Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Решения Symantec по хранению и защите данных

№ 04 (225)/2012
www.jetinfo.ru

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:

Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Шедова Е.Л.

Шкляева А.Л.
ashklyaeva@jet.msk.su

Верстка:
Кулешова Ю.В.

Корректура:
Макеева Е.И.

Над номером работали:
Быков А.В.
Котенко А.С.
Прахов М.В.
Семенюков Ю.А.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
http://www.jetinfo.ru

От редакции

Елена Шедова,
директор по маркетингу
компании
«Инфосистемы Джет»

Хранение, архивирование, резервное копирование — три кита, на которых держится современный бизнес в части обращения с данными. При этом требования к этим процессам ужесточаются год от года. Так, сегодня бизнес-приложения в подавляющем большинстве работают 24 часа в сутки — таковы условия для победы в конкурентной борьбе. И от всех видов работы с данными требуется умение соответствовать режиму 24/7. В то же время по мере увеличения объемов данных в корпоративных системах традиционные подходы, например, к резервному копированию, становятся все менее эффективными. Рынок требует новых, интегрированных решений. Так, исследования независимых аналитических агентств констатируют, что параллельно со спросом на ленточные библиотеки растет востребованность дисковых устройств. Их доступность и высокая скорость работы становятся для многих компаний решающим фактором выбора.

В этом номере мы представим свой взгляд на оптимальные с точки зрения современных реалий ИТ-рынка решения для хранения, резервирования и архивирования данных. На этот раз речь пойдет о «голубых фишках» в портфеле продуктов компании Symantec: Enterprise Vault, NetBackup, Storage Foundation и др. За 15 лет сотрудничества с Veritas/Symantec нами были реализованы десятки проектов с использованием этих решений — от маленьких до крупнейших в СНГ. Полученный опыт доказывает, что возможности продуктов вендора позволяют организовать управление хранением данных для компаний любого масштаба.

СОДЕРЖАНИЕ

Новости 5

Статистика 9

Тема номера

Сохранить и не преумножить

(Александр Котенко, старший инженер-проектировщик систем хранения данных гр. систем хранения данных компании «Инфосистемы Джет») 10

Явные резервы

(Алексей Быков, ведущий инженер-проектировщик систем хранения данных компании «Инфосистемы Джет») 17

Единство виртуального и физического. Теперь – без компромиссов

(Максим Прахов, менеджер по работе с партнерами компании Symantec) 21

Интеллектуальное хранение

(Юрий Семенюков, старший инженер-проектировщик Отдела проектирования вычислительных комплексов компании «Инфосистемы Джет») 26

Наши проекты

Консолидированная вычислительная платформа банка КРЕДИ АГРИКОЛЬ 32

Система централизованного управления учетными данными для «ОТП Банка»

Завершен первый этап проекта по внедрению системы централизованного управления учетными данными на базе технологии Oracle Identity Manager. Новая система позволила повысить эффективность процессов управления и контроля доступа пользователей в ключевых информационных системах банка. Внедрение охватило все отделения банка на территории Украины.

«ОТП Банк» является одним из лидеров в области оказания финансовых услуг на Украине. Банк предлагает своим клиентам самые современные банковские продукты и услуги: электронные платежные системы, дистанционное банковское обслуживание, продукты «Cash Management». Все приоритетные бизнес-процессы банка оптимизированы и четко выстроены. Такая бизнес-модель требует соответствующего уровня зрелости ИТ-процессов. Внедрение IdM-системы стало логическим продолжением общих тенденций оптимизации и повышения уровня информационной безопасности в банке в целом.

В качестве партнера для реализации проекта была выбрана компания «Инфосистемы Джет», обладающая необходимыми компетенциями по построению решений для управления ИТ-привилегиями пользователей как части корпоративной системы информационной безопасности. Специалисты системного интегратора провели обследование ИТ-инфраструктуры банка и процессов предоставления доступа, в результате чего были сформулированы требования к системе, которые затем были успешно реализованы в ходе выполнения проекта на основе Oracle Identity Manager.

В ходе 1-го этапа проекта в головном офисе банка была развернута инфраструктура Oracle Identity Manager и произведена интеграция решения с основными ИТ-системами заказчика. В качестве первоочередной задачи была осуществлена интеграция решения Oracle с кадровой системой SAP HR, расположенной в головном офисе материнского банка, в Венгрии. Подключение HR-системы было выполнено специалистами компании «Инфосистемы Джет» с помощью коннектора посредством web-сервисов. Это позволило обеспечить загрузку информации о сотрудниках и штатной структуре в Oracle Identity Manager. На основании данных из HR-системы средствами решения Oracle было обеспечено управление правами доступа в основных информационных системах банка. Особенностями проекта стали реализация сервиса самообслуживания пользователей в части управления паролями и автоматизация синхронизации штатной структуры с группами Active Directory.

«Для нас внедрение Oracle Identity Manager стало фундаментом для обеспечения требований безопасности процессов управления полномочиями пользователей и позволило приступить к приведению их в соответствие с установленными правилами и стандартами. Помимо этого, новая система обеспечивает единый унифицированный механизм управления доступом пользователей в информационных системах, который позволил повысить уровень автоматизации процессов управления полномочиями пользователей и предоставил возможность управления правами посредством бизнес-ролей, что существенно повышает оперативность выдачи полномочий и обеспечивает их соответствие позиции сотрудника. В дополнение портал самообслуживания предоставляет бизнес-пользователям удобный инструмент управле-

ния учетными данными, что позволило сократить количество обращений в службу поддержки пользователей», — комментирует **Сергей Васько, руководитель офиса управления проектами «ОТП Банка».**

Банк планирует провести реинжиниринг существующих процессов управления полномочиями пользователей, а также тиражировать решение на все остальные информационные системы и процессы, связанные с управлением доступом пользователей к ИТ-ресурсам.

«Мы создали систему управления процессами предоставления доступа, которая используется практически всеми сотрудниками банка, и каждый, как и банк в целом, получает от этого свои очевидные преимущества, — подчеркивает **Алексей Лаврухин, руководитель направления IdM-решений компании «Инфосистемы Джет»**. — *Внедрение IdM-системы позволило не только привести ИТ-процессы банка в соответствие с самыми высокими требованиями по обеспечению информационной безопасности, но и повысило удобство работы с ИТ-системами. Зрелость бизнес-процессов «ОТП Банка» и по-настоящему командная работа способствовали завершению проекта в короткие сроки».*

«Создание IdM-системы имеет принципиальное значение для современного банка, — отмечает **Константин Новиков, Директор по продажам OracleFusion-Middleware, Oracle СНГ**. — *Мы рады поздравить «ОТП Банк» с успешным завершением проекта. Наши решения позволили централизовать и автоматизировать процессы управления и контроля доступа пользователей в ключевых информационных системах, что дает банку дополнительные преимущества, на первом месте среди которых — соблюдение законодательных требований в области информационной безопасности».*

Банк «Санкт-Петербург» контролирует доступ в интернет

Банк «Санкт-Петербург» и компания «Инфосистемы Джет» завершили проект по созданию системы контроля доступа в интернет. Система построена на базе решений Blue Coat и позволяет Банку ускорить все бизнес-процессы, связанные с доступом в сеть, упорядочить и контролировать на более высоком уровне этот доступ в режиме реального времени, а также значительно снизить риски, связанные с утечками информации, вирусными атаками и влиянием вредоносного программного обеспечения.

«Банк «Санкт-Петербург» на сегодняшний день — один из крупнейших региональных российских банков. Одним из критериев соответствия статусу Банка, входящего в рейтинг Топ-20, является высокий уровень информационной безопасности (как сотрудников Банка, так и его клиентов). Инициация проекта по обеспечению безопасности работы сотрудников Банка в интернете стала закономерным стратегическим шагом по обеспечению комплексной ИБ

в Банке», — комментирует **ИТ-Директор Банка «Санкт-Петербург» Ярослав Шелин**.

Проект длился 3 месяца. За это время совместная проектная команда специалистов Банка и экспертов компании «Инфосистемы Джет» провела аудит инфраструктуры Банка. Также были разработаны правила использования интернет-ресурсов, модернизирован интернет-шлюз, разработаны политики доступа в сеть и развернута система контроля доступа к ресурсам сети, базирующаяся на технологии Blue Coat.

Решение оптимально соответствует требованиям Банка и предоставляет ему широкие возможности для категоризации доступа к сайтам (блокирует или разрешает доступ), защиты от вирусов. Доступ пользователей в интернет соответствует принятым в Банке политикам, а в случае необходимости может производиться анализ SSL-трафика. Это позволяет значительно снизить нагрузки на интернет-канал, осуществлять протоколирование действий сотрудников Банка при доступе в интернет, для защиты интернет-трафика от вирусов, вредоносного кода и иных веб-угроз. Кроме этого, внедренная система позволяет принимать взвешенные управленческие решения на основании регулярно формируемых системой отчетов.

«Мы видим своей первостепенной задачей обеспечение эф-

фективной защиты банковской информации на каждом участке работы Банка и прежде всего данных наших клиентов», —

комментирует **Анатолий Скородумов, Начальник отдела информационной безопасности Банка «Санкт-Петербург».** — Внедренная система контроля доступа в интернет соответствует нашим требованиям в части гибкости, отказоустойчивости и безопасности. Это, безусловно, положительно отражается на эффективности работы сотрудников Банка и нашей деятельности в целом, а значит, на качестве предоставляемых нашим клиентам сервисов и позициях Банка в рейтингах».

«Компания «Инфосистемы Джет» обладает значительным опытом работы в банковском секторе в целом и в решении задач подобного класса в частнос-

ти, — комментирует **Кирилл Викторов, Заместитель Директора по развитию бизнеса компании «Инфосистемы Джет».** — Работая над проектом, мы действовали в рамках общей ИТ-стратегии Банка. Этот проект стал планомерным стратегическим шагом в развитии системы информационной безопасности Банка. Заказчик предъявлял высокие требования к разрабатываемой нами системе, и нам удалось им соответствовать на каждом этапе проекта».

NIKOIL | BANK предотвращает незаконные банковские операции с помощью решения компании «Инфосистемы Джет»

NIKOIL | BANK запустил в промышленную эксплуатацию AML-систему, предназначенную для противодействия легализации преступных доходов. Система AzAML, разработанная компанией «Инфосистемы Джет», отвечает новым требованиям законодательства Республики Азербайджан и соответствует международным стандартам банковской деятельности.

В 2010 году Правительством Республики Азербайджан был разработан комплекс мер, направленных на повышение эффективности борьбы с незаконными финансовыми операциями. NIKOIL | BANK одним из первых банков в Азербайджане начал реализовывать новые требования и поставил перед собой цель внедрить AML-систему как средство противодействия легализации преступных доходов. В качестве решения была выбрана система AzAML — уникальная разработка компании «Инфосистемы Джет» для банковского сектора Азербайджана.

Эксперты интегратора проанализировали функциональные требования банка к системе. Для доработки AzAML была развернута тестовая среда. Учитывая требования максимальной гибкости, специалисты компании «Инфосистемы Джет» реализовывали возможность настраивать решение в соответствии с текущими бизнес-задачами заказчика. Поскольку AzAML должна была получать данные о клиентах и проводимых ими операциях из автоматизированной банковской системы (АБС) банка, параллельно шли работы по интеграции AzAML с АБС. По окончании интеграции эксперты системного интегратора совместно с командой NIKOIL | BANK-а провели финальное тестирование внедряемой системы. AzAML была запущена в промышленную эксплуатацию в декабре 2011 года.

«На начальных этапах проекта большая часть работ по внедрению системы проводилась удаленно, из московского офиса нашей компании. Со временем к проекту были подключены и специалисты азербайджанского филиала. В перспективе это даст возможность быстрого реагирования на изменения в законодательстве и своевременного внесения необходимых доработок в рамках сопровожде-

ния системы», — отмечает **Евгений Бреннейсен, коммерческий директор филиала компании «Инфосистемы Джет» в Азербайджане**.

Система состоит из нескольких модулей: анкеты клиента, анализа операций, документооборота, отчетности, аналитической отчетности и модуля администрирования. Анкета клиента содержит информацию о клиентах банка, периодически получаемую из АБС или из других внешних источников. При необходимости анкеты могут быть изменены — данные, содержащиеся в них, удалены или обновлены. AzAML предусматривает возможность определения и ведения группы риска для каждого клиента. В системе так-

же реализована проверка клиентов на присутствие в «черных» и «серых списках» банка. При этом система позволяет банку вести собственный «черный список», а также загружать списки таких международных организаций, как ООН и OFAC. Модуль реализует принцип KYC — Know Your Customer, являющийся частью международных AML-стандартов.

Эмин Мамедов, Директор Департамента информационных технологий NIKOIL | BANK-a, подчеркивает: «*Внедрение подобной системы проводилось впервые в Азербайджане. Естественно, нам пришлось столкнуться с определенными трудностями. Однако благодаря слаженной работе сотрудников нашего банка и специалистов компании «Инфосистемы Джет» нам удалось первыми в стране внедрить программное обеспечение, предназначенное для противодействия легализации преступных доходов, интегрировав его в автоматизированную систему банка».*

AzAML выявляет подозрительные банковские операции с помощью набора сценариев (скриптов), представляющих собой механизмы для анализа операций и определения заданных типов поведения клиента. Все сценарии были выполнены в соответствии с требованиями законодательства Азербайджанской Республики. Каждая выполняемая банковская операция в режиме реального времени проверяется на соответствие списку скриптов. При выявлении подозрительной операции или операции, подлежащей обязательному контролю, AzAML автоматически создает дело для дальнейшего анализа ситуации ответственными сотрудниками банка. Для работы с делами в системе предусмотрен механизм документооборота. Таким образом, система AzAML позволяет фиксировать весь ход расследования операции, на каждом его этапе делу можно присваивать определенный статус.

«Данный проект позволил нам эффективно решить сразу несколько бизнес-задач. Кроме приведения в соответствие с требованиями регуляторов, была значительно оптимизирована работа специалистов банка: ручной труд заменили автоматические средства мониторинга. Как следствие, мы минимизировали операционные риски. AzAML практически полностью соответствует нашим потребностям», — прокомментировал запуск проекта **Фуад Тагиев, Заместитель Председателя Правления NIKOIL | BANK-a**.

Обновленные облака от IBM

Корпорация IBM представила новые программные решения из портфеля IBM SmartCloud Foundation, призванные оптимизировать прозрачность, автоматизацию и контроль функционирования облачных и физических сред.

Продукты позволяют компаниям устанавливать, управлять и настраивать сервисы облачных вычислений в частных, общедоступных или гибридных cloud-средах с высоким уровнем контроля. Объединенные возможности этих решений помогут клиентам ускорить поставку, снизить риски и лучше контролировать процесс развертывания cloud-сервисов, а также существующих операционных сред.

Корпорация будет предоставлять новые возможности в рамках своего портфеля IBM SmartCloud Continuous Delivery. Новое ПО представляет собой пакет передовых практических методик для интегрированного управления жизненным циклом сервисов облачных вычислений, объединяющий в своем составе решения Rational Collaborative Lifecycle Management и IBM SmartCloud Provisioning. Недавнее приобретение IBM компании Green Hat дополнительно расширяет функционал пакета: циклы разработки сокращаются за счет оптимизации стадии тестирования, поскольку приложения переводятся для развертывания в cloud-среды.

