного вмешательства в момент аварии.

И на последнем месте – проблемы производительности, вызванные неполным соблюдением рекомендаций производителей решений и лучших практик. Несмотря на меньший уровень опасности, подобного рода проблемы могут причинять организации финансовый ущерб, вызванный необходимостью инвестиций в дополнительные вычислительные мощности, притом, что существующая инфраструктура способна функционировать с большей нагрузкой.

Новый термин – Disaster Recovery Management

Чтобы не изобретать очередной велосипед, давайте посмотрим на мировой опыт в данной области. В этом году все чаще в литературе на тему обеспечения непрерывности ИТ-сервисов стал попадаться термин **Disaster Recovery Management (DRM)** – управление послеаварийным восстановлением. Как и сам термин "Disaster Recovery", который чаще всего относят именно к восстановлению ИТ, новый подход также посвящен управлению процессами обеспечения эффективного послеаварийного восстановления.

Как правило, DRM включает в себя процессы автоматического тестирования, контроля изменений и снижения рисков, и применяется к сложной ИТ-инфраструктуре, обеспечивающей высокий уровень доступности и эффективное послеаварийное восстановление. Основным принципом DRM является регулярный мониторинг инфраструктуры с целью своевременного выявления несоответствия конфигураций, нарушения зависимостей между системами, сбоев в процессах репликации данных, нарушения соглашений об уровне сервиса и т.п. В случае обнаружения подобного рода проблем, система DRM должна своевременно информировать администратора, предоставив ему всю необходимую информацию с должным уровнем детализации.

Важным аспектом является наличие внутри DRM-решения базы знаний, описывающей существующие уязвимости в архитектуре и реализации DR- и HA-решений. По своей сути, подобная база знаний напоминает базу уязвимостей сканера безопасности, с той лишь разницей, что анализ проводится в разрезе задач обеспечения непрерывности функционирования. Немаловажным аспектом является и возможность добавления собственных сигнатур для нестандартных приложений, которые, тем не менее, могут являться ключевыми для организации.

Рынок решений DRM

Вполне логично, что первыми производителями решений DRM стали производители систем хранения данных и решений по обеспечению высокой доступности, такие, как EMC или Symantec. При высоком качестве работы этих решений применительно к системам того же производителя, существенным их недостатком является невозможность контролировать сложные среды, построенные с использованием решений различных производителей.

Следующим поколением решений DRM стали универсальные решения, работающие с системами всех основных производителей СХД и HA/DR систем. Ярким представителем этого сегмента является компания Continuity Software, которая, по оценке аналитической компании Taneja Group[2], на сегодня является *"единственным производителем решений DRM, который предлагает возможность тестирования DR-решений и устранения несоответствий в гетерогенных средах с СХД и решениями по репликации данных от различных производителей"*.

Заключение

Использование решений DRM не избавит организацию от необходимости регулярного тестирования, но оно может дать два преимущества,

1. Вероятность успешного прохождения теста существенно повышается, что позволяет сократить как трудозатраты на тестирование, так и время простоя систем

2. С максимальной вероятностью DR-решение будет сохранять свою работоспособность в промежутках между тестами, которые могут достигать года, если не больше.

А для того, чтобы принять окончательное решение о необходимости решения DRM, можно провести пробный аудит – и уже увидев количество выявленных уязвимостей, решать, стоит ли приобретать подобное решение для регулярного использования.

Завершая статью, хочется обратить внимание, что регулярный аудит работоспособности HA/DR решений – это только один из элементов эффективной системы обеспечения непрерывности ИТ-сервисов, способствующий снижению операционных рисков. Глядя на жизненный цикл создания системы обеспечения непрерывности ИТ-сервисов:

- *определение целевых показателей восстановления путем проведения анализа воздействия на бизнес;*
- *разработка стратегии обеспечения непрерывности ИТ-сервисов, определяющей, как будет обеспечиваться выполнение соглашений об уровни предоставляемого сервиса (SLA), какие подходы будут использоваться, и как будет контролироваться достижение целей;*
- *реализация стратегии – создание необходимой инфраструктуры и поддерживающих ее процессов, включая процессы мониторинга работоспособности, управления изменениями, управление инцидентами, проблемами и т.п.;*
- *разработка планов послеаварийного восстановления;*
- *обучение персонала;*
- *регулярное тестирование системы обеспечения непрерывности ИТ-сервисов;*
- *регулярный и всесторонний аудит системы обеспечения непрерывности ИТ-сервисов;*
- *периодический пересмотр целевых показателей, и, как следствие, переход на следующий цикл развития системы,*

видим достаточно широкое поле для внедрения новых технологий.

Как показывает опыт, чем большее количество элементов системы удается автоматизировать, будь то автоматизация процессов мониторинга работоспособности систем или ведение планов послеаварийного восстановления, тем эффективней работает система в целом. А следствием этого является четкое выполнение соглашений об уровне обслуживания и поддержка бизнес-процессов ИТ-сервисами на требуемом уровне.

Алексей Чеканов,
компания Almitech

HDCS выбирает 3PAR

Сентябрь 2009 г. – Глобальный провайдер облачных сервисов – Horizon Data Center Solutions (HDCS) выбрал решения 3PAR Utility Storage для своих новых сервисов FlexSafe Cloud.

Решение 3PAR InServ® T-Class Storage Server развернуто в датацентре HDCS в Далласе (США), как часть более широкого датацентра, основанного на архитектуре 3cV – комбинации 3PAR® Utility Storage с HP BladeSystem c-Class серверами и VMware® инфраструктурой.

FlexSafe Cloud сервис обеспечивает клиентов виртуализированной вычислительной мощностью, возможностями хранения данных и DR-функциональностью в рамках защищенной, высокодоступной и избыточной архитектуры в соответствии с моделью IaaS (infrastructure-as-a-service).

1) **RTO** – recovery time objective, целевое время восстановления системы, показатель, определяющий, за какое время после аварии будет восстановлена работоспособность системы, возможно, с определенным уровнем снижения производительности или ограничением функциональности

RPO – recovery point objective, целевая точка восстановления, показатель, определяющий максимальный объем данных, который может быть потерян в случае аварийной ситуации

2) http://www.infostor.com/index/articles/display/8078564342/s-articles/s-infostor/s-volume-13/s-Issue_9/s-Features/s-Why_you_need_disaster_recovery_management.html

Новое семейство жестких дисков Hitachi GST CinemaStar

Сентябрь 2009 г. – Компания Hitachi Global Storage Technologies (Hitachi GST) анонсировала новое семейство 3,5-дюймовых жестких дисков CinemaStar™. Обновленная линейка на базе 500 Гбайт пластин включает в себя винчестеры CinemaStar 7K1000.C с емкостью 1 Тбайт (7200 rpm) и CinemaStar 5K1000 CoolSpin™ с емкостью 1 Тайт.

