Почтовые системы: CDP-доступность для любых компаний

Обзор функциональных особенностей решения Acronis® Recovery для Microsoft Exchange, появившегося на рынке в конце ноября 2008 г.

Введение

Рынок программных решений для почтовых систем, позволяющих оптимизировать доступность и процедуры резервного копирования/восстановления (РКВ), привести их в соответствие регулирующим отраслевым и законодательным нормам, консолидировать их с ПО управления всеми корпоративными записями и др. стремительно развивается.

По прогнозам Gartner ("Dataquest Insight: E-Mail Archiving Software Market, Worldwide, 2008"), только рынок ПО систем активного архивирования почтовых сообщений к 2012 г. вырастет до $1,7 млрд.

Это связано, прежде всего, с повышенной критичностью почтовых систем, недоступность которых даже в течение короткого времени может крайне негативно отражаться на бизнесе многих компаний – от небольших до самых крупных.

Классификация дополняющего ПО для почтовых систем

Все ПО, расширяющее базовую функциональность таких почтовых систем, как Microsoft Exchange, IBM Lotus Notes/Domino и др., можно разделить на 2 больших класса: 1) корпоративное с широким спектром функциональности активного архивирования, e-discovery, расширенного поиска и управления на основе политик всем контентом почтовых систем, консолидированного управления почтовым контентом и другими корпоративными записями и др. и 2) ПО, ориентированное на средние и небольшие компании, в основном оптимизирующее функции РКВ с точки зрения повышения их производительности до уровня корпоративного класса. Данное разделение можно еще классифицировать по типам поддерживаемых серверных платформ, в частности, виртуальных активно набирающих свою популярность в последнее время.

Представленные 2 класса ПО, помимо функциональных отличий, имеют разную политику лицензирования. Как правило, системы первого класса имеют сложные политики и, в основном, лицензируются по числу почтовых ящиков, стоимость которых лежит в диапазоне от $10 долл. до нескольких сотен за один ящик в зависимости от их общего числа множества сопутствующих параметров (числа поддерживаемых БД/серверов, уровня сервиса, числа дополнительных модулей, особенностей управления и др.).

Системы второго класса более просты в лицензировании и, как правило, лицензируются по числу почтовых серверов. Если учесть, что, например, один восьмиядерный Windows сервер может поддерживать до 2 000 почтовых ящиков, то разница в стоимости может ,snm значительной – менее $0,5 за ящик, однако цена этому – меньшие возможности.

В современных условиях для бизнеса крайне важно еще и то обстоятельство, чтобы при развитии компании была возможность гибкого масштабирования дополняющего функционал почтовых систем до необходимого уровня по мере роста компании при минимальных первоначальных вложениях.

В соответствии с приведенной выше классификацией, решение Acronis Recovery для Microsoft Exchange (ARME) относится к ПО второго класса. Его отличительной особенностью является то, что оно позволяет с любой гранулярностью (сообщение, папка, ящик, группа папок/ящиков, сервер) восстанавливать компоненты почтовой системы с показателем RTO (Recovery Time Objective – максимально допустимое время восстановления работоспособности приложения) в пределах от нескольких десятков секунд до 1 часа и показателем RPO (Recovery Point Objective – средний период времени, в течение которого можно позволить потерю данных, или как часто должны выполняться резервные копии работающих приложений), поддерживаемым в режиме непрерывной защиты данных – по CDP-технологии (Continuous Data Protection).

Для большинства начинающих и в ряде случаев уже "зрелых" компаний этого может оказаться вполне достаточно с учетом базового функционала почтовых систем с точки зрения поддержания их доступности и решения ряда задач в целях соответствия регулирующим требованиям.