Сохранять и властвовать

Доля России на мировом рынке систем хранения данных (СХД) скромна, однако темпы роста этого сегмента за последние несколько лет стабильно высоки. По данным IDC, только за 1-й квартал 2011 г. прирост здесь составил 44%. Прогнозы на текущий год еще более оптимистичны.

Следуя мировым тенденциям и стандартам автоматизации деятельности, отечественные предприятия активно внедряют бизнес-приложения. СХД всегда являются неотъемлемой частью инфраструктуры подобных проектов. Кроме того, растет потребность в СХД для реализации проектов виртуализации серверного парка, рабочих мест пользователей.

В то же время основные технологические тренды диктуют курс на сокращение капитальных и операционных расходов на ИТ-инфраструктуру. В первую очередь заказчики стремятся сократить стоимость хранения, а также соотнести бизнес-критичность информации со стоимостью аппаратных платформ.

Еще одним направлением развития современного рынка СХД являются так называемые универсальные системы хранения (Unified Storage), позволяющие в рамках единой платформы

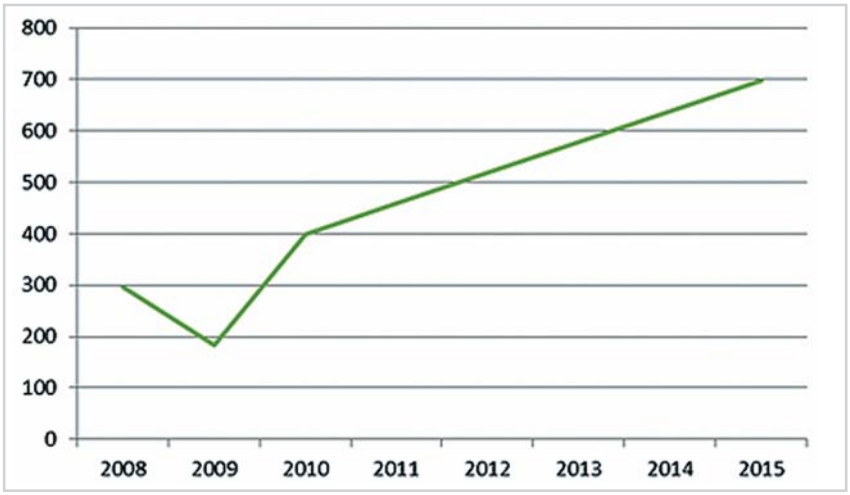


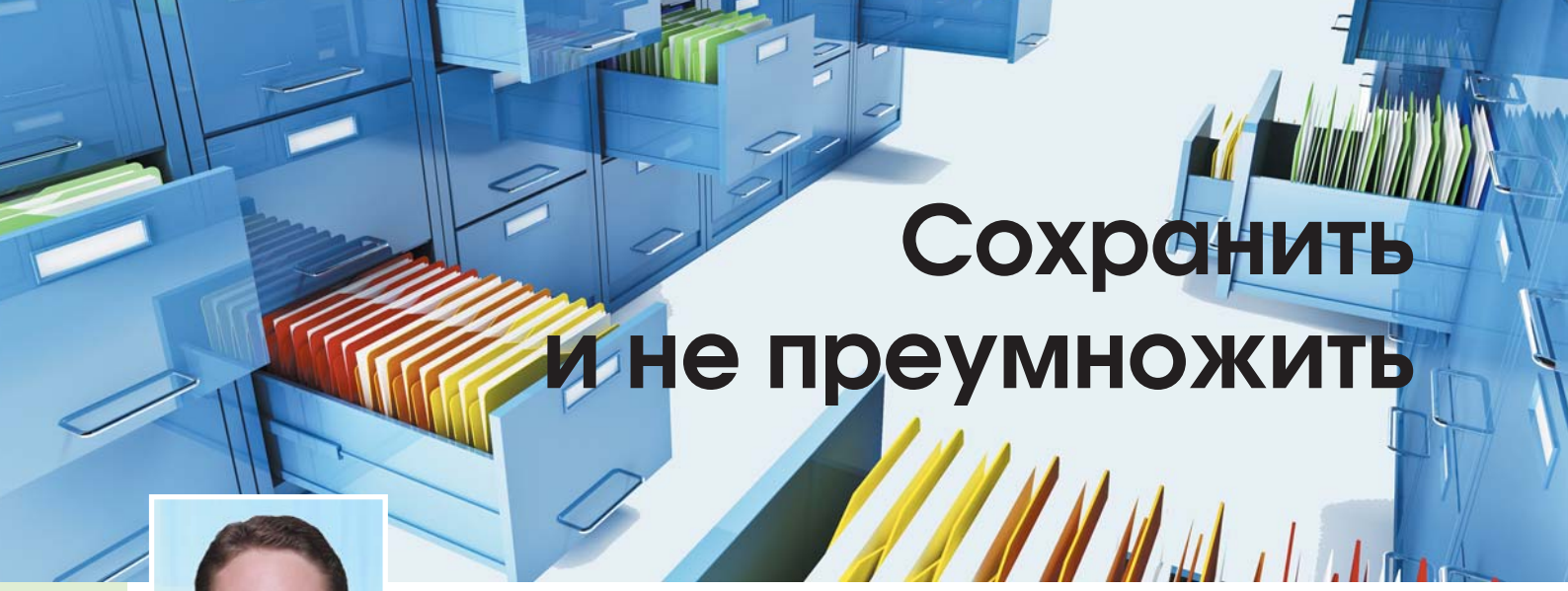
Рис. 1. Объем российского рынка СХД, млн долл.

решать задачи хранения как структурированных, так и неструктурированных данных. Эффективность таких платформ во многом определяется уровнем развития программных компонент.

Заметна тенденция вендоров к производству большого количества сопутствующего ПО для СХД. Этот пласт еще предстоит освоить российскому ИТ-рынку. Его технологическое отставание от мирового уровня на пару лет в данном случае обернется преимуществом, поскольку позволит спрогнозировать ситуацию развития рынка в будущем.

Рис. 2. Поставщики СХД в мире

Подготовлено по материалам: http://www.cnews.ru



Сохранить и не преумножить

Александр Котенко,
старший инженер-проектировщик систем хранения данных гр. систем хранения данных компании «Инфосистемы Джет»

Архивы создают, значит, это кому-нибудь нужно

Сегодня ни для кого не секрет, что объем хранимой информации во всем мире ежегодно увеличивается, причем рост данных происходит экспоненциально. Например, согласно исследованиям аналитического агентства Enterprise Strategy Group, объемы хранимой в мире почтовой переписки ежегодно удваиваются, и в 2012 году суммарный объем превысит 13 ПБ данных.

Подобная тенденция характерна не только для почты, но и для всех типов файлов. Многие компании по всему миру в полной мере ощущают на себе увеличение объемов хранимой информации. Самое простое решение этой проблемы — действовать в лоб, то есть просто увеличивать емкость хранилищ. Многими этот способ действительно рассматривается как панацея от всех бед, благо стоимость терабайта падает с каждым годом. Но не все так радужно, как кажется на первый взгляд. С ростом объемов хранения возникает целый ряд новых проблем, которые переводят эту задачу на качественно новый уровень.

Во-первых, это проблема «полезности» информации: данные растут, а ценность их в то же время падает. Чтобы объяснить ее смысл, можно провести аналогию с добычей золота. Содержание этого драгоценного металла в земной коре крайне невысоко по сравнению с такими металлами, как, например, железо или медь. В основном атомы золота рассеяны среди горных пород, и лишь изредка можно найти его в виде самородков или россыпи. Раньше способы добычи золота были сравнительно простыми: они были нацелены на поиск породы с высоким его содержанием. Но со временем подобные источники этого драгметалла были исчерпаны. Теперь для того, чтобы добыть грамм золота, нужно перерабо-

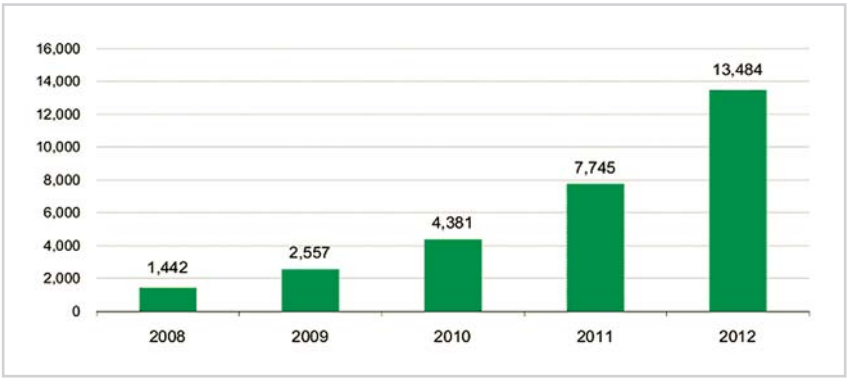


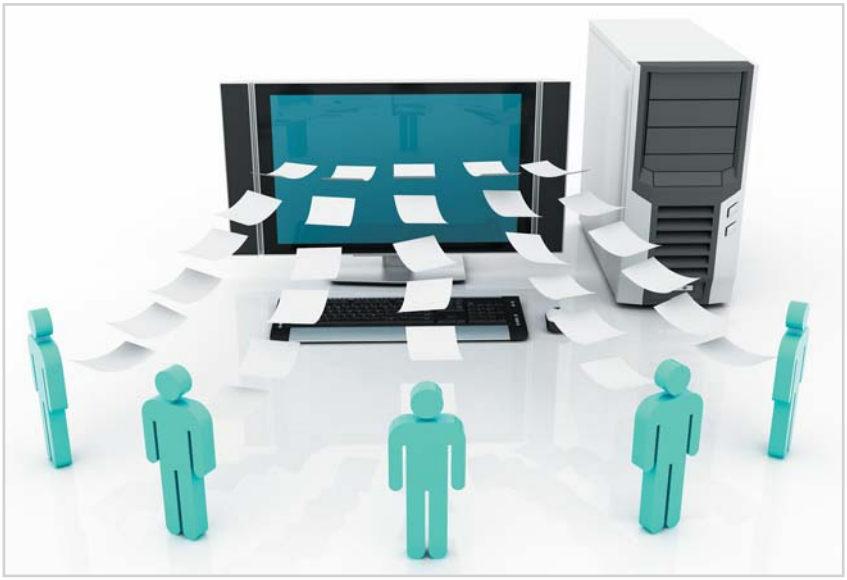
Рис. 1. Увеличение объемов хранимой почтовой переписки в 2008 — 2012 годах (в ПБ)

тать тонны руды. То же самое происходит и с данными: благодаря удешевлению стоимости терабайта пользователи могут сохранять гораздо больше информации, но доля действительно востребованных данных в этом объеме оказывается все меньше и меньше. Чтобы эффективно хранить большие объемы данных, их нужно классифицировать и уметь выделять из общей массы важную информацию.

Во-вторых, с ростом данных возрастает сложность методов их обработки и обеспечения сохранности. Большинству компаний необходимо осуществлять поиск по их данным, причем он должен выполняться за приемлемое время, иначе информация просто будет лежать мертвым грузом. Кроме того, в большинстве случаев эти данные нужно защищать, например, с помощью создания резервных копий или катастрофоустойчивого хранилища (Disaster Recovery). Вдобавок появляются дополнительные проблемы. Традиционные методы резервного копирования не справляются, сроки создания копий выходят за все допустимые лимиты, недопустимо возрастает нагрузка на сеть, серверам резервного копирования требуется все больше вычислительных ресурсов, чтобы переработать возросшие объемы данных, и т.д. Когда речь заходит о построении DR-системы для защиты данных, большинство ИТ-руководителей сразу начинают хвататься за голову: ведь здесь не обойтись просто закупкой новых дисков, нужна вторая аналогичная система, а это значит, что стоимость возрастет как минимум в два раза! Не все готовы пойти на такие жертвы, чтобы защитить данные, ценность которых порой сомнительна. С другой стороны, удалять их тоже нельзя, поскольку они «могут еще пригодиться». Из этой ситуации следует одно очевидное требование: для того чтобы эффективно хранить большие объемы данных, нужно изменить стандартные подходы к их обработке и защите.

Как же решить эти задачи? Одним из наиболее простых и недорогих способов является архивирование. Современные системы архивирования предоставляют широкий набор средств для оптимизации хранения цифрового контента. В первую очередь они позволяют классифицировать данные по уровню их востребованности. Благодаря этому все содержимое можно разделить на важные и второстепенные данные. Сортировка может осуществляться на основе многих критериев, например, по времени последнего обращения к файлам или по типам данных. После того как вся информация классифицирована, для нее выбираются соответствующие способы хранения: наиболее значимые и востребованные данные размещаются на высоконадежных и высокопроизводительных устройствах (например, Hi-End массивы с SAS/SSD-дисками), а остальные — на менее дорогостоящих (Mid-Range и Low-End дисковые массивы с SATA-дисками или магнитные ленты). Кроме того, современные системы архивирования и устройства хранения поддерживают дедупликацию и компрессию. Это позволяет экономить на приобретении дополнительных носителей, что особенно заметно в случае больших объемов данных.

Помимо этого, архивирование позволяет достичь экономии за счет снижения требований к продуктивным системам, ведь зачастую почтовые или файловые серверы функционируют на достаточно дорогом оборудовании. Разгрузка продуктивных систем с помощью архивирования дает возможность избежать масштабной модернизации ИТ-парка за счет сокращения количества размещенных на серверах и системах хранения объектов. Благодаря переносу части данных в архив в том числе значительно упрощается задача обеспечения защиты продуктивных ИТ-систем — не растут объемы данных, следовательно, не увеличивается время создания резервных копий, а в случае DR можно использовать менее дорогостоящее оборудование для резервирования систем. И по-



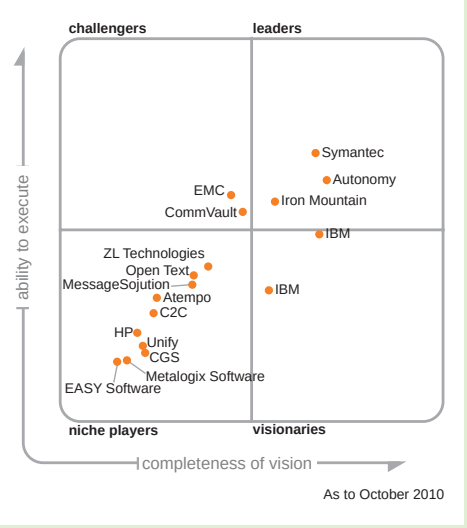
следнее, но не менее важное: современные системы архивирования способны предоставить гибкий поиск по архиву, поскольку поддерживают индексирование всех данных. Инструменты поиска могут использоваться службой безопасности для выявления подозрительного контента по всем архивам.

Symantec Enterprise Vault – серьезный выбор

В настоящий момент на ИТ-рынке существует ряд продуктов для архивирования данных, позволяющих оптимально размещать информацию и обеспечивающих эффективный доступ пользователей к ней. По нашим оценкам, одним из лидеров среди подобных решений является Symantec Enterprise Vault (EV). Это обусловлено многими факторами, в том числе «выдержанностью» продукта, способствующей стабильности программного кода существующих версий.