Оба продукта удовлетворяют самым жестким требованиям к работе с потоковым видео высокой четкости, характеризуются надежностью, большой емкостью, низким уровнем шума, улучшенными функциями работы с аудио и видео, низким энергопотреблением и тепловыделением. Диски емкостью 1 Тбайт способны хранить почти 250 часов видео в формате MPEG-41 и работать с несколькими потоками видео одновременно. Это делает CinemaStar 7K1000.C и CinemaStar 5K1000 идеальными для потребительской электроники, такой как цифровые видеомагнитофоны, устройства записи на DVD/жесткий диск, телевизоры с функцией записи цифрового видео, медиацентры и системы видеонаблюдения.

Кроме возросшего диапазона емкости от 160 Гбайт до 1 Тбайт, новое семейство CinemaStar 5K1000 обладает инновационной технологией Hitachi CoolSpin. Эта технология использует оптимизацию скорости работы привода для того, чтобы достичь уникального баланса производительности, низкого энергопотребления и бесшумности. Оптимизация работы двигателя диска направлена на уменьшение скорости вращения шпинделя, что приводит к снижению гармонического резонанса и практически бесшумной работе CinemaStar 5K1000 – 2,4 Б в рабочем режиме. При этом он потребляет менее 3,3 Вт в режиме ожидания и выделяет меньше тепла, что является решающим фактором в разработке экологически чистых цифровых видеорешений.

В жестких дисках CinemaStar реализована запатентованная инновационная технология Hitachi SmoothStream, обладающая оптимальным набором функций для безупречной работы винчестера с аудио- и видеоприложениями. К примеру, SmoothStream настраивает жесткий диск таким образом, что он воспринимает поток визуальной информации покомандно, что помогает интеграторам устанавливать различные аудио-, видео- и IT-приложения на одной платформе. Новые диски CinemaStar стали четвертым поколением на основе технологии SmoothStream.

Ключевые функции жестких дисков CinemaStar:

– *интеллектуальный командный протокол*, позволяющий оптимизировать настройки винчестера для безупречного воспроизведения потокового видео;

– *улучшенное автоматическое управление питанием* с множественными режимами питания для обеспечения необходимой производительности при наименьшем энергопотреблении;

– *расширенный диапазон температур*: 0–70°C (для CinemaStar 5K1000) и 0–65°C (для CinemaStar 7K1000), что позволяет даже при рабочем состоянии винчестера не использовать вентилятор и добиваться практически бесшумной работы. Это очень актуально для пользователей, чьи компьютеры находятся в спальне;

– *интеллектуальные функции спящего режима* поддерживают качество сигнала данных и их надежное долгосрочное хранение;

– *улучшенные механизмы привода* обеспечивают 1,2 млн часов безотказной работы (оценка времени безотказной работы основана на использовании винчестеров в типичной потребительской электронике/системах видеонаблюдения) при круглосуточном использовании компьютера любителями музыки и фильмов;

– *запатентованный Hitachi механизм загрузки/разгрузки рампы* предотвращает преждевременный износ винчестера и защищает его во время бездействия;

– *управление температурой винчестера* с целью увеличить степень надежности работы при многочасовых операциях кодирования и декодирования видео (что особенно актуально сейчас, когда фильмы в формате HD могут длиться более 3-х часов).

Жесткие диски CinemaStar 7K1000.C и CinemaStar 5K1000 с разными объемами памяти (от 160 Гбайт до 1 Тбайт) поступят в продажу в 4 кв. 2009 г.

Первый конвергентный адаптер 40GbE – Mellanox ConnectX-2 40G

Октябрь 2009 г. – Компания DSCon, официальный дистрибьютор компании Mellanox® Technologies, ведущего производителя средств коммутации InfiniBand и 10Gbit Ethernet, в России и странах СНГ, анонсировала о доступности первого в отрасли конвергегнтного адаптера 40GbE – Mellanox ConnectX-2 40G.

Адаптеры для конвергентных сетей Mellanox ConnectX-2 40G позволят увеличить до максимума эффективность использования современных многоядерных процессоров в центрах обработки данных, достичь беспрецедентного уровня соединений Ethernet между серверами и хранилищами, а также придадут ускорение усилиям, направленным на унификацию LAN и SAN. Адаптеры 40 Gigabit Ethernet Mellanox ConnectX-2 40G, обеспечивая возможность развертывания высокоскоростных сетей Ethernet, оптимизированных для максимальной эффективности, создают основу для нового поколения центров обработки данных, сокращая при этом расходы, энергопотребление и упрощая архитектуру.

Современным центрам обработки данных для обеспечения максимального количества транзакций в секунду, поддержки растущих запросов к сетевому окружению со стороны виртуальных сред и реальной консолидации ввода/вывода требуются сетевые решения с пропускной способностью более 10 Гбит/с. Адаптеры 40 Gigabit Ethernet Mellanox ConnectX-2 40G предоставляют IT-менеджерам сетевое решение для построения наиболее эффективных и совершенных центров обработки данных.

Доступные уже сейчас адаптеры ConnectX-2 40G поддерживают аппаратную виртуализацию ввода/вывода, включая Single Root I/O Virtualization (SR-IOV), и предоставляют средства, необходимые для создания конвергентной сети с поддержкой Data Center Bridging (DCB). Адаптеры 40 Gigabit Ethernet от Mellanox упрощают внедрение Fibre Channel over Ethernet (FCoE) благодаря аппаратной разгрузке и поддержке инкапсуляции кадров T11 Fibre Channel. Однопортовый адаптер ConnectX-2 EN 40G поставляется с одним коннектором QSFP, пригодным для использования с медными или оптическими кабелями, что обеспечивает высочайший уровень гибкости в использовании.

Будучи частью портфолио адаптеров 10 Gigabit Ethernet и InfiniBand от Mellanox, ConnectX-2 40G поддерживается всесторонним комплектом драйверов для Microsoft Windows, различных дистрибутивов Linux, VMware и Citrix XEN Server. Адаптеры ConnectX-2 EN 40G поддерживают непрерывную разгрузку и полностью совместимы со стандартными стеками TCP/UDP/IP.

Дополнительная информация: *http://www.dscon.ru/san/mellanox_40gig_ethernet_nic_connectx-2.htm*.

Cisco покупает TANDBERG

Октябрь 2009 г. – Cisco объявила о подписании обязывающего соглашения, позволяющего сделать официальное предложение о покупке компании TANDBERG со штаб-квартирами в Осло (Норвегия) и Нью-Йорке, мирового лидера в области видеокоммуникаций, поставщика широкого ассортимента видеотерминалов мирового класса и инфраструктурных сетевых решений, отличающихся высоким уровнем совместимости и взаимодействия. В случае удачного завершения этой сделки Cisco расширит свой портфель продуктов для совместной работы и предложит расши-

ренный спектр решений более широкому кругу заказчиков, что позволит ускорить распространение данной технологии на мировом рынке.