Архитектура Microsoft Exchange Server

Корпоративный выпуск Exchange Server 2007 поддерживает до 50 групп хранения и до 50 баз данных на каждый сервер (рис. 1). Можно настроить до 5 баз данных в каждой группе хранения и до 50 баз данных в сумме. Теперь данные почтовых ящиков можно распределить в большем количестве баз данных, а базы данных почтовых ящиков – в большем количестве групп хранения по сравнению с предыдущими версиями Exchange Server. Стандартный выпуск Exchange Server поддерживает до пяти групп хранения и пять баз данных на сервер. И корпоративный, и стандартный выпуски имеют неограниченный объем баз данных. Таким образом, отдельная база данных в Microsoft Exchange – это всего лишь зависимая часть группы хранения, создание ее индивидуальной резервной копии не имеет смысла, т. к. не гарантирует сохранения целостности данных после восстановления.

ARME – это инструмент, создающий копии необходимых таблиц, данных и

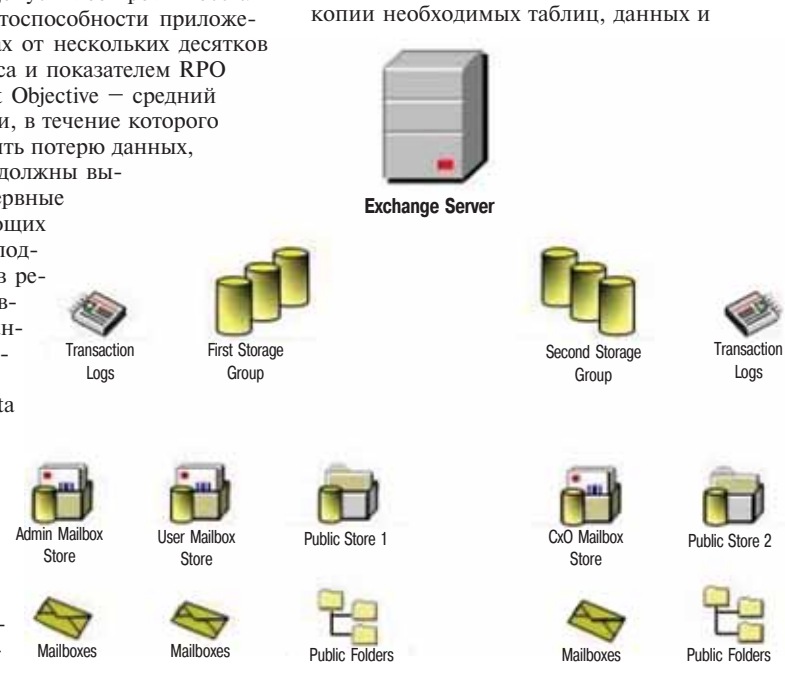

Рис. 1. Корпоративный выпуск Exchange Server 2007 поддерживает до 50 групп хранения и до 50 баз данных на каждый сервер.

объектов, выбранных пользователем, и работающий с базой данных не только как с набором файлов. Когда процедура резервного копирования начата, Acronis Recovery для MS Exchange завершает все активные транзакции, создает моментальный снимок базы данных и немедленно возобновляет транзакции. Продолжительность состояния незанятости базы данных минимальна – резервная копия сохраняется в свое местоположение, в то время как база данных продолжает работать.

Приложение Microsoft Exchange Server – это система обмена сообщениями, которая широко используется в больших и в малых организациях, и поэтому обладает масштабируемостью в обоих направлениях. Однако новые требования к обмену сообщениями – такие как совместимость, безопасность и отказоустойчивость – вызвали необходимость появления новой системы обмена сообщениями, надежно работающей как на больших, так и на малых предприятиях.

Microsoft Exchange Server предоставляет полнофункциональную систему обмена сообщениями, которая может работать на одном сервере. Это значит, что все службы Exchange располагаются на одном сервере, как в продукте Microsoft Small Business Server. Однако при этом имеются значительные преимущества для операций развертывания, управления и обеспечения безопасности, появившиеся благодаря гибкой модульной системе, которую можно установить на нескольких машинах. Можно настроить Microsoft Exchange Server 2003 вручную, создав требуемые роли сервера. Выбор роли сервера обеспечивает установку только необходимых служб и компонентов. Всего ролей может быть пять:

- *роль сервера клиентского доступа* – подобно внешнему серверу в более ранних версиях Microsoft Exchange Server, этот сервер перенаправляет интернет-трафик клиента надлежащему серверу почтовых ящиков;
- *роль сервера почтовых ящиков* – эта роль обслуживает почтовые ящики пользователей, хранящихся в базах данных, с которыми можно производить операции репликации и кластеризации;
- *роль транспортного сервера-концентратора* – эта роль предоставляет внутреннюю маршрутизацию всех сообщений от пограничных серверов, серверов единой системы обмена сообщениями или между двумя пользователями одной и той же базы данных почтовых ящиков. Эта роль также применяется там, где политика обмена сообщениями используется для сообщений, пересылаемых внутри организации и за ее пределы;
- *роль сервера единой системы обмена сообщениями* – позволяет проводить PBX интеграцию, чтобы производить доставку голосовой почты и факсимильных сообщений в почтовые ящики Exchange, и предоставляет приложению Microsoft Exchange Server функцию голосового предварительного набора номера;
- *роль пограничного транспортного сервера* – этот сервер располагается за пределами локальной сети и обеспечивает безопасность сообщений электронной почты на стороне клиента, а также антивирусную защиту и службу фильтрации нежелательных сообщений для Microsoft Exchange Server.

ARME позволяет производить резервное копирование только роли сервера почтовых ящиков.

Функциональные особенности Acronis Recovery для Microsoft Exchange

В стандартную конфигурацию ARME (рис. 2) входят: консоль управления, агент и сетевое устройство хранения, в качестве которого может выступать локальный жесткий диск; сетевой ресурс – SAN, NAS; FTP-сервер; ленточные носители, автозагрузчик, ленточная библиотека.

Агент ARME ориентирован только на поддержку приложения Microsoft Exchange Server 2007/2003/2000 (стандартный/корпоративный выпуск), работающего под управлением MS Windows ОС – Windows 2000 (SP4 Rollup 1), Windows Server 2003 (32-битная или 64-битная версии), Windows 2008 Server.

Методы резервного копирования ARME

ARME может выполнять полное и инкрементное резервное копирование для всеобъемлющей защиты данных в случае отказа оборудования, ошибок пользователя или даже природных катаклизмов. При *полном* резервном копировании в архив включаются все данные, имеющиеся на момент его создания. Можно восстановить полную базу данных путем ее восстановления из полной резервной копии в выбранное местоположение. Необходимая часть журнала транзакций включается в резервную копию, что позволяет возвратить базу данных к моменту времени, когда архивация завершилась. При восстановлении базы данных происходит откат незавершенных транзакций. Восстановленная база данных соответствует состоянию исходной базы данных (когда создание архива завершилось), но без незавершенных транзакций.

Для небольшой базы данных, которую можно архивировать быстро, удобно использовать только полное резервное копирование. Однако, если база данных увеличивается, полные ее копии создаются дольше и требуют больше дискового пространства. Поэтому для больших баз данных больше подходит полное резервное копирование с инкрементными копиями. Полная резервная копия может быть основой последующего инкрементного копирования, ее можно также использовать как самостоятельный архив.

Инкрементная резервная копия хранит все транзакции и изменения базы данных, внесенные каждой транзакцией с момента создания последнего полного или инкрементного архива. Журнал транзакций является ключевым компонентом базы данных и при сбое системы помогает возвратить базу данных в прежнее рабочее состояние. Файл журнала транзакций имеет фиксированный размер и автоматически созданное имя. После создания инкрементной резервной копии журнал транзакций сокращается.

Для выбора подходящего метода (или методов) резервного копирования, необходимо обозначить требования к имеющимся данным и применить соответствующую стратегию. Стратегия создания полной резервной копии определяет способ и периодичность создания копий, а также тип и емкость аппаратного обеспечения, необходимого для размещения архива.