На наш взгляд, Enterprise Vault является надежным решением для архивирования различных типов данных, подходит как для средних, так и для крупных компаний. Продукт Symantec представляет собой ПО, предназначенное для эффективного управления жизненным циклом информации и электронного раскрытия информации. Изначально EV разрабатывался как средство архивирования электронной почты на базе Exchange, но за время его существования функциональность значительно расширилась.

Решение поддерживает архивирование практически всех версий Exchange (в том числе 2010), клиентская часть совместима со многими операционными системами и почтовыми клиентами. Благодаря продуманной архитектуре, большому числу настраиваемых параметров и тесной интеграции с приложениями и оборудованием сторонних производителей Enterprise Vault подходит для решения широкого круга задач.



Symantec Enterprise Vault в настоящее время – одно из наиболее зрелых решений для архивирования. Продукт начал разрабатываться более 10 лет назад специалистами компании DEC. Затем права на него были выкуплены основателями компании KVS, которая позднее была приобретена корпорацией VERITAS. После поглощения VERITAS Symantec в 2005 году Enterprise Vault стал одним из флагманских продуктов вендора и в настоящее время занимает существенную часть рынка архивирования данных. Согласно отчетам «Gartner Magic Quadrant for Enterprise Information Archiving» за 2008–2012 годы, решение Symantec занимает лидирующие позиции в магическом квадранте.

Архивирование Exchange

Enterprise Vault использует программный интерфейс MAPI для архивирования почтовых сообщений MS Exchange. В отличие от некоторых аналогичных продуктов при открытии пользователем архивного сообщения EV не восстанавливает его на сервер Exchange. Чтение архивных сообщений осуществляется непосредственно с сервера Enterprise Vault по протоколам HTTP или HTTPS.

При архивировании почтовых ящиков используются политики, имеющие гибкие настройки. В хранилище попадают только те сообщения, которые удовлетворяют критериям, указанным в политиках. В Enterprise Vault 10.0 можно настроить архивирование писем, используя в качестве критериев дату получения, размер сообщения, наличие вложения, уровень заполнения почтового ящика (например,

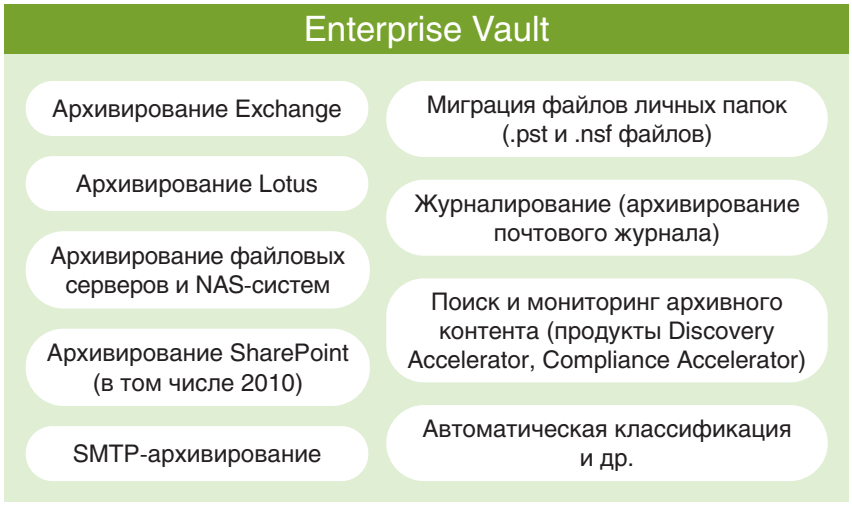


Рис. 2. Модули Enterprise Vault

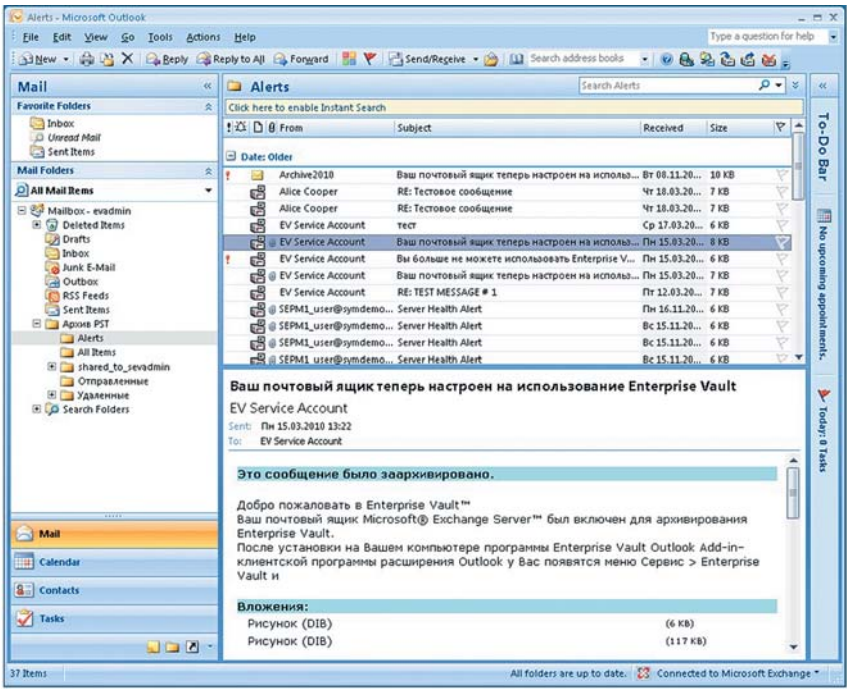


Рис. 3. Внешний вид архивных сообщений в MS Outlook

70% от установленного лимита; при превышении значения наиболее старые письма автоматически перенесутся в архив). Процедура осуществляется прозрачно для пользователей: у сообщения, попавшего в архив, просто изменится пиктограмма. Применяя соответствующие настройки в Outlook, пользователи могут самостоятельно добавлять письма или восстанавливать их из хранилищ.

Продукт поддерживает интеграцию с Outlook Web Access (OWA), благодаря чему пользователи имеют доступ к архиву из любой точки мира, где есть подключение к интернету.

Устранение дубликатов и сжатие

Сообщения и файлы, попавшие в архив, подвергаются дедупликации (Singe Instance) и сжатию. В результате они попадают в хранилище в единственном экземпляре, даже если были у разных пользователей. Дедупликация работает между разными типами архивов — файловым, почтовым, SharePoint и т.д. За счет этих технологий достигается эффективное использование дискового пространства, выделяемого под хранилище.

Миграция файлов PST и NSF

Enterprise Vault позволяет осуществлять миграцию личных папок пользователей в централизованное хранилище, благодаря чему уменьшается риск потери данных и появляется возможность мониторинга ранее не контролируемой информации. Для миграции PST-файлов рекомендуется использовать метод Client-Driven, т.к. в большинстве случаев ее нужно проводить без прерывания доступа почтового клиента к файлу личных папок. На данный момент среди продуктов архивирования почты только Enterprise Vault обеспечивает перенос личных папок пользователей без прерывания работы Outlook.

Благодаря Client-Driven миграция полностью автоматизирована и не требует вмешательства администратора. По ее окончании исходные файлы личных папок могут быть удалены с рабочей станции или помечены атрибутом «Hidden», после чего Outlook перестанет их использовать. Сообщения, которые содержались в файле личных па-

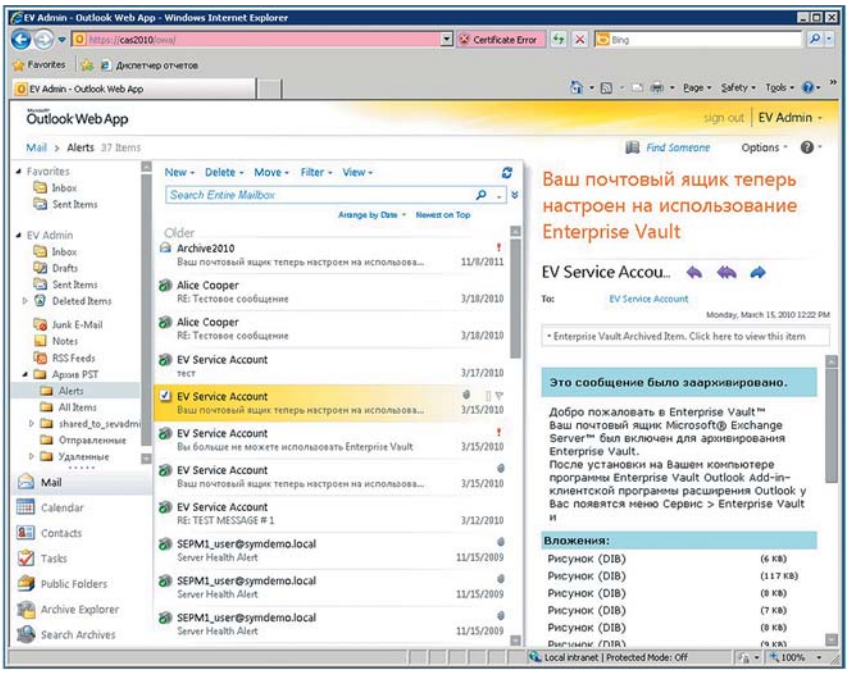


Рис. 4. Внешний вид архивных сообщений в OWA

В российских компаниях не редкой стала ситуация, когда объем данных почтовой системы или системы документооборота переваливает за 10 ТБ, и приложения становятся неповоротливыми и сложно управляемыми. Часто проблемы связаны с большим количеством файлов PST/NSF, которые были накоплены в течение многих лет. Причина их возникновения почти всегда связана с наличием жестких квот на размер почтового ящика. Администрирование этих разрозненных файлов, в свою очередь, является довольно трудоемким процессом, кроме того, почтовая переписка, хранимая в них, недоступна для централизованного мониторинга. Встречаются также проблемы, связанные с переходом на новую версию почтового сервера, – миграция десятков терабайт данных может затянуться на многие недели. Как показывает наш опыт, все эти проблемы решаются с помощью Enterprise Vault. Так, в одном из наших проектов требовалось провести миграцию файлов PST для ~5000 пользователей. Понятно, что этот процесс занимает не один день, более того, если при миграции каждого пользователя прекращать работу почтового клиента, работа сотрудников будет серьезно нарушена. Поэтому заказчиком было поставлено обязательное требование к миграции файлов личных папок – не прерывать работу почтового клиента. Таким условиям на тот момент удовлетворял только Symantec Enterprise Vault. В результате внедрения EV всего за несколько месяцев была проведена миграция PST-файлов для всех пользователей. Этот процесс был полностью автоматизирован и незаметен для сотрудников компании. Теперь вся почтовая переписка, накопленная за многие годы, находится в центральном хранилище, а пользователи получили практически безграничные объемы почтовых ящиков.

пок, переместятся в автоматически созданный раздел в структуре каталогов Outlook. Доступ к сообщениям из личных папок, перенесенных в архив, осуществляется из почтового клиента путем двойного щелчка мышью по пиктограмме архивного сообщения.

Индексация и поиск

Индексация архива, осуществляемая встроенными средствами, позволяет как пользователям, так и администраторам системы выполнять поиск по хранилищу. Enterprise Vault 10.0 имеет 64-битную архитектуру, за счет чего достигается высокая скорость индексирования данных. Начиная с 10-й версии продукта, большинство задач, связанных с администрированием индексов, осуществляется с помощью простых помощников, запускаемых из консоли администратора. Встроенные средства предоставляют возможность поиска по ключевым словам, фильтрации результатов и просмотра найденных сообщений.

Журналирование почты

Средства Microsoft Exchange позволяют создать почтовый ящик (журнал), в котором сохраняются копии всех писем, прошедшие через определенный Data Store. Процесс, обеспечивающий создание копий всех входящих и исходящих сообщений, именуется журналированием. При его настройке осуществляется привязка к одному или ко всем хранилищам Exchange. Это означает, что для каждой почтовой базы Exchange может быть создан отдельный журнал.

Журналирование чаще всего применяется в целях мониторинга корпоративной почты, а также хранения полной базы почтовой переписки для последующего ее использования в юридических целях. Отметим, что журналирование требует заметного увеличения емкости почтовых хранилищ сервера Exchange. ПО Enterprise Vault позволяет заметно сократить объемы хранимых данных за счет их сжатия и дедупликации, а также снизить нагрузку на почтовый сервер путем удаления с него оригиналов сообщений и замены их ссылками.

Поиск по журнальному архиву может осуществляться как встроенными средствами EV, так и с помощью специализированных приложений Symantec Discovery Accelerator (DA) или Compliance Accelerator (CA).

По сути, акселераторы представляют собой надстройку к Enterprise Vault и используют готовый архив для осуществления поиска. Критериями для них могут быть даты, ключевые слова, использование булевых полей, типы вложений и т.д. Результаты на этапе анализа поддаются быстрой сортировке с помощью расширенного поиска в ветках сообщений и разнообразных функций фильтрации. Кроме того, можно устранять дублирование данных в процессе их просмотра и экспорта, таким образом повышая эффективность работы администраторов. Все задания поиска можно запланировать, а специальные папки поиска использовать для упорядочивания элементов, связанных с заданиями.

В большинстве случаев в качестве источника поиска выступает архив почтового журнала, содержащий всю базу сообщений, тем не менее, его можно осуществлять и по архивам отдельных пользователей. DA также позволяет искать данные по хранилищам файлов, SharePoint, и общим папкам. CA предназначен только для поиска по почтовым архивам. Сравнивая оба акселератора, можно отметить, что

функционал DA и CA очень похож. Тем не менее, есть и отличия: в DA администратор сам должен запускать поиск, а затем передавать подозрительные письма для исследования группе, отвечающей за безопасность. В CA этот процесс автоматизирован: сообщения, попавшие в архив, сразу же проверяются на предмет соответствия требованиям безопасности, подозрительные попадают в отдельную категорию, требующую изучения специалистами.

По сравнению с функциями, предоставляемыми стандартными средствами поиска Enterprise Vault, отличительными особенностями акселераторов являются:

- наличие базы данных, в которой сохраняется вся история поисковых запросов;
- разделение ролей пользователей и наличие готовых ролей с определенным перечнем функций;
- возможность изучения как отдельных сообщений, так и всей цепи пересылки информации между несколькими пользователями.

В приложениях можно создать несколько баз данных с целью разделения и обеспечения безопасности информации для определенных групп сотрудников (юридического управления, отдела кадров и т.д.) или согласно определенным требованиям (например, к конфиденциальности данных).

На счету нашей компании – внедрения Enterprise Vault в крупных российских банках, в том числе проект по архивации Exchange и миграции PST-файлов для ~5000 пользователей. В 2011 году компания «Инфосистемы Джет» первая в России получила специализацию Symantec Archiving and eDiscovery, которая включает в себя работу с продуктом Enterprise Vault.

Миграция файлов

Миграция предназначена для разгрузки продуктивных файловых серверов или NAS-систем. В качестве источников для Enterprise Vault могут выступать не только серверы Windows, но и сетевые хранилища с поддержкой CIFS: Symantec FileStore, NetApp FAS, EMC Celerra. Кроме того, EV интегрируется со специализированными контентными платформами, такими как Hitachi Content Platform, EMC Centera, Fujitsu ETERNUS и т.д.