По условиям подписанного соглашения, Cisco сделает тендерное предложение о покупке всех находящихся в обороте акций TANDBERG по цене в 153,5 норвежских крон за акцию на общую сумму около 3,0 млрд долларов. Это на 11,0 процентов выше цены акций TANDBERG на конец предыдущего биржевого дня и на 25,2 процента выше средневзвешенной цены акций TANDBERG за предыдущие 3 месяца. Данное предложение получило единогласную поддержку в совете директоров TANDBERG.

Завершение сделки ожидается в первой половине календарного 2010 г. Точная дата будет зависеть от выполнения стандартных договорных условий, включая согласование сделки в регулирующих органах США и других стран. Cisco планирует включить это приобретение в прибыль, рассчитываемую без учета правил GAAP, за 2011 финансовый год.

Лучшие разработки TANDBERG для видеотерминалов и сетевых инфраструктур будут интегрированы в архитектуру мирового класса – архитектуру Cisco для совместной работы. В результате расширятся возможности межкорпоративной и мультивендорской совместимости и упростится использование продуктов всех типов – от настольных устройств до многоэкранных систем TelePresence, погружающих пользователя в виртуальную среду. Широкая совместимость будет выгодна не только заказчикам, но и партнерам Cisco, а также ее конкурентам, поскольку повысит интерес пользователей к системам совместной работы во всех странах мира.

В случае завершения сделки в состав Cisco вольются полторы тысячи сотрудников TANDBERG, включая специалистов норвежского и британского исследовательских центров. Это особенно важно для Cisco, стремящейся упрочить свое лидирующее положение в области новаторских видеотехнологий и увеличить объемы бизнеса на этом рынке. По завершении сделки главный исполнительный директор TANDBERG Фредрик Халворсен (Fredrik Halvorsen) возглавит новую технологическую группу TelePresence, которая будет работать под руководством старшего вице-президента Cisco по новым технологиям Мартина де Бира (Marthin De Beer).

2 Тбайт HGST HDD со скоростью 7200 rpm

Август 2009 г. – Компания Hitachi Global Storage Technologies (Hitachi GST) объявила о начале поставок винчестеров объемом 2 Тбайт со скоростью вращения 7200 rpm. Новый 3.5-дюймовый накопитель Deskstar™ 7K2000 в продаже в России с сентября 2009 г.

Hitachi Deskstar 7K2000 представляет четвертое поколение винчестеров с 5-пластинной конструкцией с разряженной плотностью и технологией, перпендикулярной магнитной записи. Накопитель характеризуются сверхнизким уровнем шума, обладает 32 Мбайт кэш-памяти и интерфейсом SATA с производительностью 3 Гбит/с.

В дополнение к выпуску Deskstar 7K2000 Hitachi GST обновляет линейку жестких дисков большой емкости. Компания представила семейство накопителей Deskstar 7K1000.C со скоростью вращения шпинделя 7200 rpm, плотностью 500 Гбайт на пластину и объемом от 160 Гбайт до 1 Тбайт. Как и в предыдущих поколениях жестких дисков Hitachi, размер секторов на пластине накопителей 7K2000 и 7K1000.C составляет 512 байт. Винчестеры оснащены запатентованным наклонным механизмом загрузки/разгрузки диска для повышения уровня противоударной защиты и поддерживают технологию Thermal Fly-height Control (TFC), которая управляет высотой головок диска во время процесса чтения/записи для повышения надежности хранения данных.

За счет применения технологии управления питанием восьмого поколения и такой технологии снижения энергопотребления, как Hitachi Voltage Efficiency Regulator (HiVERT™), жесткие диски Deskstar 7K2000 и 7K1000.C демонстрируют исключительные возможности управления питанием и низкий уровень тепловыделения. Например, в новом Deskstar 7K2000 уровень энергопотребления в режиме ожидания снижен на 10% по сравнению с накопителями предыдущих поколений, а показатель "ватт на гигабайт" улучшен на 120%. Предполагается, что новые Deskstar 7K1000.C будут иметь лучшие в своем классе показатели потребления энергии – не более 4,4 Вт в режиме ожидания.

Кроме соответствия стандартам RoHS (Restriction of Hazardous Substances) и низкого энергопотребления, все новые диски в линейках Deskstar 7K2000 и 7K1000.C произведены без использования галогена и относятся к категории Hitachi EcoTrac™.

EDS становится подразделением HP Enterprise Services

Сентябрь 2009 г. – Компания HP объявила о том, что входящая в ее состав компания EDS становится подразделением корпоративных услуг HP (HP Enterprise Services). Создание нового подразделения знаменует начало нового важного этапа в деле интеграции EDS в бизнес структуру HP и указывает на рост объема корпоративных технологических услуг в портфеле HP.

Группа технологических решений HP (HP Technology Solutions Group) будет переименована в Группу корпоративных решений HP (HP Enterprise Business). Тем самым делается акцент на том, что приобретение EDS расширило возможности HP. Группа корпоративных решений работает с коммерческими компаниями и государственными организациями любого уровня. Кроме корпоративных услуг, ее портфель включает серверы, системы хранения, программное обеспечение, сетевые устройства и технологические сервисы.

В 3 квартале 2009 финансового года выручка Группы корпоративных решений HP составила 47% от общих показателей компании, а операционный доход, рассчитанный в соответствии с необщепринятыми принципами бухгалтерского учета (non-GAAP), – 60%. Все бизнес-подразделения Группы корпоративных решений HP останутся подотчетными исполнительному вице-президенту HP Энн Ливермор.

Лидеры ИТ-услуг 2008 г.

Сентябрь 2009 г. – По данным исследования IDC Russia IT Services Competitive Analysis, ведущими поставщиками ИТ-услуг по итогам 2008 г. стали компании IBS, "Техносерв", "КРОК", "ЛАНИТ" и "КомпьюЛинк". Совокупная их доля в общем объеме рынка увеличилась по сравнению с прошлым годом и составила 29,9%.

Локальные поставщики ИТ-услуг попрежнему удерживают ведущие позиции – в десятке лидеров нет ни одной иностранной компании. Российские интеграторы имеют более тесные взаимоотношения с местными заказчиками, особенно в государственном секторе и в оборонной промышленности, и часто выступают в качестве генподрядчиков.

Paragon представляет виртуализацию

Сентябрь 2009 г. – Компания Paragon Software Group представила Virtuali-zation Manager – первый продукт компании на рынке средств виртуализации, который предлагает легкий и быстрый способ миграции ОС и данных в любую виртуальную среду от Microsoft и VMware в режиме реального времени – Live Migration! Новая концепция "живой миграции" предполагает обработку данных online, без остановки физической машины и прерывания работы приложений. В рамках данной концепции можно "на ходу" переносить любой образ системы с возможностью загрузки в новой среде, а корректный перенос и гарантия работоспособности ОС на новой платформе достигается за счет интеллектуального процесса внедрения дополнительных драйверов устройств в ходе миграции.