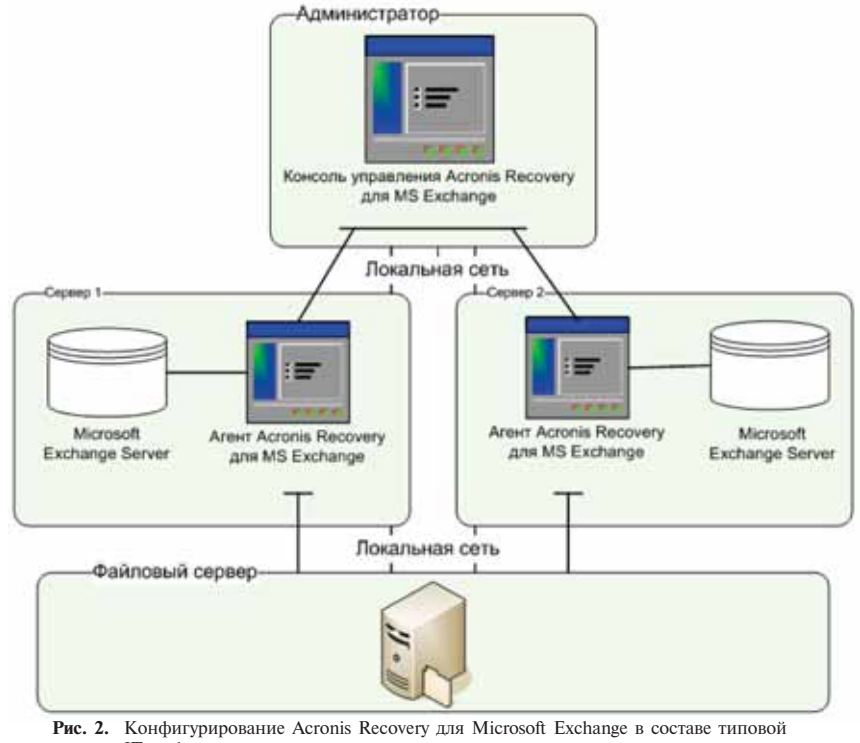

Рис. 2. Конфигурирование Acronis Recovery для Microsoft Exchange в составе типовой IT-инфраструктуры.

Стратегии создания резервных копий

В качестве стратегии резервного копирования можно выбрать следующие варианты:

- запланировать задание на резервное копирование с помощью ARME;
- определить стратегию вручную;
- использовать технологию непрерывной защиты данных – CDP;
- создать резервную копию сразу.

При создании задания по архивации с использованием технологии CDP можно запланировать создание только полных архивов. ARME контролирует папки, содержащие архивированные журналы, и производит резервное копирование всех новых журналов в архив CDP. Архив CDP содержит набор полных резервных копий и журнал архива, созданный после последнего полного архива. Поэтому можно восстановить данные в состояние последнего полного архива или в состояние имеющихся журналов резервного копирования, хранящихся в архиве CDP. После создания нового полного архива журнал CDP будет сокращен.

Задание по непрерывной защите данных выполняется двумя способами: в составе обычного сценария задания и в реестре. Формат такого задания в реестре известен только службе CDP (CDP-агенту). Поэтому для изменения или удаления задания по непрерывной защите данных из консоли управления ARME необходимо также наличие запущенной службы CDP (технология CDP не может использовать для резервирования данных ленты и FTP).

Стратегии резервного копирования, отличные от CDP, выполняются на основе создаваемого плана задач резервного копирования, которые могут состоять из двух подзадач: создание полного или инкрементного архива (журнала транзакций). Этими подзадачами можно управлять по отдельности.

При определении стратегии резервного копирования следует учитывать множество факторов: показатели RPO/RTO, размер базы данных, частота обращений к БД и др. Пример плана заданий с учетом ее размера и частоты обращения может быть следующим (по рекомендациям Acronis, *прим. ред.*):

- *низкая или средняя активность базы данных*:
  - создание полного архива раз в неделю;
  - архивация журнала транзакций каждые 12 часов;
- маленький или средний размер базы данных при высокой активности:
  - создание полного архива раз в два дня;
  - архивация журнала транзакций каждые 10 минут;
- большой размер базы данных при высокой активности:
  - создание полного архива раз в неделю;
  - архивация журнала транзакций каждые 10 минут.