После осуществления миграции на файловом сервере происходит замена файлов на ярлыки или гиперссылки, имеющие размер всего 4 кб. Соответственно для архивных файлов, изменяется и внешний вид пиктограммы.

Восстановление файлов средствами EV является прозрачным для пользователей: при попытке открытия они практически мгновенно восстанавливаются на сервер. При этом в EV присутствуют механизмы, препятствующие массовому восстановлению файлов в случае выполнения процедур антивирусного сканирования или резервного копирования.

Для архивирования используются соответствующие политики: благодаря им в хранилище попадают только те файлы, которые удовлетворяют их критериям. В качестве критериев могут быть выбраны:

- тип файла;
- время создания;
- время последнего доступа или изменения;
- размер;
- атрибуты файла.

Модуль файлового архивирования включает в себя функцию блокирования нежелательного контента, за которую отвечает File Blocking Service. Последний обеспечивает запрет на запись тех типов файлов, которые указаны в соответствующей политике. Пользователи не могут нарушить работу сервиса простой сменой расширения файла или путем упаковки его в архив – Enterprise Vault верифицирует содержимое файла на уровне сигнатуры.

Кроме того, имеется возможность настройки автоматического удаления файлов по истечении заданного срока. Удаление

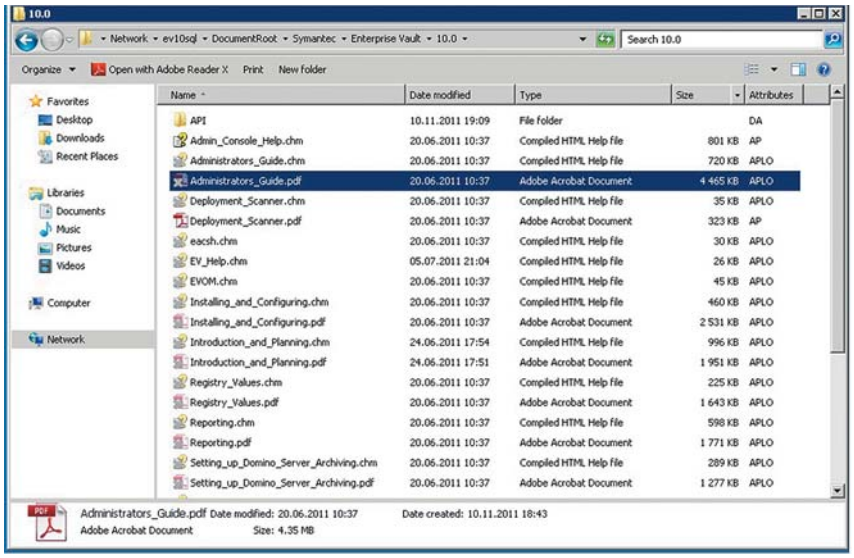


Рис. 5. Внешний вид архивных ярлыков на файловом сервере

определяется категориями Retention, которые могут устанавливаться индивидуально на каждую отдельную папку файлового хранилища.

Хранение архива на магнитных лентах

Система архивирования Enterprise Vault может быть интегрирована с ПО резервного копирования Veritas NetBackup или Symantec BackupExec, которые позволяют осуществлять автоматическую миграцию архива с дискового массива на магнитные ленты. Перенос на ленты обеспечивает долговременное хранение контента с минимальными затратами. Он происходит автоматически в соответствии с выбранными критериями, например, по истечении заданного времени или при достижении определенного уровня заполнения тома на дисковом хранилище.

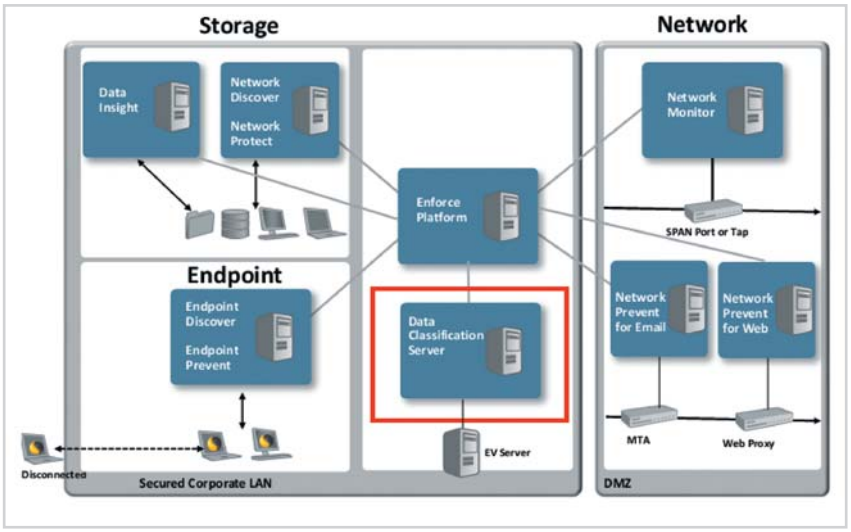


Рис. 6. Схема интеграции EV с DLP

Интеграция с DLP

Начиная с 10-й версии Enterprise Vault, появилась интеграция решения с Data Classification Services в Symantec Data Loss Prevention (DLP). В результате стали доступны более гибкие механизмы классификации входящих почтовых сообщений. Входящую почту можно автоматически отсортировать по различным признакам (например, по наличию ключевого слова, почтового домена в адресах, конкретному отправителю и т.п.) и разместить по соответствующим архивам с разными сроками хранения. Для использования сервера Data Classification Services в инфраструктуре EV не требуется отдельная лицензия, необходимо только наличие компонентов DLP.

Востребованными в последнее время оказались совместные решения Symantec и CommonDesk по доступу к архиву с мобильных устройств для BlackBerry и iOS – ведь большинство руководителей сейчас пользуются смартфонами и планшетами.

Решение ARCviewer позволяет установить приложение на смартфон и пользоваться архивом удаленно. При этом доступны такие функции, как просмотр архивных сообщений EV, их поиск, добавление и восстановление из архива и даже пересылка. В настоящее время ведется разработка аналогичного продукта для платформы Android.

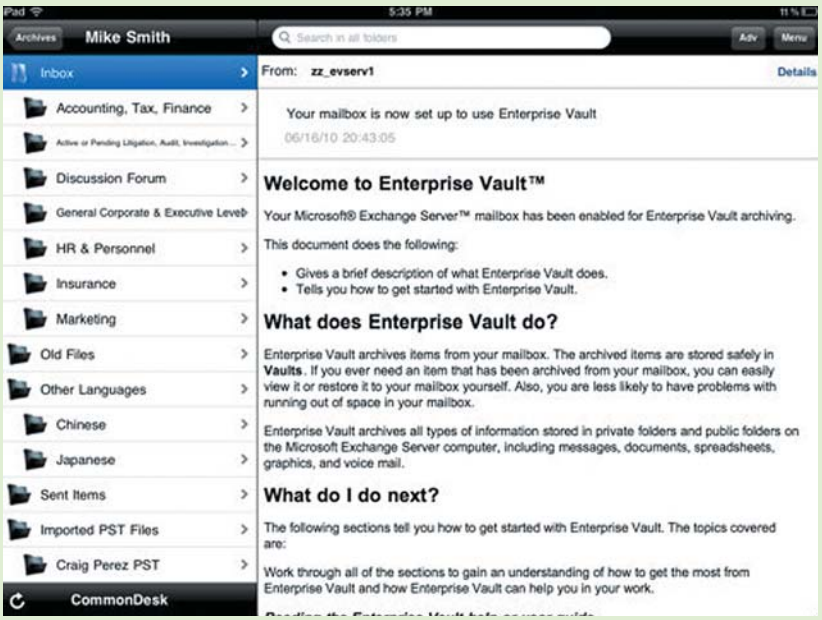
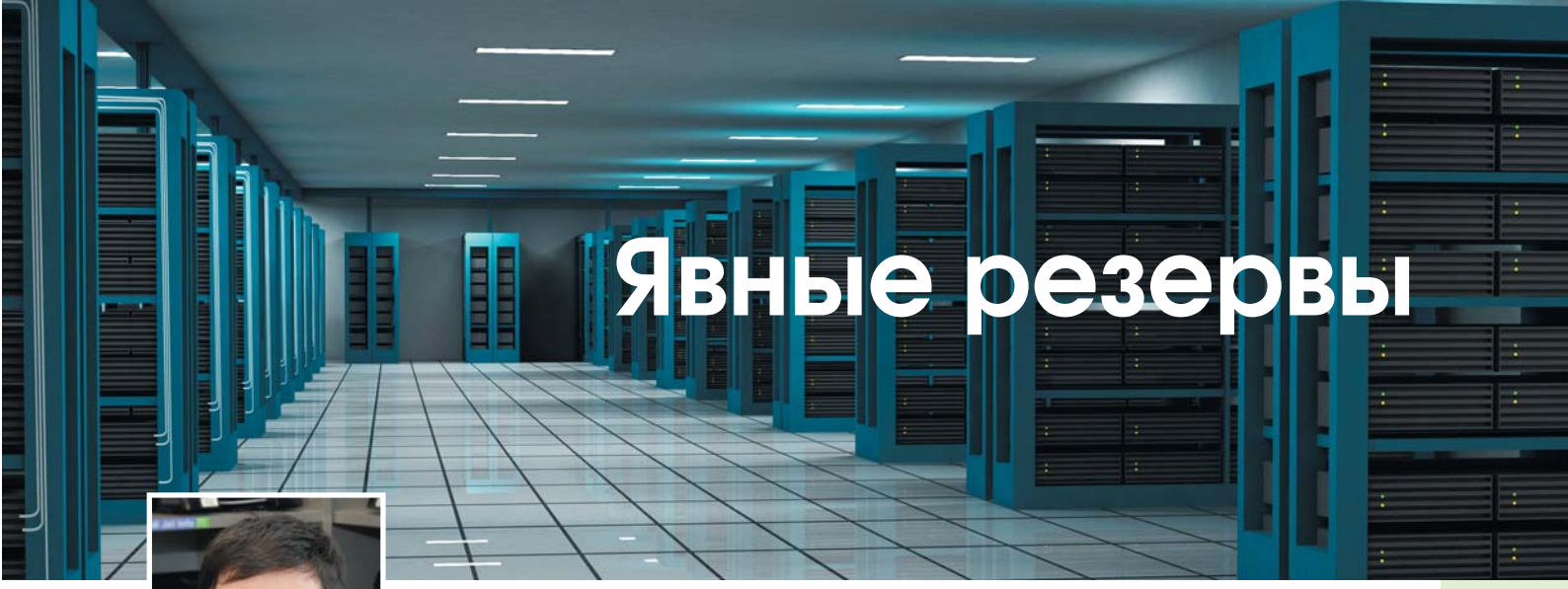


Рис. 7. Просмотр архивных сообщений на iPad с помощью ARCViewer

Резюмируя

Если вам не чужды проблемы, озвученные в этой статье, и вы задумываетесь о рациональном использовании ресурсов внутри вашей компании — добро пожаловать в мир Enterprise Vault, где мы готовы стать вашим проводником и помощником.



Явные резервы

Алексей Быков,
ведущий инженер-проектировщик систем хранения данных компании «Инфосистемы Джет»

СРК – какой она должна быть

Система резервного копирования (СРК) является одной из важнейших составляющих в деле защиты данных и зачастую — последней надеждой в случае аварий, приводящих к их потере в продуктивных системах. Именно поэтому при построении СРК важно выбрать продукт, который, помимо широкого функционала, отличался бы еще и надежной, стабильной работой. Для того чтобы понять схему функционирования решений для резервного копирования, необходимо начать с азов — с принципов построения любой СРК. Несмотря на разные названия компонентов у разных вендоров, подходы практически везде одинаковы (см. рис. 1). Так, основными составляющими системы резервного копирования являются:

- Мастер-сервер, который выполняет функции управления СРК, политиками и расписаниями резервного копирования, а также хранит БД копий.
- Медиа-сервер, отвечающий за передачу данных от клиентов СРК и их запись на устройства хранения. Функциональность мастер- и медиа-сервера может быть объединена в одном физическом сервере.
- Клиент СРК — сервер или рабочая станция, данные которых необходимо резервировать.

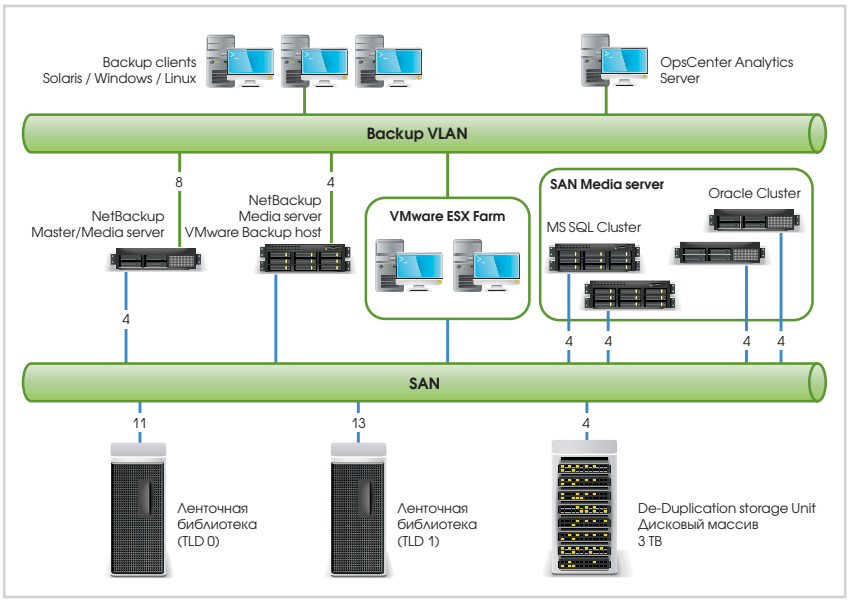


Рис. 1. Пример компонентной схемы СРК (основано на реальных событиях)

Рис. 2. Схема взаимодействия программных компонентов NetBackup

- Устройства хранения — ленточные или дисковые накопители, служащие хранилищем для резервных копий.

В соответствии с заданным расписанием мастер-сервер по LAN инициирует процесс передачи данных от клиента СРК на заданное устройство хранения, присоединенное к какому-либо медиа-серверу. После того как устройство хранения становится доступным, клиентские данные начинают передаваться на медиа-сервер по локальной сети, а оттуда — записываться на ленты или диски, подключенные напрямую (SCSI, SAS) или через сеть хранения данных (SAN).

От теории к практике

Сегодня на ИТ-рынке присутствует довольно много решений, способных справиться с задачами, которые ставятся перед СРК, — требованиями надежности хранения информации и простоты эксплуатации. В то же время некоторые из предлагаемых средств имеют в своем составе более широкий набор инструментов, востребованных в том числе российскими компаниями.

Так, продукт от компании Symantec — NetBackup (NBU) (см. рис. 2) — обладает рядом преимуществ по сравнению с аналогичными решениями других производителей. Одно из них — стабильность. NBU может непрерывно функционировать в течение продолжительного времени, требуя только плановых остановок/перезагрузок в случае профилактических работ на оборудовании или установок патчей.