Решение создано на базе усовершенствованной технологии Paragon Adaptive Restore, которая впервые была использована в продуктовой линейке Drive Backup 9.0 и позволяла восстанавливать образ работоспособной системы на любое оборудование с различной аппаратной конфигурацией. Теперь данная технология была адаптирована и под работу с такими средами как: Microsoft Hyper-V/Virtual Server/ Virtual PC и VMware ESX Server/Fusion/Workstation.

Выход русифицированной коммерческой версии – конец октября 2009 г.

Решения Double-Take будут продвигаться в России

Сентябрь 2009 г. – Компания Double-Take Software, подписала соглашение с компанией Business Continuity International (BCI) о передаче прав на эксклюзивное продвижение и поддержку решений Double-Take на рынке СНГ. В России и других странах СНГ компания BCI будет, в том числе, являться единственным эксклюзивным поставщиком решений Double-Take. В Азиатско-Тихоокеанском регионе компания Business Continuity International уже более 7 лет является официальным представителем компания Double-Take Software.

Слева направо: **Сергей Бондарев** – генеральный директор Business Continuity International в России и СНГ; **Виктор Бабков** – представитель Double-take по развитию продукта в России и СНГ.

Решение о выходе продуктов Double-Take на российский рынок не случайно. С одной стороны, в последние несколько лет рынок ИТ-индустрии России бурно растет, и даже кризис незначительно повлиял на его развитие. Многие страховые, банковские, финансовые, а также государственные компании и ведомства уделяют большое внимание своей ИТ-инфраструктуре. При этом предпочтение отдается лицензионным программам, установка которых не только гарантирует надежность и качество, но и комплексное обслуживание систем. Оптимизация же в связи с кризисом бизнес-процессов компании увеличивает нагрузку на ИТ-инфраструктуру компаний и, соответственно, увеличивает требования к ПО. Подтверждением этого служит тот факт, что за последний год число обращений за лицензионными решениями Double-Take со стороны российских компаний увеличилось на 15%. Так, за последние полгода в общем объеме мировых продаж решений Double-Take продажи на территории России составляют порядка 0,3%.

Во всем мире решение по организации непрерывности бизнес процессов Double-Take используют более 19 тыс. компаний, в том числе международные банковские, финансовые и юридические компании, предприятия розничной торговли, обрабатывающей промышленности, сферы образования, здравоохранения и правительственные структуры. На сегодняшний день ПО Double-Take используют такие гиганты ИТ-индустрии, как Dell, IBM, и др. В 2008 году в мире доля продуктов Double-Take на рынке решений по организации непрерывности бизнес-процессов составляла 8%, лицензированных решений Double-Take было продано на сумму порядка 84 млн. долл.

По словам представителя Double-Take по развитию продукта в России и других странах СНГ Виктора Бабкова, "российский рынок нам уже хорошо знаком и у компании хорошие перспективы. Уже сейчас решениями Double-Take пользуется ряд российских компаний, таких как банк ВТБ, Deutsch Bank Россия, ЗАО "Объединенная финансовая группа", ЗАО "Панавто", Территориальный фонд Обязательного медицинского страхования Воронежской области и некоторые другие. В первый год мы планируем продать в России порядка 1200 лицензий, планируемый оборот должен составить около 5 млн. долл., и, в дальнейшем, используя благоприятную для нас конъюнктуру, а также наш мировой опыт по выходам на рынки других стран, мы планируем увеличить продажи на 40%. В качестве основного канала продаж решений Double-take мы рассматриваем системных интеграторов".

По оценкам компании Business Continuity International объем российского рынка решений по организации непрерывности бизнес-процессов составляет порядка 80 млн. долл. и ежегодно будет увеличиваться на 15%. Доля решений Double-Take на этом рынке может составить порядка 6%

Oracle+Sun=Exadada 2

Сентябрь 2009 г. – Компания Oracle объявила о доступности в продаже 2-й версии Exadata Database Machine – специализированного консолидированного хранилища данных как для BI- (Business Intelligence), так и для OLTP-приложений (online transaction processing). Решение построено на базе стандартных Sun-серверов с использованием FlashFire технологии и ПО от Oracle: Oracle Database 11g Release 2 и Oracle Exadata Storage Server Software Release 11.2.

Exadata Version 2 в сравнении с версией 1 имеет удвоенную производительность и доступна в 4 модификациях: полнорэковой (8 database-серверов и 14 storage-серверов), полурэковой (4 database-серверов и 7 storage-серверов), 1/4 стойки (2 database-сервера и 3 storage-сервера) и в базовой комплектации (1 database сервер и 1 storage сервер).

Среди других особенностей Exadata Version 2 ***(от Sun)***:

- на 80% более быстрые CPUs – Intel Xeon (Nehalem) процессоры;
- на 50% более быстрые диски – 600 Гбайт SAS-диски с интерфейсом 6 Gbit/sec;
- на 200% более быстрая память – DDR3;
- на 125% больше памяти – 72 Гбайт на database-сервер;
- на 100% более производительная сеть коммутации – 40 Gbit/sec InfiniBand;
- общая емкость (на рэк) хранимых данных – 100 Тбайт (SAS) или 336 Тбайт (SATA).

Среди особенностей Exadata Version 2 в сравнении с Exadata 1 ***(от Oracle)***:

- наличие опции Oracle 11g Release 2, поддерживающей flash-хранение БД;
- гибридное поколоночное сжатие данных – до 10-50 раз;
- возможность сканирования/поиска на сжатых данных для более быстрого выполнения запроса;
- введение storage-индексов для снижения интенсивности дисковых I/O-операций;
- уменьшение требуемой вычислительной мощности при обработке запроса за счет использования Smart Scans (включая и storage-серверы);
- достижение уровня производительности приложений при выполнении на Sun Oracle Database Machine в 1 млн операций ввода/вывода в секунду за счет Flash Storage.

Каскадная репликация для DR-инфраструктур

Сентябрь 2009 г. – Корпорация EMC анонсировала новые программные расширения для репликации данных для Data Domain inline deduplication СХД. Возможность каскадировать реплицируемые данные позволяет оптимизировать стратегию аварийного восстановления, используя высокоэффективную сетевую репликацию для передачи дедуплицированных и архивных данных на другие сайты. ПО Replicator позволяет поддерживать передачу данных со 180 удаленных сайтов на 1 контроллер для расширенной автоматизированной кроссайтовой дедупликации и на 100% повышенной производительностью, за счет использования высоко оптимизированного, многопотокового реплицирования.

Вместе эти функции формируют гибкое и масштабируемое решение для крупных организаций с географически распределенными офисами. Теперь появилась возможность за счет использования глобальных сетей с низкой пропускной способностью упростить и удешевить инфраструктуру аварийного восстановления данных и одновременно с этим повысить степень готовности организации к восстановлению данных в случае сбоев.