Табл. 1. Стратегии резервного копирования в соответствии с требованиями к скорости операции и объему архива.

Период изменения данных	Метод резервного копирования	Быстродействие	
		Быстрое архивирование и наименьший размер архива	Быстрое восстановление и наибольший размер архива
Час	Полный	Неделя	День
	Инкрементный	1 час	1 час
День	Полный	Неделя	День
	Инкрементный	12 часов	12 часов

Пример возможных стратегий резервного копирования с учетом требований к показателям RPO/RTO и объема архива приведен в табл. 1.

С целью минимизации времени восстановления предусмотрена возможность создания консолидированных архивов из полной копии и инкрементальных во время наименьшей загруженности хранилища архивов (например, в воскресенье, ночью). В этом случае консолидированный архив при возникновении сбоя сразу (или почти) готов для проведения процедуры восстановления.

Процедуры создания резервных копий имеют еще две полезные опции. *Во-первых*, все РК стандартно могут сжиматься, что позволяет экономить от 50% до 90% объема занимаемого дискового пространства при незначительном увеличении времени при процедурах РКВ.

Во-вторых, чтобы освободить часть ресурсов сети для других процессов можно ограничить пропускную способность сети, используемую при резервном копировании. Это задается максимальным значением скорости передачи данных при выполнении процедур РКВ.

Процедуры восстановления данных

ARME предлагает четыре способа восстановления данных:

- *восстановить на точку сбоя* – данные будут восстановлены в состояние на момент сбоя. Для восстановления в точку сбоя, последовательность логов, а также вновь созданные файлы журнала (включая текущий журнал) должны быть доступны в выбранном местоположении. В противном случае будет доступно только восстановление к моменту создания последней резервной копии;
- *восстановить на момент последнего резервного копирования* – восстановление данных в состояние, когда создавалась последняя резервная копия (процедура работает быстрее, чем предыдущая);
- *восстановить на указанный момент времени* – ARME позволяет выбрать дату и время для восстановления состояния данных, имевшегося в этот момент времени (при использовании CDP-технологии);
- *восстановить из указанной резервной копии* – позволяет выбрать архив, из которого необходимо произвести восстановление.

При выполнении процедур восстановления можно уточнить элементы для восстановления – почтовые ящики, общие папки, отдельные или группа сообщений.

Помимо этого, ARME предоставляет два специальных способа быстрого восстановления – опция на основе использования функции Acronis Active Restore и опция аварийного восстановления.

При *использовании опции Acronis Active Restore* доступ к серверу Microsoft Exchange предоставляется немедленно. После запуска операции восстановления архивированная база данных подключается из архива напрямую. Затем используется журнал транзакции, получаемый из архива. Важно, что при этом база данных становится доступной для пользователей в короткий срок, что позволит им работать со своими папками, календарями, сообщениями электронной почты. Все остальные данные будут восстанавливаться из архива в фоновом режиме. После завершения операции восстановления база данных будет подключена заново, что займет меньше минуты.

При использовании *опции/процедуры аварийного восстановления* пользователи могут отправлять или получать сообщения пока восстанавливаются другие данные (только в Microsoft Exchange Server 2007). Вся процедура может занять несколько часов. Режим аварийного восстановления можно использовать только при восстановлении данных из самого последнего архива.

Основным преимуществом использования аварийного восстановления является независимость операции от размера журнала и почти мгновенное получение доступа к службе электронной почты. Сначала создается временная незаполненная аварийная база данных. Затем Microsoft Exchange Server создает в этой базе данных новые почтовые ящики (с теми же идентификаторами, что и у старых). После этого пользователи могут начинать отправку и получение сообщений, но другие данные (такие как список контактов, правила, сохраненные сообщения, и т. д.) будут все еще недоступны.