Для NetBackup, как и для других своих продуктов, Symantec регулярно выпускает патчи, направленные на устранение обнаруженных ошибок (как правило, превентивное), а также добавляющие функционал и обеспечивающие поддержку новых версий смежного ПО. Таким образом, при регулярных обновлениях NBU компания может апгрейдить свои прикладные системы или внедрять новые, гарантируя себе их совместимость с существующей СРК.

Что умеем – как храним

Резервное копирование приложений

NBU обладает достаточно широким списком совместимости с наиболее популярными приложениями и БД: SAP, Oracle, DB/2, MS Exchange, MS SQL и др. Специализированный программный модуль Database Agent интегрируется с Backup API приложения и обеспечивает целостность данных при записи на ленту.

Для приложений Microsoft (SQL, Exchange, SharePoint, AD) поддерживается возможность гранулярного восстановления данных из резервных копий, выполненных целиком на уровне файлов. Она особенно актуальна для последних версий MS Exchange, в которых нет встроенных средств для РК на уровне отдельных почтовых ящиков, папок и сообщений. Чтобы обеспечить возможность гранулярного восстановления, резервные копии приложений должны размещаться на дисковых устройствах хранения.

Дедупликация

Начиная с версии 7.0, в NetBackup появилась возможность встроенными средствами выполнять дедупликацию резервных копий. Она может осуществляться на любом этапе их создания — на клиенте или медиа-сервере. Дедуплицированные резервные копии хранятся на дисковых устройствах хранения, присоединенных к медиа-серверу. Такой комплексный подход позволяет строить СРК с использованием этой технологии в рамках решений одного вендора. Только так дедупликация даст максимальный эффект по всей цепочке следования данных — от клиента до устройства хранения.

В частности, мы использовали описанную технологию в проекте с крупным ритейлером, когда возникла задача хранения резервных копий MS Exchange 2010 с возможностью гранулярного восстановления. Поскольку в этом случае нужны копии, размещенные на дисковом устройстве хранения, без применения

дедупликации их объем был бы весьма велик. Использование технологии позволило сократить объемы хранения более чем в 4 раза.

NBU обладает функционалом для тесной интеграции с VMware, благодаря чему компании могут:

- осуществлять РК виртуальных машин целиком на уровне VMDK-файлов с сохранением возможности пофайлового восстановления;
- восстанавливать приложения Microsoft (MS SQL, Exchange…) из резервной копии, выполненной через vStorage API;
- выполнять резервное копирование на уровне VMDK-файлов через SAN, не нагружая при этом ESX-серверы трафиком РК.

Система мониторинга и отчетности

Помимо стандартного интерфейса управления, в состав NetBackup входит дополнительный модуль для мониторинга состояния СРК и отчетности NetBackup OpsCenter. OpsCenter позволяет генерировать отчеты, содержащие необходимую информацию о ресурсах системы резервного копирования, выполненных заданиях по РК, возникших ошибках при backup/restore и многом другом. Они могут генерироваться в том числе в автоматическом режиме и отправляться по e-mail администраторам СРК или ответственным за прикладные системы. Кроме того, актуальную информацию, которую необходимо мониторить в режиме online, можно вывести на Dashboard.

OpsCenter способен работать не только с NetBackup, но и с СРК других производителей (TSM, DataProtector, CommVault) через специального программного агента. Это позволяет из одной точки мониторить все системы резервного копирования в ИТ-инфраструктуре заказчика. Еще одной функцией OpsCenter является возможность подсчитывать потребление ресурсов СРК и в соответствии с заданными метриками конвертировать их в конкретную стоимость. Это весьма полезно для крупных компаний с разветвленной организационной структурой, различными центрами финансовой ответственности и собственными бюджетами у каждой бизнес-единицы, а также для хостинговых операторов и провайдеров облачных сервисов.

Если заказчику не достаточно большого набора стандартных отчетов, то, приобретя расширенную лицензию OpsCenter Analytics, можно строить собственные. Этим функционалом воспользовался один из наших заказчиков — крупная ритейловая компания: она разработала набор уникальных отчетов об использовании ресурсов СРК, регулярно отсылаемых ответственным за бизнес-системы.

NBU совместим с большим количеством оборудования от разных производителей и может интегрироваться с API для создания снапшотов на дисковых массивах. Использование агентов для резервного копирования приложений (Oracle, SAP, DB/2, MS SQL, Exchange и др.) гарантирует целостность копий, выполненных без их остановки. Эти опции позволяют говорить о Symantec NetBackup как об оптимальном инструменте для резервного копирования Enterprise-класса.

Преодоление узких мест

При стандартной схеме резервного копирования (РК) нередко возникает проблемы, связанные с его производительностью. Попробуем описать имеющиеся в NBU возможности для их решения.

Первая трудность связана с возможной разницей в скорости передачи данных от клиента на медиа-сервер по сети и записи на устройство резервного копирования (ленту). Так, для Gigabit Ethernet реальная скорость составляет 50 Мб/с, для не самого современного привода LTO4 — 120 Мб/с без учета компрессии. Разница в производительности между Back-end и Front-end — более чем в 2 раза. В случае, когда клиент способен обеспечить высокую скорость чтения, уз-

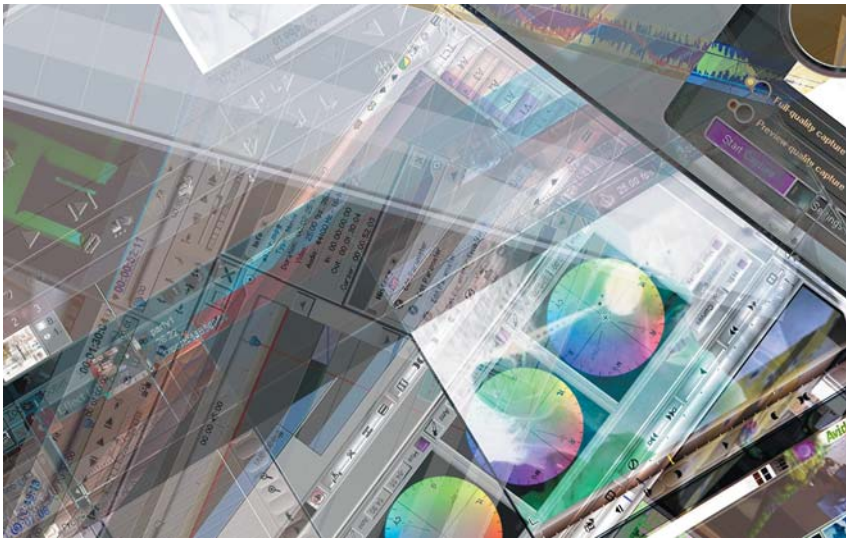
ким местом становится сеть. Для решения этой проблемы используется опция «SAN Media Server». Ленточные приводы присоединяются к клиентам через SAN, и скорость РК ограничивается уже, как правило, скоростью записи на привод. Такая технология используется у многих наших заказчиков, имеющих развитую инфраструктуру SAN и серверы с большими объемами данных.

Следующая проблема — это медленное резервное копирование для файловых систем (ФС) с большим количеством файлов. Задержки здесь связаны с архитектурой ФС, которая не позволяет быстро прочитать всё содержимое. Опция Enterprise Client дает возможность выполнять РК по технологии FlashBackup: весь дисковый том копируется целиком как «сырое устройство», при этом сохраняется возможность пофайлового восстановления данных. В частности, такая схема РК эффективно применялась нами в телекоммуникационных компаниях для резервирования файловых систем с данными о трафике. За счет использования этой технологии производительность РК удалось поднять более чем в 4 раза.

Поскольку FlashBackup имеет ограничения по совместимости, в ситуациях, где ее применение невозможно, прибегают к Multistreaming — многопоточному резервному копированию. Набор резервируемой информации делится на ряд потоков, и данные с клиента считываются несколькими разными процессами одновременно, что повышает суммарную производительность. Например, мы применили такую схему в одном из банков для РК почтовой системы GroupWise с большим количеством почтовых ящиков пользователей. Используемая заказчиком конфигурация ПО не позволила обратиться к другим технологиям, поэтому мы разделили backup на 8 независимых потоков, после чего продолжительность резервного копирования сократилась в 8 раз.

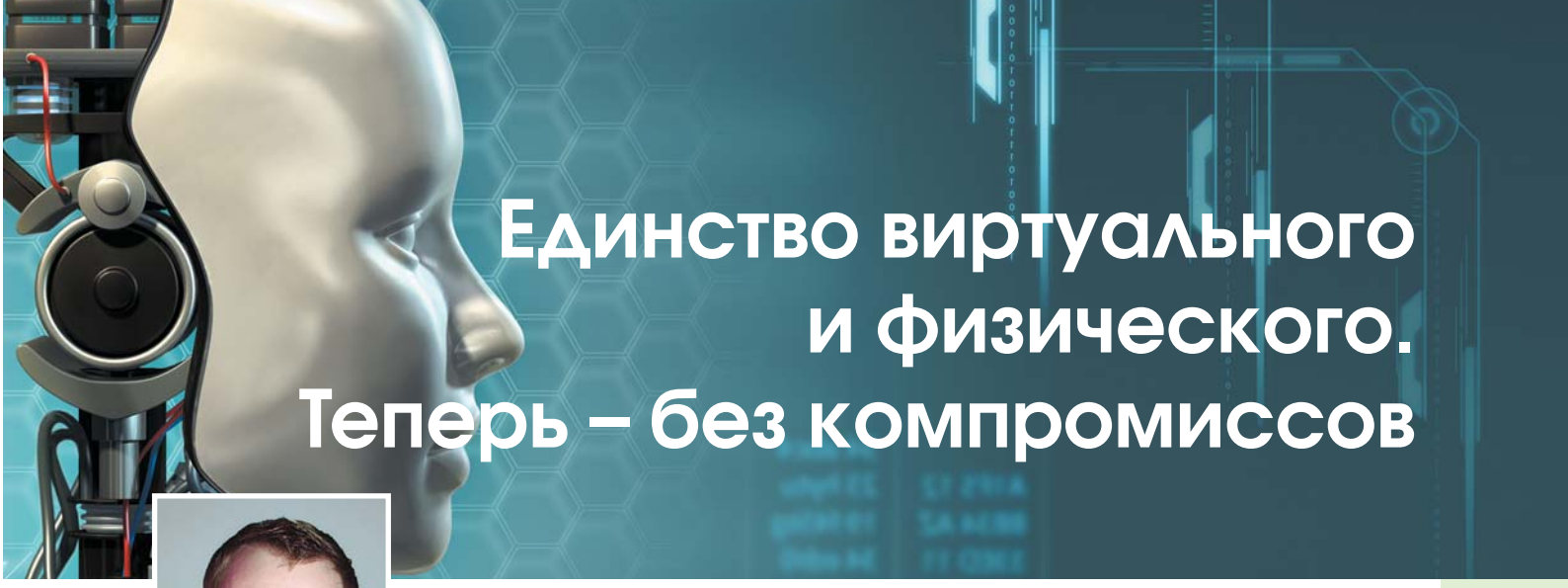
Также возможно объединение медленных потоков в один с помощью Multiplexing. Технология обеспечивает запись на ленточный привод не одного, а нескольких потоков данных (если необходимо, с разных клиентов) для более полной утилизации привода. Эта схема достаточно успешно применялась нами в проекте, реализованном для телекоммуникационной компании. Для сокращения общего окна backup'а при небольшом количестве доступных приводов мы мультиплексировали несколько медленных backup'ов файловых серверов для записи на 1 привод LTO4.

Еще одним способом повышения производительности РК является копирование данных со Snapshot'ов, которые могут быть как программными (созданными с помощью Symantec Storage Foundation), так и выполненными средствами дисковых массивов. NetBackup имеет в своем составе инструменты взаимодействия с управляющим ПО для большинства популярных платформ Enterprise-класса, представленных на российском рынке.



Резюме

В процессе общения с заказчиками нам часто приходится сталкиваться с тем, что ПО резервного копирования уже через пару лет не устраивает компанию по своему функциональному наполнению, и его приходится менять. NBU может избавить вас от этих проблем: как показывает практика, система приобретается один раз и практически навсегда, покрывая собой все потребности в резервном копировании.



Единство виртуального и физического. Теперь – без компромиссов

Максим Прахов,
менеджер по работе с партнерами компании Symantec

Резервное копирование как метод защиты данных остается актуальным вопросом: половина компаний малого и среднего бизнеса сталкивалась с потерей данных, лишь треть из них считает применяемые методы защиты удовлетворительными, а более половины компаний не могут допустить более 4 часов простоя. Многие производители предлагают решения для резервного копирования виртуальных сред, но лишь немногие из них позволяют одинаково эффективно защищать и физическую, и виртуальную инфраструктуру, при этом до 65% виртуальных машин (ВМ) продолжают оставаться незащищенными. Очевидно, что использование одного средства в качестве щита для ИТ-среды, состоящей из физических и виртуальных серверов, уменьшает сложность администрирования и связанные с этим риски, а также снижает затраты на программное обеспечение.

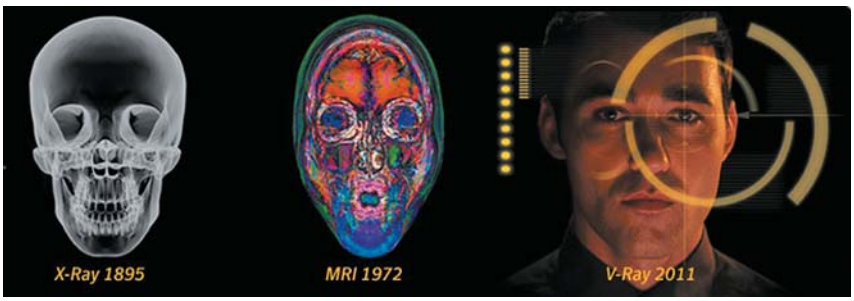
Использование системы резервного копирования (СРК) в ИТ-среде компании позволяет защитить данные от потери или искажения в случае не только сбоев или выхода из строя оборудования, но и ошибок программных средств и пользователей. Несмотря на название, главным предназначением СРК является восстановление данных, которое должно быть удачно выполнено при первой же необходимости вне зависимости от причин, обусловивших его выполнение. Главное отличие резервного копирования от технологий репликации — это версионность, т.е. возможность восстановления данных по состоянию на определенный момент времени.

По оценкам аналитического агентства Gartner (System Backup/Recovery Revenue Market Share, 2010), компания Symantec занимает лидирующую позицию на рынке ПО резервного копирования с рыночной долей не менее 35%. Это стало возможным благодаря наличию линейки из трех специализированных решений, ориентированных на разные масштабы компаний-заказчиков — от малого бизнеса до Enterprise-уровня: System Recovery, Backup Exec и NetBackup. Мы подробно остановимся на втором решении, поскольку именно Backup Exec способен удовлетворить потребности широкого круга компаний из SMB-сектора.

Symantec Backup Exec как самостоятельный продукт развивается более 10 лет. В рамках версии 2010 за последние 2 года состоялись несколько релизов, благодаря которым произошло усовершенствование техноло-

гий дедупликации, защиты виртуальных сред и встроенного функционала архивирования почты и файлов. Несмотря на выпуск этих мини-релизов, не прекращалась разработка новых технологий, которые позволили осуществить кардинальное обновление продукта. Итак, что же предлагает релиз новой, 2012-й версии Backup Exec?