"Мы старались преодолеть множество трудностей, связанных с резервным копированием на магнитной ленте, быстрым ростом объемов данных и ограниченной пропускной способностью нашей сети. Нам требовалось надежное и масштабируемое решение для корпоративных систем, – говорит менеджер инфраструктуры министерства рыболовства и охоты Аляски Кори Кос. – Объединив системы хранения дедуплицированных данных Data Domain и программу репликации и развернув услуги по управлению инфраструктурой, мы получили более эффективное, надежное и недорогое решение

для резервного копирования и аварийного восстановления наших основных центров обработки данных в городах Джуно, Анкоридж, Кадьяк и Фэрбенкс".

"Особенно мы довольны результатами тестирования каскадной репликации для резервного копирования во внешних системах, которая работает быстро и эффективно и не требует внимания после настройки, – продолжает Кос. – В данный момент мы обеспечиваем защиту кластеров VMware, Microsoft 2008 Active Directory, а также баз данных SQL и Oracle. Наборы данных из центров обработки данных Фэрбенкса и Кадьяка копируются в Анкоридж и затем повторно копируются в наш основной центр в Джуно. Теперь мы можем быстро восстановить любой сайт министерства рыболовства и охоты Аляски из Джуно или Анкориджа".

"По результатам нашего исследования за 2009 год о корпоративных расходах, наиболее крупные корпоративные инвестиции в области хранения данных корпорации ожидаются в направлении систем репликации для защиты данных из внешних центров, – говорит старший аналитик Enterprise Strategy Group Брайан Бабино. – Совершенно ясно, что компании хотят отказаться от перевозки магнитных лент с резервными копиями как основного способа передачи данных между центрами и найти доступную альтернативу с использованием дисков. Решение EMC Data Domain предлагает доступное решение для создания точек аварийного восстановления, где данные хранятся на дисках во внешних центрах и передаются туда по сети с минимальными требованиями к ее пропускной способности. Благодаря разработке функции каскадной репликации и возможности принятия данных сразу со многих удаленных сайтов корпорации теперь могут внедрить еще больше приложений с минимальными затратами, независимо от места хранения данных".

Продукты EMC из семейства систем хранения данных с дедупликацией Data Domain легко интегрируются в большинство информационных сред, поддерживают основные приложения резервного копирования и архивации, а также многие типы сетей и протоколов. Сюда входят файловый сервер CIFS или NFS через Ethernet, библиотека VTL через Fibre Channel и интерфейс OpenStorage от Symantec Veritas NetBackup. ПО Data Domain Replicator уже поступила в продажу.

Павел Карнаух *(BURA-IP Business Development Manager, EMC Россия и СНГ)* на вопросы SN, связанные с последними анонсами решений с использованием технологий дедупликации, дал следующие ответы.

SN: Как изменится позиционирование продуктов EMC, в частности EMC Disk Library и EMC Avamar, после покупки DD и анонса новых систем DD880? Означает ли приобретение DD отказ от EMC Avamar?

П.К.: Разумеется, нет. Продукты EMC Data Domain приходят на смену системам EMC DL3D. Мы продолжаем развивать и дисковые библиотеки серии EDL 4x06 и решения EMC Avamar. Более того, до конца этого года будут анонсированы новые версии этих продуктов с расширенными функциональными возможностями.

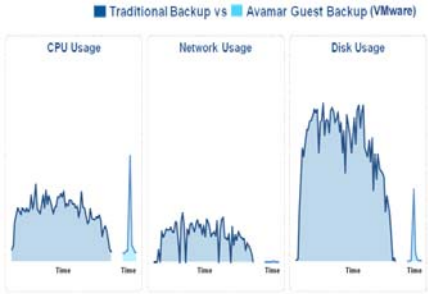
Мы позиционируем EMC Avamar как систему с дедупликацией на источнике, EMC Data Domain – как систему с дедупликацией на целевом устройстве. Соответственно, решения Avamar, прежде всего, предназначены для заказчиков, желающих минимизировать использование аппаратных ресурсов при резервном копировании виртуальных машин, удаленных офисов, серверов, подключенных к ЛВС и т.п.

Дисковые системы EMC Data Domain в наибольшей степени подходят заказчикам, которые не желают кардинально менять существующую систему резервного копирования, но при этом хотят повысить ее эффективность, надежность и быстродействие. Несмотря на то, что системы Data Domain осуществляют дедупликацию в реальном времени, их производительность (в частности, для недавно анонсированной модели DD880) одна из самых высоких и позволяет полностью использовать возможности высокоскоростных сетей Fibre Channel и 10GBE.

Мы ожидаем, что большинство наших заказчиков сделает выбор в пользу систем Data Domain. В тоже время тем из них, для кого важна максимальная производительность, будут по-прежнему интересны классические дисковые библиотеки EMC Disk Library.

SN: Какое влияние оказывают накладные затраты, связанные с дедупликацией, на работу приложений?

П.К.: Например, при сравнении EMC Avamar, выполняющегося как guest backup в среде VMware, с традиционным бэкапом загрузка больше, но много короче.



HDS: новая версия ПО для мониторинга ЦОД

Октябрь 2009 г. – Компания Hitachi Data Systems Corporation (дочернее предприятие Hitachi, Ltd.), объявила о выпуске Hitachi IT Operations Analyzer версии 1.2, комплексного ПО мониторинга систем хранения данных среднего уровня. Hitachi IT Operations Analyzer 1.2 оснащен адаптированным интерфейсом для прикладных продуктов (Application Product Interface, API), интеграцию с которым в настоящий момент поддерживают 6 независимых поставщиков ПО (ISV), и, кроме того, обеспечивает расширенную поддержку операционных систем, схем виртуализации и коммутаторов.

Программный пакет Hitachi IT Operations Analyzer, появившийся в апреле 2009 г. – продукт, рассчитанный на средний сегмент рынка, который позволяет осуществлять мониторинг и диагностику до 250 разнородных серверов, коммутаторов и узлов систем хранения данных в центре обработки данных с помощью единого унифицированного интерфейса. Этот программный пакет предлагает простые в использовании, комплексные инструменты мониторинга, позволяющие оптимизировать работу ИТ-отделов и улучшить качество обслуживания клиентов при одновременном снижении совокупной стоимости владения. ПО Hitachi IT Operations Analyzer 1.2 оснащено мощным интерфейсом API, который в настоящее время интегрируется с продуктами DeepNines Technologies, Lumeta, Netcordia и Sentrigo, Inc. Hitachi IT Operations Analyzer 1.2 позволяет расширить перечень операционных систем, для которых возможен мониторинг – теперь, помимо ранее поддерживаемых Microsoft Windows и Red Hat Linux, система поддерживает еще и ОС Solaris от Sun Microsystems.