Эта операция занимает две минуты или даже меньше. После восстановления базы данных в выбранное местоположение и использования журнала все восстановленные данные объединяются с новыми сообщениями электронной почты (отправленными или полученными во время аварийного восстановления), что позволяет привести почтовые ящики в актуальное состояние, при отключении базы данных всего на несколько минут. По завершении операции временные аварийные базы данных удаляются.

Сравнение процедур Acronis Active Restore и аварийного восстановления приведено в табл. 2.

Дополнительные особенности управления

ARME ориентировано на широкий спектр компаний, в штате которых не обязательно есть квалифицированные IT-специалисты. Это достигается, прежде всего, наличием в ARME простого интерфейса управления с оптимизированным множеством опций, а также:

- *централизованным управлением* – консоль управления ARME автоматиче-

Табл. 2. Сравнение процедур Acronis Active Restore и аварийного восстановления.

	Acronis Active Restore	Аварийное восстановление
Доступность MS Exchange при восстановлении	да	ограниченная
Восстановление общих папок	да	нет
Поддерживаемые выпуски MS Exchange	все	только MS Exchange 2007
Влияние размера журнала	да	нет

ски находит все серверы баз данных в сети и отображает их текущее состояние. Это позволяет легко управлять корпоративными ресурсами и процессами РКВ;

- *управлением ресурсами,* в частности, загрузкой процессора и пропускной способностью во время операций РК предотвращает замедление работы основных приложений;
- *аварийным восстановлением по инструкции* – предоставление плана аварийного восстановления баз данных с пошаговыми инструкциями этого процесса, что позволяет даже неподготовленным сотрудникам успешно выполнять все процедуры РКВ;
- *интеграцией с Acronis True Image Echo,* что позволяет полностью восстановить весь сервер (операционную систему и банк сообщений) на "голое железо" с помощью загрузочного носителя или из PXE;
- *простое администрирование* – интуитивный графический пользовательский интерфейс позволяет эффективно настраивать и применять профессиональные стратегии резервного копирования.

Заключение

Появление решений класса ARME с высокой гранулярностью восстановления и поддержкой технологии непрерывной защиты данных значительно расширяет спектр компаний, которые могут иметь корпоративный уровень доступности данных почтовых систем с перспективой дальнейшего развития их функциональности.

aQua-CryptoAll – ноутбук с шифрованием

Октябрь 2008 г. – Компании "Аквариус" и Aladdin представили aQua-CryptoAll — персональный ноутбук бизнес-класса Aquarius с системой защиты данных от Aladdin.

Появление такого решения вызвано необходимостью борьбы с ростом уровня угроз в сфере утечки конфиденциальной информации, хранящейся на мобильных носителях. В состав решения входит ноутбук Aquarius NE515 на базе Intel Centrino 2 с предустановленной и настроенной системой защиты конфиденциальной информации производства компании Aladdin — Secret Disk 4, в комплекте с защищенным носителем информации USB-ключом eToken NG-FLASH (flash-памятью объемом от 1 Гбайт до 4 Гбайт).

Решение aQua-CryptoAll предназначено для директоров и владельцев бизнеса, руководителей высшего и среднего звена, хранящих на своих ноутбуках и съемных носителях конфиденциальные данные и ценную информацию, а также для сотрудников компаний, работающих с персональными данными и с любой другой информацией, подлежащей защите.

Защищаемые данные на жестком диске ноутбука и съемных носителях всегда хранятся в зашифрованном виде. При чтении с зашифрованного диска происходит автоматическое и незаметное для пользователя расшифрование данных, а при записи на зашифрованный диск – их шифрование. Все операции первоначального шифрования и последующего перешифрования дисков проводятся в фоновом режиме с возможностью приостановки и продолжения операции в любое удобное время. Это обеспечивает быстрый запуск системы и не влияет на производительность компьютера.

Важным условием обеспечения защиты является раздельное хранение ноутбука и USB-ключа eToken. Но даже если вместе с ноутбуком произошла утрата eToken, дополнительным рубежом защиты данных будет являться персональный PIN-код. Входящий в состав комплекта USB-ключ eToken может быть также применен в любом приложении для дополнительной аутентификации.