В первую очередь это полноценная и прозрачная защита виртуальных сред VMware и Hyper-V, реализуемая набором технологий, известных под общим названием V-Ray (по аналогии с рентгеновскими лучами X-Ray является «рентгеном» для виртуальной среды).



Рентген XXI века

V-Ray — это и технологии, и полнота видения, которая достигается за счет комплексного применения продуктов Symantec для виртуальных сред: решений из области резервного копирования (Backup Exec и NetBackup), высокой доступности (ApplicationHA), безопасности (Endpoint Protection), хранения данных (Storage Foundation) и мониторинга ИТ-среды (IT Management Suite).

Перечислим основные составляющие технологии V-Ray, реализованной в Backup Exec 2012.

- **Гранулярное (выборочное) восстановление** позволяет как восстанавливать ВМ целиком, так и извлекать отдельные файлы и элементы приложений (например, письма Exchange или объекты Active Directory) из сформированного за один проход образа виртуальной машины. При создании резервной копии ВМ Backup Exec имеет полное представление о ее содержимом. Это достигается за счет чтения и индексирования томов VMDK или VHD на уровне дисковых разделов и использования технологий vStorage APIs for Data Protection и Changed Block Tracking. Даже в случае восстановления отдельного файла из инкрементальных копий ВМ не требуется выполнять никаких дополнительных компиляций данных — Backup Exec обращается к индексу и сразу извлекает только требуемые данные.
- **Консистентное копирование приложений внутри ВМ** выполняется при помощи специального VSS-провайдера VMware, позволяющего собрать дополнительные данные, требуемые для выборочного восстановления отдельных элементов приложений за один шаг.
- **Автоматическое обнаружение виртуальных машин** (в том числе новых) и связанных с ними дисков. Осведомленность о том, сколько параллельных процессов резервного копирования происходит в данный момент, позволяет оптимизировать и при необходимости ограничить нагрузку на ESX-хост. Этот функционал также позволяет защищать новые виртуальные машины сразу после их создания.
- **Мониторинг и управление резервным копированием ВМ** можно вести напрямую из основной консоли управления виртуальной средой VMware vSphere. Для решения этой задачи был разработан специальный плагин Backup Exec Management Plug-in for VMware, поставляемый в рамках агента для защиты виртуальных сред.
- **Автоматизированная проверка созданной копии виртуальной машины** Recovery Validator и интеграция с ApplicationHA. При помощи функции Recovery Validator, реализованной в интерфейсе Management Plug-in for VMware, можно выполнить пробный запуск ВМ из резервной копии в изолированной рабочей станции VMware. Интеграция с Symantec ApplicationHA — средством высокой доступности приложений в виртуальной среде — позволяет автоматически извлекать виртуальную машину из резервной копии, если перезапуск приложения и виртуальной машины уже не может помочь восстановить работоспособность приложения.
- **Эффективная и гибкая дедупликация данных** для сред Windows/Linux, выполняемая на клиентах или на сервере резервного копирования.

Резервные копии? На диету!

Функционал Backup Exec позволяет выполнять единую дедупликацию для виртуальных и физи-

ческих сред, производить управление всеми процессами и мониторинг резервного копирования из одной консоли. В условиях, когда до 70% данных в резервных копиях дублируется, важным аспектом становится применение технологии дедупликации, причем качественной. Важно, чтобы процесс анализа и отбора уникальных блоков данных и их сохранение в единственном экземпляре выполнялись глобально — применительно ко всем заданиям резервного копирования. В противном случае такой алгоритм правильнее будет назвать компрессией, нежели дедупликацией. В Backup Exec используется технология PureDisk, доказавшая свою эффективность при работе в ИТ-инфраструктуре крупных компаний в рамках многочисленных инсталляций Enterprise-решения Symantec NetBackup.

Дедупликация, выполняемая на клиенте (Source Deduplication), предотвращает передачу избыточных блоков данных на сервер резервного копирования, за счет этого сокращаются и окно копирования, и нагрузка на сеть. По сути, этот метод полностью заменяет привычные инкрементальные/дифференциальные копии: можно настроить ежедневное создание полной копии с дедупликацией на клиенте, при этом резервироваться будут лишь те блоки данных, которые являются новыми по отношению к ранее созданным.

Исходя из практического опыта, можно утверждать что дедупликация позволяет сокращать объемы хранимых копий от 2 до 20 раз. Такой разброс обусловлен потенциальным количеством типов данных и степенью их дублированности, что является индивидуальной характеристикой каждой компании. Чтобы упростить проектирование СРК, в том числе оценить окно резервного копирования, нагрузку на сеть и требуемые объемы дисковой системы хранения резервных копий, была выпущена утилита Deduplication Assessment Tool, доступная для партнеров Symantec. Утилита может быть установлена на одном из x86/x64 Windows-серверов и позволяет оценить эффективность дедупликации во всей среде заказчика — при помощи агентов она обеспечивает сбор данных с удаленных систем. Установка агентов выполняется в режиме Мастера, они оказывают минимальное воздействие на продуктивную систему и удаляются сразу после выполнения вычислений. В данный момент поддерживается оценка эффективности дедупликации файловых систем, приложений Exchange и MS SQL, а результаты могут отображаться по серверам или по типам данных.

Поднять сервер из backup'а

Новая версия Backup Exec оснащена встроенным функционалом быстрого восстановления систем, доступным в рамках основных лицензий. Быстрое развитие Backup Exec в этом направлении произошло за счет переноса в решение технологий из специализированного продукта Symantec System Recovery.

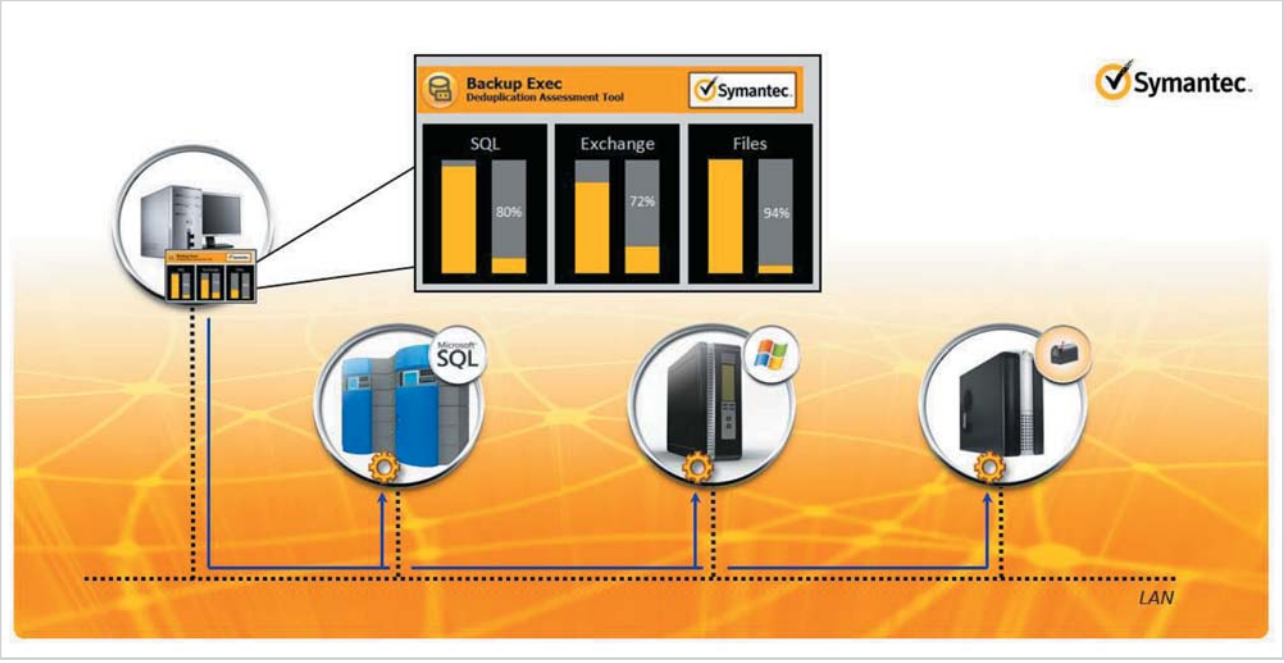


Рис. 1. Принципы работы утилиты оценки эффективности дедупликации

Рис. 2. Новый функционал — преобразование резервной копии в виртуальную машину

Теперь Backup Exec способен быстро восстанавливать системы на «голое железо» (при помощи универсального загрузочного диска), в том числе на «новое железо» и в виртуальную среду. Для восстановления работоспособности сервера с использованием виртуальной среды достаточно лишь взять файл виртуальной машины, подключить и запустить его через гипервизор. При этом образ системы может быть заранее (по расписанию) сконвертирован в виртуальный формат. По сравнению с System Recovery новый Backup Exec имеет дополнительный функционал, например, есть возможность создания образа ВМ сразу при резервном копировании.

Встроенный функционал быстрого восстановления систем также может быть использован для защиты физического медиа-сервера Backup Exec и базы данных каталога.

Встречаем по интерфейсу

Реализованный в версии 2012 русскоязычный интерфейс построен на новой концепции, в основу которой положена защита серверов, а не создание и настройка политик резервного копирования. Это означает, что теперь администратор может сразу оценить состояние защиты всех серверов и то, как проходило резервное копирование в каждый день недели.

Теперь для настройки резервного копирования нескольких серверов можно одновременно выбрать их в списке, а затем определиться с наиболее подходящим методом: копирование на диск, на ленту, на диск с последующим дублированием на ленту (D2D2T), на диск с одновременным или последующим соз-

Для компаний, в которых виртуальная инфраструктура является преобладающей, предназначена редакция Backup Exec 2012 V-Ray Edition. Продукт лицензируется по сокетам виртуального хост-сервера и включает в себя защиту неограниченного количества ВМ, виртуализированных приложений и баз данных.

Для малого бизнеса существует специальная редакция Backup Exec 2012 Small Business Edition, в которую уже включена защита файловых систем, приложений Exchange, MS SQL, AD, SharePoint и сред Hyper-V. Продукт ориентирован на компании, имеющие не более трех серверов, и позволяет установить и настроить систему резервного копирования за три шага, занимающие не более 10 минут.

Для заказчиков, ИТ-инфраструктура которых включает в себя большое количество сервисов при сравнительно небольшом объеме данных, предусмотрена возможность лицензирования нового Backup Exec именно по объему информации (Front End TB).

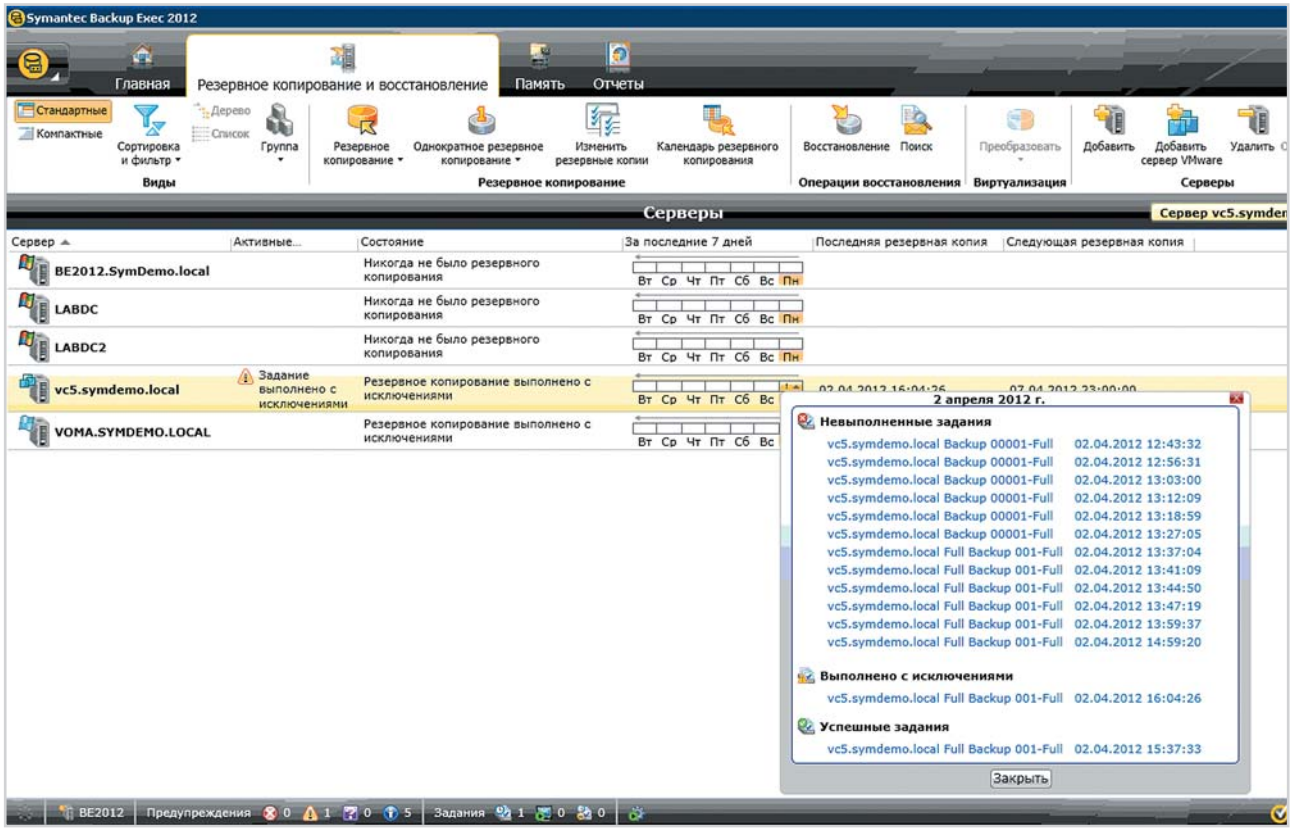


Рис. 3. Новый интерфейс Backup Exec 2012 — защита серверов в центре внимания

данием виртуальной машины и т.д.

Адаптивность интерфейса проявляется в том, что при настройке защиты сервера будут отображаться лишь те части интерфейса и опции, которые актуальны для имеющихся на нем приложений и баз данных. Это стало возможным благодаря предварительному сканированию ИТ-среды и выявлению сервисов, подлежащих защите.

Мы полагаем, что выход новой версии Backup Exec является своевременным и соответствует ИТ-тенденциям и вызовам, с которыми сталкиваются компании из сегмента малого и среднего бизнеса. Symantec не намерена останавливаться на достигнутом, вполне вероятно, что к концу года увидят свет следующие версии продуктов, которые в очередной раз внесут свою лепту в технологическое развитие ИТ-индустрии.

Интеллектуальное хранение

Юрий Семенюков,
старший инженер-проектировщик Отдела проектирования вычислительных комплексов компании «Инфосистемы Джет»

Пакет решений Symantec Veritas Storage Foundation (VxSF) на сегодняшний день является одним из лидирующих продуктов Enterprise-уровня для управления хранением данных. VxSF обеспечивает эти функции для всех основных платформ и оборудования, применяемых в настоящее время у заказчиков. Из всех подобных продуктов он предоставляет наиболее полный стек программного обеспечения — от менеджера томов и собственной файловой системы до кластерного решения. При этом Veritas Storage Foundation дает возможность индивидуального подбора необходимой функциональности, обеспечивая тесную интеграцию между выбранными компонентами и предоставляя большое число различных редакций пакета. В то же время интеграция значительно упрощает настройку и администрирование программного обеспечения.