"Меньше чем за год наше решение IT Operations Analyzer вызвало огромный интерес у сообщества независимых поставщиков программного обеспечения, особенно в условиях роста продаж этого продукта и увеличения спроса на комплексные, удобные в использовании решения для мониторинга инфраструктур, включающих в себя мультиплатформенные серверы, сетевые устройства и системы хранения данных от различных производителей, – говорит Шон Моузер (Sean Moser), вице-президент по управлению программными продуктами Hitachi Data Systems. – Новая версия программного пакета предлагает еще более широкий спектр функций для центров обработки данных, причем для его использования администраторам ИТ не требуется каких-либо дополнительных специальных знаний. Это решение способствует быстрому устранению проблем и обеспечивает снижение совокупной стоимости владения".

Помимо прочего, новая версия Hitachi IT Operations Analyzer 1.2 включает в себя поддержку мониторинга платформ NetApp FAS, Cisco FC и Juniper EX-Series, а также расширенные возможности виртуализации VMware благодаря поддержке VMware ESXi. Новая версия ПО поддерживает следующие дополнительные возможности:

- автоматизированный анализ причины проблем (причинно-следственный анализ): помогает быстро восстанавливать работоспособность после сбоев и способствует сокращению простоев;
- безагентная архитектура избавляет от необходимости устанавливать программные агенты мониторинга на все устройства центра обработки данных;
- одновременное управление мониторингом всех ИТ-компонентов посредством единого унифицированного интерфейса.

Виртуализация и безопасность

Публикация – обзор возможных угроз с точки зрения информационной безопасности в ИТ-среде на базе серверной виртуализации и методов борьбы с ними.

Алексей Чеканов – генеральный директор, компания Almitech

Введение

Виртуализация в последние годы является, пожалуй, самым перспективным направлением развития информационных технологий, и большинство организаций уже используют ее для решения своих задач. При этом, задавая вопрос "а насколько безопасна виртуальная инфраструктура", можно получить самый широкий спектр ответов. Производители заявляют, что решения виртуализации обеспечивают более высокий уровень безопасности, чем их "железные" аналоги, а наиболее скептически настроенные пользователи, напротив, пока не готовы доверить решениям по виртуализации свои критические данные. Истина, как водится, находится где-то посередине. Т.е. безопасность обеспечить можно, но как – до конца еще непонятно.

В этой статье мы попробуем на нескольких наиболее ярких примерах, связанных с серверной виртуализацией, разобраться, что же появилось принципиально нового с точки зрения безопасности и как с этими угрозами можно бороться.

Новые угрозы

Атаки на гипервизор

Ключевой элемент архитектуры сред виртуализации, который отсутствует в традиционных серверных инфраструктурах, – гипервизор. Учитывая практически неограниченные возможности, которые может получить злоумышленник, получив контроль над гипервизором, логично предположить, что именно к нему будет приковано внимание хакеров. Если посмотреть на доклады на конференциях типа Black Hat, какое-то время назад возможность скомпрометировать гипервизор обсуждалось крайне активно, однако потом эта тема практически сошла на нет.

И, действительно, несмотря на серьезные последствия в случае осуществления такой угрозы, на другой чаше весов оказалось слишком много аргументов, среди которых – пристальное внимание производителей ПО виртуализации к данной проблеме, оперативное устранение обнаруженных уязвимостей, и, наконец, ограниченное пространство для поиска уязвимостей в силу относительно небольшого размера кода гипервизора.

В результате, применением классических мер безопасности, таких как оперативная установка обновлений, жесткий контроль доступа к гипервизору и к среде управления, контроль целостности, вероятность этой угрозы удалось понизить до вполне приемлемых величин. По-крайней мере, на сегодняшний день еще не приходилось слышать о сколь-нибудь масштабных проблемах в реальных информационных системах, связанных с компрометацией гипервизора.

Аналогичная ситуация наблюдается и со средой управления виртуальной инфраструктурой – наличие механизмов контроля доступа и действий администраторов позволяет минимизировать данный риск.

Плохо управляемый парк виртуальных машин

Часто приходиться слышать, что серьезной угрозой безопасности, возникающей при использовании технологии виртуализации, является неконтролируемое разрастание парка виртуальных машин (ВМ). Если для физических машин есть серьезное препятствие в виде стоимости приобретения нового сервера, то для виртуальной среды создание или копирование виртуальной машины может быть выполнено за несколько кликов мыши. Действительно, это так, но при одном условии – если у администраторов есть возможность бесконтрольно выполнять подобного рода действия.

Решается данная проблема достаточно эффективно сочетанием двух мер: четкими регламентами, описывающими жизненный цикл машин – от момента создания до момента вывода из эксплуатации, и использованием специализированных решений, позволяющих контролировать действия администраторов.

Было бы, по меньшей мере, неразумно отказываться от возможностей, предлагаемых новыми технологиями, но важно с самого начала выстроить четкие процессы управления.

Сетевая безопасность

Задача обеспечения сетевой безопасности в среде виртуализации несколько отличается от той же задачи в инфраструктуре физической, в основном по причинам:

- невозможности применять уже привычные средства обеспечения сетевой безопасности (межсетевые экраны, системы предотвращения вторжений) в том виде, в котором они существуют;
- высокой динамики среды, связанной с перемещением виртуальных машин.

Тем не менее, и эта угроза уже не так страшна. Начиная с этого года, базовые средства обеспечения сетевой безопасности внутри виртуальной инфраструктуры появились в решении VMware, а продукты третьих фирм, об одном из которых пойдет речь далее в статье, достигли уровня зрелости, сопоставимого с их аналогами из мира "физического".

Безопасность СХД, используемых ВМ

Поскольку ВМ представляет собой совокупность файлов, возникает риск того, что эти файлы могут быть скопированы либо подменены. Угроза действительно реальная, причем риск модификации ВМ представляет, пожалуй, большую угрозу, чем просто копирование самой ВМ. По той простой причине, что чаще всего в серьезных промышленных решениях данные отделены от серверов их обрабатывающих, а вот модифицированный сервер может выполнять любую вредоносную нагрузку.

Впрочем, меры противодействия данному риску не отличаются особенной сложностью. За редкими исключениями, в продуктивных системах файлы виртуальных машин хранятся на внешних, по отношению к серверам, системам хранения данных. Соответственно, задача обеспечения безопасности во многом решается ограничением на уровне СХД

доступа к файлам виртуальных машин только со стороны серверов виртуальной инфраструктуры. Протоколирование таких действий, как клонирование виртуальных машин, резервное копирование и т.п., позволяет контролировать администраторов, а правильное определение ролей позволяет минимизировать число администраторов, которым доступны подобные действия.

Параллельно с контролем доступа к СХД необходимо также обеспечить комплекс мер по защите резервных копий виртуальных машин, что, впрочем, так же важно и для резервных копий обыкновенных серверов.