Специализированная BI-платформа экономкласса

Октябрь 2008 г. – Корпорация Teradata объявила о выпуске нового решения специального семейства платформ – Teradata Extreme Data Appliance 1550, которое позволяет выполнять анализ данных объемом 50 и более петабайт с минимальными затратами.

Teradata Extreme Data Appliance – это специальная аналитическая платформа, предназначенная для узкой группы специалистов, которые занимаются анализом корпоративных данных. Она позволяет выполнять анализ исключительно больших объемов редко используемых данных, таких как статистика посещений сайтов, многолетняя нормативная документация, данные производственных процессов и результаты тестирования, сведения о перемещении RFID устройств и информация о трафике сотовых сетей.

Teradata Extreme Data and CDR Appliance – это новое экономичное решение с возможностями полной интеграции и анализа всех элементов телефонной связи, включая коммутацию, сообщения голосовой почты и пересылаемые данные, при неограниченной масштабируемости.

Это хранилище данных дает совершенно новый уровень детализации при решении корпоративных задач в нескольких областях: проектирование и эксплуатация сети, финансы, служба поддержки абонентов, маркетинг, система тарификации и защита от мошенничества. В дополнение к существующей технологии сжатия данных для хранилищ данных объемом более 50 Пбайт проходит тестирование решение Teradata Labs, которое должно повысить эффективность сжатия в 20 раз.

Teradata Extreme Data Appliance – это экономичная, полностью интегрируемая и масштабируемая платформа с четырехъядерным процессором Intel® Xeon® и вместительным хранилищем данных. Эта платформа поддерживает передовые приложения и базу данных Teradata 12 под управлением системы Novell® SUSE® Linux. Все компоненты устанавливаются заранее.

В основе решения Teradata Extreme Data Appliance лежит та же архитектура с низким потреблением энергии, что и у остальных платформ семейства Teradata, но при этом оно занимает относительно малую площадь, что позволяет снизить капитальные и эксплуатационные затраты на вычислительный центр.

Teradata Extreme Data Appliance дополняет растущее семейство специальных платформ Teradata, в которое входят Teradata Data Mart Appliance, Teradata Data Warehouse Appliance и Teradata Active Enterprise Data Warehouse.

8Gb FC и SSD в составе NetApp FAS и V-Series

Ноябрь 2008 г. – Компания NetApp усилила линейку систем хранения среднего уровня, представив системы FAS3160 и V3160. Также NetApp обнародовала планы по внедрению адаптеров 8Gb Fibre Channel (FC) и оснащению линеек FAS и V-Series корпоративного уровня твердотельными флэш-накопителями (Solid-State Drive, SSD) и флэш-модулями кэширования.

Поставки дополнительного адаптера для систем NetApp FAS и V-Series, обеспечивающего поддержку 8Gb FC, начнутся в феврале 2009 г. Поставки флэш-модулей начнутся во 2-м кв. 2009 г.

3Gb SAS блэйд-коммутатор от HP

Ноябрь 2008 г. – Компания HP анонсировала доступность своего первого SAS коммутатора – HP StorageWorks 3Gb SAS BL Switch, предлагаемого в составе шасси c3000 или c7000.

В сравнении с аналогичными решениями на базе iSCSI или Fibre Channel, HP позиционирует SAS-решения как более дешевые, т.к. не требует аналогичной Ethernet/FC инфраструктуры. SAS-коммутатор поставляется с 8 или с 16 3Gb SAS-портами и позволяет блэйд-серверам расширять разделяемую емкость хранения на базе подключаемых внешних дисковых полок или/и SAS-, SATA-дисков. Агрегированная полоса пропускания коммутатора – 3Gb и он полностью совместим с 1,5Gb SATA-технологией.

Поддерживаемые ОС серверов: MS Windows Server 2008/2003/2003 R2 (32/64), Red Hat Linux 5 (32/64), SuSE 10 (32/64), VMware ESX 3.5 (32/64).