Поскольку VxSF совместим практически со всем ПО и оборудованием основных вендоров Enterprise-рынка, компании могут гибко настраивать его под свои нужды (например, вместо встроенного менеджера томов или файловой системы использовать уже функционирующие в ИТ-инфраструктуре решения). Гибкость в настройке позволяет построить единое стандартизированное решение для разных платформ, на которых размещаются бизнес-системы заказчика. Это ведет к сокращению расходов на внедрение и администрирование VxSF, упрощению архитектуры, а также повышению общей надежности работы систем.

Для обеспечения высокой доступности приложений и снижения времени незапланированных простоев в составе VxSF предусмотрено кластерное ПО Veritas Cluster Server (VCS), которое на данный момент является, пожалуй, наиболее функционально развитым решением на рынке. Надежность функционирования также обеспечивают и другие компоненты VxSF — менеджер томов, файловая система и т.д.

Наша компания обладает обширным опытом по внедрению и эксплуатации программного пакета Veritas Storage Foundation. Многим нашим заказчикам мы рекомендуем использовать его как решение по управлению хранением данных для всего парка серверов (это позволяет стандартизировать методы и интерфейсы управления). Широкие, постоянно увеличивающиеся функциональные возможности VxSF, качественная поддержка продукта, отлаженный код обеспечивают при его применении высокую надежность и отказоустойчивость практически на всех уровнях ИТ-инфраструктуры вычислительных комплексов.

Смотрим на состав

Рассмотрим подробнее основные компоненты, входящие в VxSF. **Менеджер томов Veritas Volume Manager** (VxVM) и **файловая система Veritas File System (VxFS)** являются «главными скрипками» пакета VxSF и представляют собой фундамент, на котором строятся остальные функциональные возможности продукта.

VxVM — это менеджер логических томов, который обеспечивает представление на сервере логических объектов, соответствующих физическим дисковым устройствам. После того как устройства вводятся под управление VxVM, над ними строятся объекты — subdisk, plex, volume, disk groups и т.д. Именно благодаря такой структуре и достигается гибкость в настройке и применении менеджера томов. Так, VxVM позволяет собирать тома, состоящие из регионов разных физических дисков, и тома различной геометрии (concat, stripe), зеркалировать их между разными дисками, в том числе между физическими массивами, и др. Объединение томов в общие дисковые группы по заданному логическому критерию позволяет управлять ими как единым целым, например, в две команды перемещать между разными узлами тома, на которых размещаются все данные какой-либо системы. VxVM активно используется многими нашими заказчиками для замены встроенных в ОС штатных решений, таких как SVM в Solaris или LVM в AIX, которые предоставляют сравнительно ограниченную функциональность.

Veritas File System является высоконадежной журналируемой файловой системой, заточенной под большие объемы данных и обеспечивающей высокую производительность. Выполнение любой транзакции предварительно записывается в служебную область файловой системы — журнал, после чего непосредственно производится сама операция. Журналирование позволяет в случае сбоя гораздо быстрее и с большей вероятностью восстановить все данные файловой системы. Еще одним преимуществом VxFS является использование extent'ов переменной длины для выделения места под файлы (в отличие от традиционных фиксированных блоков). Это позволяет более эффективно размещать файлы и снижает фрагментацию файловой системы при записи. Применение нашими заказчиками Veritas File System в совокупности с VxVM вместо встроенных файловых систем в ОС UNIX обусловливается их большей производительностью и надежностью работы.

Другая значимая опция пакета VxSF — решение по управлению путями подключения серверов к дисковым массивам — **Veritas Dynamic Multipathing** (VxDMP), которое также может приобретаться как отдельный продукт. Если существует несколько путей подключения серверов к массивам через SAN, VxDMP осуществляет балансировку нагрузки трафика ввода-вывода по ним, а также перевод трафика между путями в случае выхода одного из них из строя. VxDMP поддерживает дисковые массивы практически всех производителей и имеет встроенные модули под каждый из них. При этом решение не зависит от применяемой файловой системы или менеджера томов. Таким образом, использование VxDMP экономит средства компании (не нужно приобретать дополнительные решения от производителя массивов) и позволяет создавать multi-vendor environment.

В целом VxVM, VxFS и VxDMP являются той базой, которую применяют практически все наши заказчики, выбирающие для себя Veritas Storage Foundation. Зачастую использование этих компонентов является стандартной практикой для всех эксплуатируемых серверов, в том числе и для наиболее критичных бизнес-систем.

Широкораспространенным продуктом из состава редакции Veritas Storage Foundation High Availability является **кластерное**

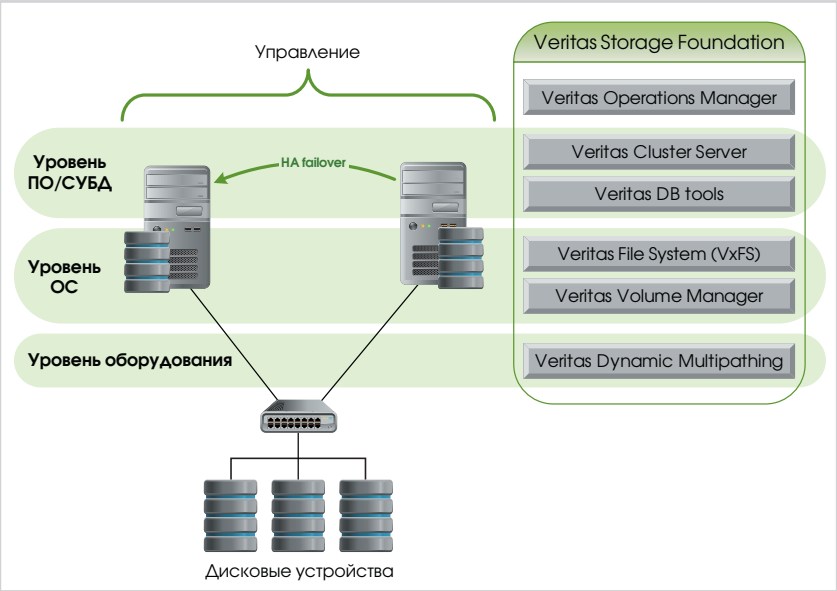


Рис. 1. Логическая структура основных компонентов Veritas Storage Foundation

ПО Veritas Cluster Server (VCS). VCS может поставляться и как отдельный продукт в случае, если заказчику требуется только его функциональность. Кластер предназначен для обеспечения высокой готовности и отказоустойчивости функционирования бизнес-приложений компании. VCS обеспечивает мониторинг и управление всеми элементами системной инфраструктуры ОС и сервера, необходимыми для работы приложения или СУБД. В случае сбоя одного из ресурсов либо сервера целиком VCS переводит выполнение системы на резервный сервер. Помимо обеспечения высокой готовности, кластер гарантирует простоту администрирования приложения. Так, переключение БД Oracle и всех сопутствующих ресурсов на резервный узел может быть произведено за несколько минут по одной команде администратора, в то время как без кластера специалист должен выполнять эти действия вручную.

Основными преимуществами VCS относительно других решений по кластеризации являются гораздо более широкие функциональные возможности (значительное число встроенных агентов, поддержка различных приложений и СУБД), поддержка большого количества кластерных конфигураций и топологий (включая режимы Active/Active, географически распределенные кластеры и т.д.), а также простота в настройке и администрировании. Как уже говорилось, все компоненты VxSF интегрированы между собой, таким образом, возможно совместное использование стека VxVM – VxFS – VCS.

За последние несколько лет мы реализовали множество проектов по построению отказоустойчивых решений с использованием VCS. Этот продукт наиболее востребован для систем, которые требуют высокой надежности, управляемости и отсутствия/минимизации простоев. Понятно, что подобные системы есть у заказчиков из практически любой отрасли бизнеса. Так, один из наиболее интересных проектов был реализован нами в одном из крупнейших российских банков. Он предусматривал построение 3-узлового кластерного комплекса, располагающегося на двух разных площадках, которые территориально удалены друг от друга. На узлах кластера размещались как продуктивный экземпляр процессинговой АБС, так и ее реплика, используемая для отчетности. Широкая функциональность и возможность гибкой настройки VCS позволили решить все задачи заказчика. Была обеспечена заданная логика переключения продуктивного и отчетного экземпляров АБС между узлами кластера на одной и между площадками с приоритетом для продуктивного экземпляра. Также было настроено автоматическое обновление адресации узлов в DNS домене банка для обеспечения непрерывного доступа клиентов к АБС в случае переключения кластера между площадками.

Одна из возможных опций кластерных редакций VxSF – **кластерная файловая система Cluster File System** (CFS), которая функционирует на базе кластерного же менеджера томов – Cluster Volume Manager (CVM). Подобная конфигурация позволяет нескольким узлам кластера монтировать файловую систему, размещаемую на внешнем дисковом массиве, и одновременно работать с ней. Для таких решений по параллельным кластерам СУБД, как Oracle RAC и Sybase ASE CE, Symantec предлагает специализированные редакции пакета VxSF.

Cluster File System востребована нашими заказчиками в параллельных кластерах СУБД, в кластере из нескольких экземпляров web-серверов и т.д. В качестве примера можно привести проект внедрения Oracle Siebel CRM в крупной компании-ритейлере. Серверы БД Siebel функционируют в кластере Oracle RAC, благодаря чему обеспечивают балансировку нагрузки между его узлами, а также восстановление сессий в случае сбоя одного из них. Для реализации этого кластера было использовано ПО Veritas Storage Foundation for Oracle RAC. Применение кластерных менеджера томов и файловой системы позволило обеспечить возможность одновременной работы экземпляров БД на разных серверах с одним набором данных, а использование Veritas Cluster Server – мониторинг и

контроль элементов системной инфраструктуры серверов.

Veritas Cluster File System оптимальна для применения в сложных и комплексных проектах, в которых требуется параллельный доступ к данным (банковские системы, CRM и т.д).

В деле

Рассмотрим подробнее некоторые из задач, решение которых становится возможным или значительно упрощается благодаря использованию средств VxSF. Одна из них — безостановочная миграция данных продуктивной системы между двумя дисковыми массивами. Применение средств зеркалирования **Veritas Volume Manager** позволяет безболезненно выполнить подобную миграцию. Добавив в структуру тома диски с другого физического массива путем создания второго плекса, зеркалирование информации можно начать автоматически. При этом нагрузка остается минимальной, и в целом для приложения этот процесс происходит прозрачно. По окончании зеркалирования плекс с первого массива просто удаляется, и приложение продолжает работать с данными — без каких-либо перерывов и уже на новом массиве. В то же время без применения VxSF это был бы гораздо более сложный процесс, включающий в себя ручное копирование и остановку приложения.

Отметим, что эта технология широко применяется нами у многих заказчиков в проектах внедрения новых дисковых массивов, которые заменяют устаревшее оборудование. Один из последних примеров — замена трех морально устаревших массивов Sun FLX380 на новый HDS AMS уровня Mid-Range. В ходе проекта было проведено обследование систем, дисковые ресурсы которых размещались на старом оборудовании, после чего составлен план работ по миграции. На финальной стадии системы были последовательно переведены на новый массив. При этом миграции проводились в рабочее время без остановки систем и были «прозрачными» для приложений.

Еще одна задача, выполнение которой значительно упрощается благодаря VxSF, — кросс-платформенная миграция данных. Она актуальна, когда нужно перенести информацию на другую ОС, например, с Sun Solaris на IBM AIX, либо в целом на другую платформу — с Unix на Linux x86. Как уже отмечалось ранее, VxSF поддерживает все основные платформы и операционные системы. Для поддержки такого широкого набора платформ разной архитектуры в решении применяется технология Portable Data Containers. При добавлении новых дисковых устройств под управление Veritas Volume Manager им по умолчанию присваивается CDS-формат. Формат обеспечивает такую структуру хранения данных на диске, что он может быть импортирован на любую платформу: AIX, Solaris, HP-UX, Linux. Файловая система при этом обеспечивает возможность доступа к файлам на этих дисках из разных ОС.

Эти опции мы эффективно использовали в проекте с одним из наших заказчиков из телекоммуникационной сферы. Осуществлялась замена устаревшего оборудования платформы Sun/Solaris на современные серверы линейки IBM Power/AIX с миграцией БД Oracle. И на существующем, и на целевом серверах было установлено VxSF, и дисковые ресурсы находились под управлением Veritas. После остановки продуктивной БД с использованием средств Portable Data Containers дисковые ресурсы были в несколько команд отключены от сервера Sun и подключены к оборудованию IBM. Нам осталось провести конвертацию БД Oracle на новую платформу — и система была запущена в эксплуатацию на новом оборудовании.

Возможность создания копий данных — одна из наиболее востребованных функций VxSF, которая реализуется **опцией Veritas FlashSnap**. Этот пакет предоставляет большой выбор возможных типов создания мгновенных копий (так называемых point-in-time copy, или SnapShot), и заказчик может подобрать вариант, подходящий именно под его задачи. Копии данных могут обрабатываться как на исходном, так и на любом другом сервере и имеют самое разнообразное применение: для отчетности или в системах принятия решений, для создания резервных копий (в том числе так называемых off-host backup), для тестирования и отладки, обеспечения защиты целостности БД от логических ошибок и т.д. Отличительная особенность копий данных — их создание в режиме online, без необходи-

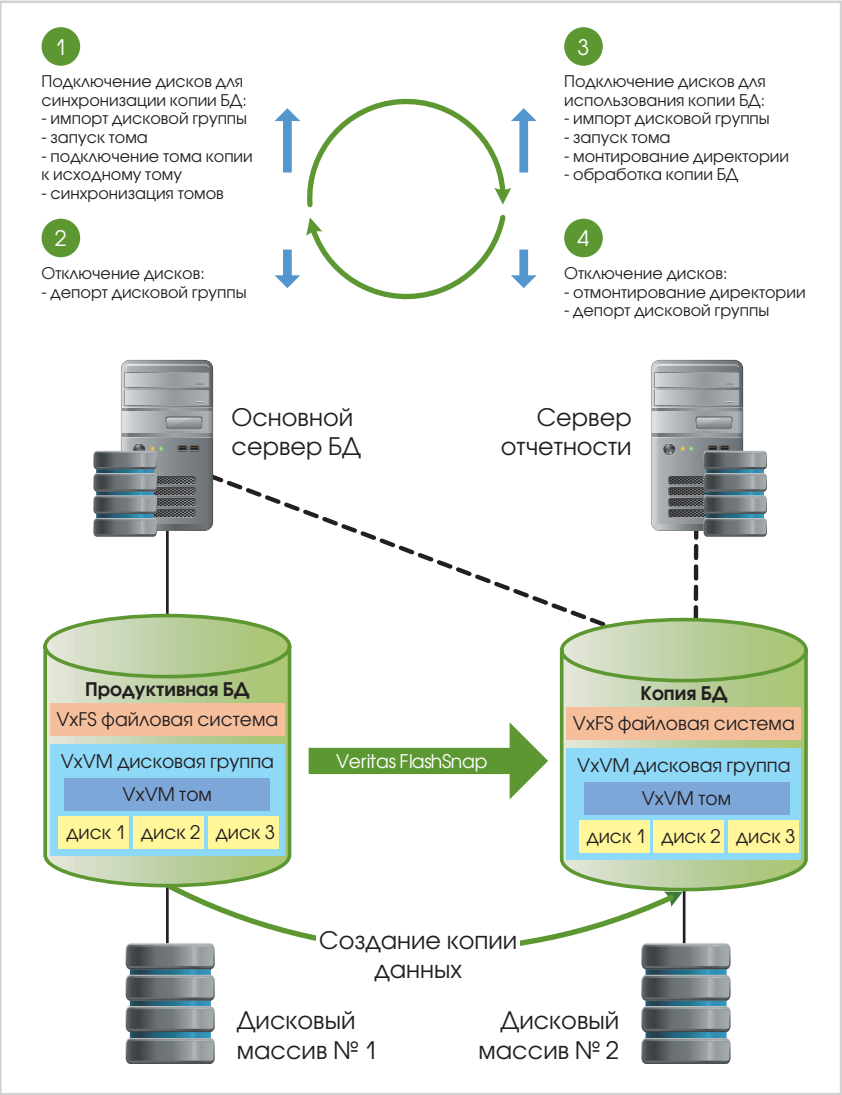


Рис. 2. Схема создания копии БД с использованием Veritas FlashSnap

мости остановки исходного тома. Более того, большая часть видов копий доступна немедленно после их инициализации, нет необходимости ждать окончания процесса репликации.