Атаки на виртуальные машины

Сравнивая уязвимость самих виртуальных машин, видим, что они подвержены абсолютно тем же атакам, что и машины физические, что, впрочем, абсолютно естественно, ведь концепция виртуализации и заключается в том, чтобы быть прозрачной для самих виртуальных машин. Единственная особенность, пожалуй, заключается в том, что виртуальная машина может долгое время пребывать в оффлайне, что приводит к тому, что последние обновления и базы данных антивирусов могут оказаться неустановленными на эту машину. Но тут нам на помощь приходят новые технологии, предоставляемые средствами виртуализации.

Новые возможности

Security API

В этой области VMware выступила ярким лидером, представив сообществу своих партнеров технологию VMsafe. Технология VMsafe позволяет без установки агентов внутрь виртуальных машин осуществлять контроль всех составляющих виртуальной инфраструктуры: памяти, дисков, сетевого взаимодействия и т.п. VMsafe позволяет работать даже с машинами, находящимися в выключенном состоянии, например, осуществлять их антивирусное сканирование. Интеграция с технологией перемещения виртуальных машин vMotion позволяет применять при перемещении машины в новое окружение (например, из ЦОД организации в ЦОД сервис-провайдера, или, используя "облачную" терминологию, из внутреннего облака во внешнее) новые политики информационной безопасности.

Этот шаг позволил VMware, не проходя самостоятельно путь по созданию полноценного набора средств обеспечения информационной безопасности, дать лидерам рынка решений ИБ доступ к своему гипервизору, обеспечивая контроль за действиями виртуальных машин на самом низком уровне, и в результате поддержать должный уровень защиты инфраструктуры.

Новые решения

Чтобы воплотить сказанное выше в конкретные решения, которые могут быть использованы на практике, в этом разделе вкратце рассмотрим два продукта, победившие в категории "Безопасность и виртуализация" на VMworld в 2008 и 2009 г.

Reflex VMC

С тех пор, как решение Reflex VMC получило две награды на VMworld 2008, произошло немало изменений – вышла новая версия, решение было первым сертифицировано VMware на использование технологии VMsafe, получило еще два приза от Red Herring и Network Products Guide.

Итак, какие возможности предоставляет продукт сегодня? Reflex VMC позиционируется, как комплексное решение по управлению и обеспечению безопасности в средах виртуализации. Не претендуя на замену встроенных инструментов управления, Reflex VMC существенно расширяет их возможности.

Основные функции Reflex VMC:

- *обеспечение сетевой безопасности внутри сетевой инфраструктуры.*

  Помимо функциональности межсетевого экрана и системы предотвращения вторжений, Reflex VMC предоставляет гибкий механизм динамического формирования так называемых "зон доверия", для которых позволяет определять политики безопасности;

- *контроль соответствия (compliance).*

  Определяя политики соответствия для индивидуальных виртуальных машин, или зон доверия, Reflex VMC контролирует их выполнение, и, в случае нарушения, позволяет предпринимать корректирующее воздействие (например, блокировать сетевое взаимодействие виртуальной машины), или просто информировать заданный круг лиц;

- *мониторинг основных параметров.*

  Протоколируя все изменения среды, Reflex VMC позволяет администратору получить целостную картину конфигурации по состоянию на любой момент времени, а возможности корреляции событий позволяют оценить влияние изменений конфигурации на работу систем.

Версия Reflex VMC для сервис-провайдеров позволяет обеспечивать необходимый уровень безопасности и для "облачных" технологий, когда при миграции виртуальных машин из ЦОДа заказчика в ЦОД сервис-провайдера, вместе с ними мигрируют (или даже применяются более жесткие) политики обеспечения безопасности.

Пожалуй, на сегодняшний день Reflex VMC является наиболее комплексным решением по обеспечению безопасности внутри виртуальной инфраструктуры.

HyTrust

Призером VMworld 2009 г. стала компания HyTrust, предложившая решение, ориентированное на контроль действий администраторов виртуальной инфраструктуры. Как уже говорилось выше, значительное количество угроз безопасности виртуальной инфраструктуры может быть нейтрализовано на уровне регламентов и ограничения прав доступа к управляющей инфраструктуре. Именно для решения этой задачи и предназначено решение HyTrust.

HyTrust Appliance перехватывает взаимодействие по всем каналам управления виртуальной инфраструктурой: доступ к Virtual Center, прямой доступ к серверам ESX, и т.п. и ограничивает действия администратора в строгом соответствии с определенными политиками безопасности. При этом, все действия администраторов протоколируются с детализацией, достаточной, как для проведения расследования инцидентов.

Еще одной особенностью HyTrust Appliance является возможность проверки конфигурации гипервизора в соответствии с рекомендациями производителя, требованиями отраслевых (например, PCI DSS) и корпоративных стандартов и устранения несоответствий одним щелчком мыши.

Если решение Reflex VMC сфокусировано на контроле и управлении действиями самих виртуальных машин, то HyTrust отлично дополняет его в части контроля соблюдения корпоративных политик безопасности в области контроля конфигураций и действий администраторов.

Заключение

Подводя итоги, можно сказать, что задача обеспечения требуемого уровня информационной безопасности в средах виртуализации уже вполне реализуема. Да, это не простой процесс, который потребует разработки внутренних стандартов и политик, внедрения новых регламентов, выбора и внедрения подходящих решений. Зато в конце пути вы сможете получать все преимущества от технологии виртуализации, не подвергая риску свою информацию.

Алексей Чеканов,
компания Almitech

Расширение функциональности Cisco MDS9000

Август 2009 г. – Компания Cisco анонсировала дополнительную функциональность для своего семейства MDS9000: Multilayer Directors – 9506, 9513, 9509 и Multilayer Fabric Switch – 9216. Новые возможности повышают уровень безопасности и ускоряют передачу данных на большие расстояния для сред хранения с мэйнфреймами IBM System z и на основе открытых систем.

Технологические расширения для семейства многоуровневых директоров Cisco MDS 9000:

- *более быстрая передача данных на расстояние – Cisco XRC Acceleration.*

  Разработанное совместно с IBM и предназначенное для использования с системой IBM z/OS Global Mirror, решение Cisco XRC Acceleration ускоряет передачу данных на большие расстояния через глобальную сеть (WAN), снижает нагрузку на канал передачи данных и сокращает время, необходимое для обновлений;

- *защита данных, передаваемых за пределы центра обработки данных – Cisco TrustSec Fibre Channel Link Encryption.*

Данная система представляет собой аппаратное решение, которое может быть задействовано индивидуально на любом порту без какого-либо снижения производительности. Это позволяет заказчикам шифровать данные, передаваемые за пределы их ЦОД через городские сети (например, данные, передаваемые между центрами обработки данных). При особых требованиях к безопасности, эту технологию можно применять внутри ЦОД. При этом весь трафик между коммутаторами будет шифроваться. Данные могут шифроваться как для систем FICON (IBM Fibre Connectivity), так и для открытых систем;

– *повышение скорости резервного копирования и аварийного восстановления – Cisco I/O Acceleration (IOA).*

Cisco MDS 9000 I/O Acceleration – приложение сетей хранения данных, предлагающее экономичные, более быстрые и гибкие решения для резервного копирования данных и аварийного восстановления. Службу IOA можно использовать для дисковых или ленточных систем хранения с любым транспортным протоколом (FC или FCIP), независимо от местонахождения устройства (с прямым подключением, через WAN или через MAN);

– *управление крупномасштабными сетями хранения данных – Cisco SAN Fabric Manager.*

Улучшенные характеристики диспетчера Cisco SAN Fabric Manager позволяют значительно увеличить число устройств, управляемых с помощью Fabric Manager. Теперь каждый сервер Fabric Manager обладает емкостью в 15.000 устройств, причем до 10 серверов можно объединить для получения отчетов, что позволяет более эффективно управлять средами крупных хранилищ.

IBM: расширенные возможности аварийного восстановления информации на основе устранения дубликатов данных

Август 2009 г. – Корпорация IBM анонсировала ключевое расширение своего решения для дедупликации данных. Новый функционал даст возможность значительно улучшить показатель непрерывности бизнеса, позволяя компаниям быстро восстанавливать операционную активность в случае аварийных ситуаций.

IBM добавляет возможности электронной передачи данных, или собственной репликации (native replication – встроенного механизма дублирования данных) в продуктовую линейку ProtecTIER Deduplication, повышая эффективность защиты корпоративных данных и улучшая показатель непрерывности бизнеса. Осуществляется это путем электронной передачи данных с устраненными дубликатами на удаленные серверы, что позволяет значительно снизить требования к пропускной способности сетевого канала и избежать необходимости физической перевозки и хранения ленточных носителей с резервными копиями в удаленных офисах.

Механизм репликации десятилетиями использовался для обеспечения удаленной защиты важных данных, однако из-за больших издержек, связанных с применением широкополосных сетей и высокой стоимостью системы хранения для поддержки оперативного доступа к данным, репликация применялась, как правило, для защиты наиболее критичных для бизнеса приложений и данных. Новое решение уменьшит проблему высоких затрат на широкополосные каналы, давая возможность осуществлять репликацию больших объемов данных при меньших издержках по сравнению с традиционными подходами. При использовании запатентованной технологии редупликации ProtecTIER лишь небольшие пакеты уникальных данных посылаются по сети в любой момент времени, что, в конечном итоге, позволяет передавать большой объем данных с минимальной пропускной способностью канала, расширяя спектр корпоративных приложений с поддержкой репликации.

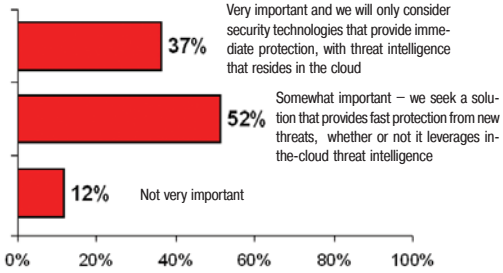
В 2005 году технология ProtecTIER помогла изменить подход организаций к защите данных благодаря выпуску первой на рынке "виртуальной ленточной библиотеки" Virtual Tape Library (VTL) с функцией удаления дублирующихся данных. Сегодня подавляющее большинство VTL-систем обладают той или иной формой дедупликации – удаления дубликатов данных. Ожидается, что функция редупликации – резервного тиражирования данных – в течение ближайших 5 лет будет повсеместно применяться в центрах обработки данных по всему миру.

Ранее в этом году IBM анонсировала продукт TS7650 ProtecTIER Deduplication Appliance, интегрированное устройство, включающее сервер, систему хранения данных и ПО для дедупликации данных, которое устраняет избыточные данные и позволяет клиентам сохранять данные дольше, защищать данные более эффективно и надежно, и экономить деньги благодаря снижению энергопотребления, сокращению арендуемых площадей помещений и упрощению требований к техническому обслуживанию.

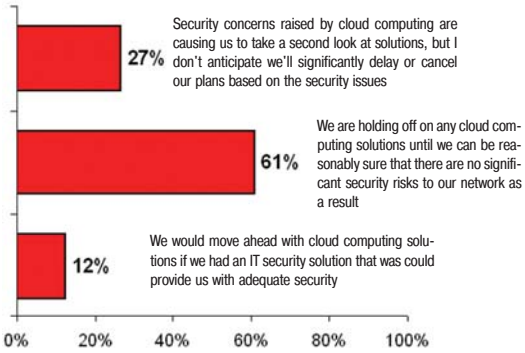
Функция собственной репликации (Native Replication) доступна с 4 сентября, в виде дополнительной опции. Обновление программного обеспечения доступно для всех существующих конфигураций TS7650G ProtecTIER Deduplication Gateway и TS7650 ProtecTIER Deduplication Appliance.

Компании интересуются облачными вычислениями, но не решаются их внедрять из-за неуверенности в ИБ своих данных

Сентябрь 2009 г. – Недавний опрос Trend Micro, проведенный среди примерно 200 ИТ-менеджеров и директоров, не входящих в число клиентов Trend Micro, показал, что 9 из 10 респондентов (89%) ищут такое решение для защиты своей информационной системы, которое было бы построено на облачной архитектуре. Для некоторых такая опция не является важным критерием при выборе того или иного решения. Почти 40% респондентов готовы рассматривать только решения по безопасности, которые построены на облачной архитектуре (например, система Trend Micro Enterprise Security создана на базе клиентской инфраструктуры Trend Micro Smart Protection Network).



Существующая система безопасности или ее отсутствие могут повлиять на решение о системе облачных вычислений в ту или иную пользу. Согласно опросу, 61% респондентов заявили, что они откладывают решение относительно облачных вычислений до момента, пока не получат полную уверенность, что это не повлечет за собой рисков для безопасности их сетей. 27% заявили, что вопросы безопасности могут побудить их пересмотреть свою позицию, а выгода от облачных вычислений превышает риски безопасности и не повлияет на решение внедрить такой продукт.



Компания Trend Micro разработала совершенно новый подход к обеспечению безопасности как самих облачных инфраструктур, так и их содержимого – систему Trend Micro Enterprise Security, который представляет собой комплекс тесно взаимосвязанных продуктов, услуг и решений, созданный на базе инфраструктуры Trend Micro Smart Protection Network. Вместе они обеспечивают мгновенную защиту от новых угроз, отличаясь при этом низкой стоимостью и простотой управления.

Недавно был создан блог Trend Cloud Security Blog *(http://cloudsecurity.trendmicro.com)*, посвященный обсуждению вопросов безопасности в облачных инфраструктурах. Среди его главных участников – генеральный директор Ева Чэн и технический директор Раймунд Генес. Они обратятся к вопросам, связанным с безопасностью инфраструктуры, и дадут рекомендации по организации защиты как самой облачной инфраструктуры, так и ее содержимого.