Наша компания реализовала довольно много проектов, в которых используются те или иные виды копий данных, создаваемые средствами VxSF. В том числе можно назвать проект создания ежедневной копии БД системы биллинга абонентов у одного из российских операторов связи. Эта копия используется в системе отчетности. Процесс ее создания настроен на запуск по расписанию в автоматическом режиме раз в сутки. Том Veritas Volume Manager, содержащий копию БД, подключается к исходному тому с продуктивной базой данных, и все изменения за сутки синхронизируются. После этого том с актуальной копией подключается к выделенному серверу отчетности. Копия БД создается в ночное время, без остановки продуктивной базы данных, и доступна к началу рабочего дня.

Не обязательно, но…

Вкратце отметим наличие различных опций, которые предлагаются Symantec для работы под разными СУБД. Например, для СУБД Oracle предлагаются так называемые «ускорители» — опции Veritas Extention for Oracle Disk Manager, Veritas Cached Oracle Disk Manager, Veritas Quick I/O и т.д., которые позволяют увеличить производительность работы системы управления базами данных. Они активно используются у многих наших крупных заказчиков, в том числе в телекомах и банках, т.к. позволяют обеспечить производительность файловых систем на уровне RAW-устройств. Veritas Oracle Disk Manager одинаково хорошо подходит для баз данных с различным характером нагрузки — как OLTP, так и DWH, поэтому выбран многими компаниями в качестве опции, которая включается по умолчанию для каждой БД Oracle.

Еще одна опция — Smart Storage Tiering, которая позволяет в автоматическом режиме перемещать востребованные данные на более производительные диски. Один из наших заказчиков применил эту технологию для более экономичного размещения 10-терабайтной БД на дисковых массивах. Было создано 2 типа хранилища: раздел хранения оперативных (за последние 6 месяцев) и архивных данных (за 30 месяцев). Первый тип размещается на массиве уровня Hi-End, а второй — на Mid-Range. При создании новых файлов в БД они находятся в разделе хранения оперативных данных. По мере их устаревания Smart Storage Tiering в автоматическом режиме осуществляет копирование файлов данных в архивное хранилище. Копирование идет фоном, с пониженным приоритетом и в прозрачном режиме, что не сказывается на производительности или работе системы в целом.

Контролируй, управляя

Естественно, как и в случае с любым другим комплексным продуктом встает вопрос об управлении всеми его функциями и опциями. Каким образом обслуживающие подразделения могут управлять VxSF? Тем более если этот пакет решений применяется в масштабах всего дата-центра на разных платформах? Symantec предлагает единую централизованную графическую **консоль управления продуктами семейства VxSF – Veritas Operations Manager**. Используя VOM, администраторы могут осуществлять мониторинг и управление объектами VxSF, а также составлять различные аналитические отчеты.

VOM имеет классическую архитектуру «клиент – сервер», где сервером обычно является выделенная станция (Management Server), а клиентами – агенты, инсталлируемые на всех хостах, которые должны быть в контуре управления VOM. Подключение к серверу управления осуществляется по HTTPS через web-браузер. Таким образом, используя один инструмент, администраторы могут централизованно решать все повседневные задачи по управлению ресурсами VxSF.

Рассмотрим на конкретном примере: у одного из наших заказчиков есть два Hi-End сервера IBM Power 795, которые разбиты на большое количество логических разделов. На каждой паре разделов реализованы кластерные конфигурации Veritas Cluster Server. Таким образом, в состав любого кластера входят два логических раздела, представленные как два физических узла. Для остановки одного сервера (например, с целью проведения работ по сервисному обслуживанию) администратору необходимо зайти на выделенную консоль каждого кластера и выполнить его переключение. Используя же консоль Veritas Operations Manager, администратор может осуществить переключение всех кластеров централизованно, что экономит время, а также минимизирует человеческий фактор.

В рамках одной статьи невозможно охватить весь функционал продукта VxSF, поэтому мы постарались сконцентрировать внимание на наиболее важных и востребованных в реальной эксплуатации опциях. В заключение отметим, что внедрение продукта VxSF позволяет эксплуатирующим подразделениям компаний значительно упростить администрирование и решение многих рутинных задач, таких как расширение файловых систем, перенос данных и т.д. Практически все отраслевые специалисты отмечают значительно большее удобство VxSF и относительную простоту работы с этим пакетом решений по сравнению с другими продуктами аналогичной функциональности.

Консолидированная вычислительная платформа банка КРЕДИ АГРИКОЛЬ

О ЗАКАЗЧИКЕ

ПАО «КРЕДИ АГРИКОЛЬ БАНК» — универсальный банк с иностранным капиталом, который представлен во всех сегментах рынка и предлагает качественные финансовые услуги как для бизнеса, так и для частных клиентов. В 2006 году банк стал частью одной из крупнейших финансовых групп в Европе — Credit Agricole (Франция). С этого момента начался новый масштабный виток его развития, который проявился в виде усовершенствования всех процессов и услуг. Сегодня региональная сеть банка КРЕДИ АГРИКОЛЬ покрывает все регионы Украины и насчитывает более 200 точек продаж. Решение своих финансовых вопросов банку доверили около 370 тыс. частных и более 25 тыс. бизнес-клиентов.

ПРЕДПОСЫЛКИ

Каждый региональный филиал банка работал как отдельное МФО, используя для этого локальную автоматизированную банковскую систему (АБС), позволяющую в режиме реального времени управлять деятельностью всех отделений, а также формировать необходимую финансовую и управленческую отчетность только этого филиала. Данные из АБС филиалов ежедневно реплицировались в центральный офис, где производилась их обработка и формирование обязательной финансовой отчетности для предоставления в Национальный Банк и другие регулятивные органы Украины на уровне всего банка. Для оптимизации работы филиальной сети, повышения ее управляемости, мобильности и конкурентоспособности на рынке банковских услуг руководством группы Credit Agricole было принято решение централизовать банк путем перевода всех региональных филиалов на работу с единым МФО. Для решения поставленной задачи необходимо было осуществить объединение всех региональных АБС на единой вычислительной платформе.

ЗАДАЧИ

Основной задачей для банка была разработка новой единой вычислительной платформы. Задача была разделена на несколько основных направлений деятельности: разработку новой архитектуры АБС, выбор для нее аппаратной платформы, проработку изменившегося ИТ-ландшафта банка с учетом централизации всех основных бизнес-процессов.

РЕШЕНИЕ

По результатам проведенного тендера разработчиком архитектурного решения для аппаратной платформы новой АБС была выбрана компания «Инфосистемы Джет». Компания предложила наиболее эффективное решение как с технической точки зрения, так и с точки зрения начальной стоимости и эксплуатационных расходов.

На начальном этапе проекта не было четких представлений о необходимой производительности аппаратной платформы. Для оценки оптимальных параметров системы инженеры компании «Инфосистемы Джет» в тесном сотрудничестве с разработчиками АБС заказчика провели несколько серий нагрузочных тестов с целью определить необходимую вычислительную мощность. Компания «Инфосистемы Джет» предоставила

заказчику достаточно мощную тестовую аппаратную платформу для проведения как нагрузочных тестов с использованием реальных данных, так и тестирования модулей новой разрабатываемой АБС. Анализ полученных результатов позволил сформулировать требования по целевой производительности платформы.

Для обеспечения непрерывности бизнеса и минимизации рисков при внедрении централизованной системы одновременно решались важные задачи по обеспечению высокой доступности сервисов АБС и созданию консолидированного катастрофоустойчивого комплекса.

С учетом всех этих требований специалисты компании «Инфосистемы Джет» спроектировали бесконфликтную мультивендорную систему, состоящую из двух территориально удаленных друг от друга площадок (основной и резервной) с повторяющимся набором оборудования на них.

В качестве аппаратной вычислительной платформы было выбрано оборудование компании Oracle Hardware.

Система хранения данных была размещена на массивах Hi-End класса Hitachi Data Systems (HDS USP-VM). Для интеграции вычислительного комплекса с СХД был выбран пакет решений Symantec Veritas Storage Foundation. На выбор данного ПО повлияли следующие важные характеристики:

- гибкое управление;
- прозрачность процессов;
- возможность одновременного ведения нескольких процессов за счет оптимального распределения дискового пространства.

«Изначально мы планировали использовать под миграцию оборудования технологическое окно сразу двух майских праздников – выходные 1 и 9 мая, – рассказывает **Александр Зачешигрива, коммерческий директор филиала компании "Инфосистемы Джет" на Украине**. *– Благодаря активному участию в процессе специалистов ИТ-службы банка мы смогли значительно сократить время переноса техники – уже за первые три дня нам удалось раскоммутировать более двух десятков серверов, перевезти их на новое место, а затем собрать в нужной конфигурации и запустить. Сложность при этом заключалась в том, что необходимо было не просто перевезти и скоммутировать оборудование, а собрать, по сути, новую площадку с изменившимся набором оборудования».*

Кроме того, благодаря динамической балансировке нагрузки Symantec Veritas Storage Foundation позволяет достичь большей производительности, обеспечивает требуемую доступность дисковых ресурсов и защиту сервиса от сбоев. Также с использованием данного ПО был создан высокопроизводительный и отказоустойчивый файловый сервер, представляющий собой кластер, территориально разнесенный между площадками.

Еще одним масштабным проектом стало внедрение новой системы резервного копирования. На сегодняшний день на каждой площадке имеется полный набор резервных копий всех необходимых данных. Это позволит возобновить работу всех систем на любой из площадок в случае каких-либо нештатных ситуаций.

В процессе внедрения аппаратной платформы банк решил выполнить физический перенос и логическую реорганизацию своей резервной площадки. У банка уже была резервная площадка, но она не в полной мере соответствовала современным требованиям. В итоге площадку было решено расформировать, а актуальную техническую базу перенести на новый «резерв».

Учитывая большой объем работ по демонтажу и последующему монтажу на новой площадке, а также недопустимость простоев систем даже на один час, было принято решение выполнить работы по переводу оборудования и систем со старой резервной площадки на новую в майские праздники 2010 года.

Задача защищенности сервиса от потери основной площадки была решена за счет фактической удаленности элементов распределенного ЦОД. Помещение под резервный ЦОД выбиралось таким образом, чтобы в случае катастрофы или стихийного бедствия площадки находились друг от друга на безопасном расстоянии. Кроме того, каждая

площадка локально защищена в соответствии с требованиями Национального Банка Украины.

РЕЗУЛЬТАТ

В результате реализации этого проекта банк получил оптимальную платформу для своей АБС – распределенный центр обработки данных, состоящий из двух независимых площадок: основной и резервной. Благодаря обновлению оборудования удалось решить ряд важнейших задач: обеспечить бесперебойную работу и надежную защиту сервиса по обработке данных, минимизировать затраты на техническое обслуживание системы и снизить расход электроэнергии. Использование резервного хранилища позволило создать дополнительную защиту сервиса АБС на случай непредвиденных сбоев в работе, стихийных бедствий и других форс-мажорных обстоятельств.

Активное непосредственное участие разработчиков АБС и специалистов департамента ИТ банка на всех стадиях внедрения решения позволило выполнить этот комплексный проект в сжатые сроки, с высоким качеством и без малейших простоев в работе.

РАЗВИТИЕ ПРОЕКТА

Специалисты компании «Инфосистемы Джет» разработали модель технической поддержки, позволяющую комплексно обслуживать мультивендорную ИТ-инфраструктуру банка. В область ответственности интегратора входят дисковые массивы HDS, ПО Symantec, серверное оборудование и ленточные библиотеки Oracle Hardware. Техподдержка осуществляется по программе «Операционная поддержка 24x7», обеспечивая максимальную доступность ИТ-сервисов банка без праздников и выходных.

Специалисты интегратора осуществляют консультирование по «горячей линии» поддержки, ремонт и замену неисправных компонентов оборудования, восстановление работоспособности оборудования и ПО, предоставление новых версий программного обеспечения, программных коррекций и отчетности. Но самое важное – это проактивная поддержка, позволяющая выявлять проблемы на стадии их образования и проводить превентивные действия по их предотвращению.

Разработанная для банка программа технического обслуживания и поддержки позволила снизить количество инцидентов, минимизировать время простоя оборудования и ПО и обеспечить быстрое восстановление его работоспособности.

«Проектное решение, реализованное специалистами компании "Инфосистемы Джет", гарантирует непрерывность работы ключевой системы банка – АБС. Качество обслуживания клиентов возросло, поскольку вся информация по банковским операциям хранится в единой системе. Это позволяет предоставлять необходимые услуги в любом из наших филиалов, независимо от того, в каком из них "прописан" клиент банка», – комментирует **Дмитрий Шейкин, заместитель директора департамента информационных технологий КРЕДИ АГРИКОЛЬ.**

«Мы уже отработали ряд похожих проектов в России, но для Украины это был первый опыт подобного внедрения. Основные сложности были связаны с географической распределенностью консолидируемых объектов, поскольку в зону покрытия сети банка входят все области Украины, а также со сжатыми сроками реализации проекта», – резюмирует **Владимир Резник, генеральный директор филиала компании «Инфосистемы Джет» на Украине**.

«Имея опыт сотрудничества с компанией "Инфосистемы Джет", мы доверили интегратору обслуживание критичного для бизнеса банка оборудования и системного ПО. Таким образом, мы смогли обеспечить непрерывность работы основной информационной системы банка, сведя к минимуму риски ее простоя», – отметил **Сергей Проценко, директор департамента информационных технологий банка КРЕДИ АГРИКОЛЬ**.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Главный редактор: Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01 факс (495) 411 76 02
e-mail: JetInfo@jet.msk.su *http://www.jetinfo.ru*

Подписной индекс по каталогу Роспечати **32555**

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем