CAS-решения: особенности и применение

Обзор тенденций, состояния рынка, а также архитектурных и функциональных особенностей решений для хранения и доступа к неизменяемому контенту.

Введение

Термин "CAS" (Content Addressable Storage) появился в конце весны 2002 г., когда компания EMC анонсировала новый класс устройств – EMC Centera, ориентированный на работу с неизменяемым (фиксированным/постоянным) контентом в составе справочно-информационных и архивных систем. Одновременно с термином "CAS" стал широко использоваться и новый способ доступа к файлам (блоку данных) – не по имени файла или номеру блока данных, а по уникальному идентификатору файла, вычисляемому на основе содержимого файла. И хотя CAS-системы (с точки зрения обращения к файлам) имеют ряд неоспоримых преимуществ, например, с точки зрения обеспечения безопасности информации, к CAS-решениям мы будем условно относить и другие разработки данного класса, непосредственно не использующие контентно-адресуемый доступ к файлам.

Тенденции, позиционирование и обзор рынка CAS-решений

Тенденции и требования рынка

Почему возрастает интерес к решениям архивирования контента и CAS-решениям, в частности? Этому способствуют, прежде всего, две тенденции: во-первых, рост информации, а, во-вторых, увеличивающиеся требования к ее доступности.

Согласно последним исследованиям IDC ("A Forecast of Worldwide Information Growth Through 2010", *март 2007 г., IDC*), объем информации накапливаемой человечеством ежегодно, увеличивается более чем на 80%. При этом рынки Восточной Европы (куда относят и Россию) будут развиваться на 30% быстрее "устоявшихся" рынков Западной Европы, Северной Америки, Японии.

Интеграция России в международные рынки приводит к тому, что все большее число регламентирующих норм и актов деятельности для западных компаний распространяется и на российские. Это значительно повышает требования к хранению и доступности информации. Так, уже в 2008–2009 гг. Центробанком РФ планируется внедрение в России Basel II (инструкции, разработанные и предложенные Базельским комитетом по банковскому надзору), в соответствии с которыми банки будут обязаны собирать и хранить всю детальную информацию о своих процессах и операциях. При этом данные не только должны быть собраны со всех подразделений, но и проверены и консолидированы. Обычно это выливается в создание новых или расширение существующих центров хранения данных (хотя многие организации уже имеют центры хранения данных, большинство все же не удовлетворяет требованиям Basel II в этом плане). Еще одним очень важным элементом Basel II является IT-безопасность, в соответствии с которым банк должен внедрить средства контроля над центром хранения данных.

Телекоммуникационные российские компании, работающие в странах Евросоюза, к 15 сентября 2007 г. должны будут обеспечить выполнение директивы 2002/58/EC, которая была принята в рамках мер по борьбе с международной организованной преступностью. При каждом звонке по мобильному телефону создается отдельная запись call data record (CDR), которая затем может использоваться для биллинга, сегментации рынка, выявления случаев мошенничества и др. Данные, которые нужно сохранять в соответствии с директивой, – это вся информация CDR за исключением голосовых данных. Также нужно сохранять данные обо всех неудачных звонках. В соответствии с директивой, данные CDR должны храниться от 6 месяцев до 2 лет со времени сеанса связи и, если государственные или местные органы правопорядка запросили эти данные, то оператор обязан предоставить их немедленно. За один рабочий день может накопиться в среднем 10 млн CDR (до миллиарда CDR). При ориентировочном размере одной CDR – 500 байт – за день, в среднем, накапливается 5 Гбайт, которые нужно сохранить.

Кроме того, операторы из стран, не входящих в ЕС, должны выполнить требования по сбору информации, действующие в ЕС. Это означает, что данные о звонке с мобильного телефона в России и на Украине абоненту, зарегистрированному в ЕС, должны быть сохранены оператором, обслуживающим этого абонента.

Российские компании, которые хотели бы стать участницами фондового рынка США, должны будут выполнить требования закона Sarbanes-Oxley (Sarbanes-Oxley Act – SOX). Согласно этому закону, все компании, которые либо представлены на фондовом рынке США, либо планируют выйти на эти рынки, должны в обязательном порядке соответствовать требованиям SOX в сфере создания эффективной системы внутреннего контроля при составлении финансовой отчетности, а также отчитываться в надежности и достоверности данной финансовой отчетности. А данные по финансовой деятельности в электронной форме должны предоставляться по запросу в течение 48 часов, даже если с момента события прошло 5 лет. Личную ответственность за соблюдение этих требований несут генеральный и финансовый директора компании.

Подобные акты и регулирующие нормы рассматриваются для принятия в России, кроме упомянутых, и в других отраслях, в частности, медицине, страховании и др.

Позиционирование CAS-решений в составе архивных систем

До недавнего времени под архивом подразумевалось хранение вторичных резервных копий на более дешевых носителях, чем первичные (рис. 1). При этом архив использовался только в случае, если первичная резервная копия повреждена, а по объему соответствовал совокупности первичных резервных копий. Существенным недостатком данной схемы являлось то, что по мере роста биз-

Рис. 1. Архив в "классическом" понимании (в "традиционной" схеме обеспечения надежности данных) обеспечивал хранение резервных копий на более дешевых носителях.

неса резервные копии начинали "раздуваться", вследствие чего неоправданно начинали расти затраты на их хранение и, соответственно, требовалось все больше времени на процедуры резервного копирования/восстановления.

Следующим этапом явился шаг, когда из производственных данных (а, соответственно, и из первичных резервных копий) стали удаляться устаревшие данные, которые записывались в архив (рис. 2). Вместо последовательной двухэтапной схемы, стала использоваться параллельная, где процедуры архивирования данных и резервного копирования выполнялись одновременно. Все процедуры были значительно оптимизирова-

1. **Архивирование *статической*** информации:
   - улучшает производительность основных приложений;
   - уменьшает TCO, используя многоуровневые системы хранения;
   - освобождает емкость на системах хранения 1-го уровня;
   - прозрачно для пользователей и приложений.
2. **Резервное копирование *активной*** информации:
   - не нужно копировать и восстанавливать архивные данные;
   - сокращение окна резервного копирования;
   - повышение надежности, высокий процент полных копий.
3. **Извлечение *из архива*** или **восстановление *из резервной копии*:**
   - запросы на восстановление обрабатываются быстрее;
   - ранее недоступная информация теперь стала доступна.

Рис. 2. При данной архитектуре архивирования удалось в значительной степени оптимизировать процедуры резервного копирования/восстановления.

ны и, соответственно, были снижены затраты на их поддержание. Дополнительно появилась возможность использовать архивные данные в режиме "nearonline". Архив стал активной компонентой в составе ILM-решений.

На последнем этапе архивирование стало выполняться на специализированном (appliance или CAS-решение), в значительной степени интеллектуализированном, устройстве, самостоятельно выполняющем функции по обеспечению целостности, надежности, поиску/предоставлению данных/информации приложениям, никак не связанным с "основными" (рис. 3).

Рис. 3. Активный архив, или CAS-решение, непосредственно предоставляет данные "сторонним" приложениям.

В общем случае к CAS-решениям можно отнести большое семейство программно-аппаратных и законченных систем (appliance), обеспечивающих архивирование и дальнейшее использование данных. Однако при позиционировании CAS-решений в контексте вышесказанного этот круг сужается и появляется ряд условий, которым должны отвечать "классические" CAS-системы. Прежде всего, это:

- законченные системы, имеющие высокие степени самоуправляемости (без вмешательства извне) и защищенности данных при минимальных усилиях по эксплуатации;
- системы, имеющие простую и высокую масштабируемость, допускающую совместное использование аппаратных компонент разных версий;
- возможность поиска данных по метаданным/содержимому объекта;
- возможность управления хранимыми данными (по уровню безопасности, времени хранения и др.) на основе политик, выполняемых самой CAS-системой.

Чем больше объем и срок хранимых данных в CAS-системе, а также чем более жесткие SLA и compliance-требования к ним, тем в бóльшей степени CAS-система должна удовлетворять выше названным требованиям законченной самоуправляемой системы.

В настоящий момент в мире CAS-решения подобного уровня производят 4 вендора (все они доступны и поставляются в Россию): EMC – Centera, HP – RISS, HDS – Content Archive Platform и Sun Microsystems с недавно анонсированной системой Sun StorageTek 5800 (проект Honeycomb). Помимо этих, на рынке представлен и ряд других производителей – с менее специализированными системами (в Россию практически не поставляются), в частности: Bycast Inc. (Bycast Storagegrid – программная платформа); Caringo Inc. (CAStor – программная платформа); ExaGrid Systems Inc. (ExaGrid System); IBM Corp. (решения на основе продуктов SENCOR); Nexsan Technologies Inc. (Assureon) и др.

Поскольку краткая аннотация CAS-решений не может дать полного представления о возможных областях их применения, рассмотрим более подробно первые 4 решения.

Обзор CAS-решений

Все 4 решения, выбранные для рассмотрения, представляют собой законченные решения – кластерные системы – примерно одного уровня масштабируемости (от нескольких до десятков терабайт и до 1 Пбайт и более). С "внешним миром" все системы связываются по IP-протоколу, внутри системы узлы кластера также связаны IP-интерфейсом, в отдельных системах дополнительно используются и другие интерфейсы, например, FC. Как правило, базовым элементом (узлом) таких систем является стандартный сервер. Все они отличаются архитектурными особенностями, реализованной функциональностью, уровнем поддержки разработчиков ECM-продуктов (Enterprise Content Management) и др.

Все рассматриваемые CAS-системы нельзя сравнивать как с традиционными дисковыми системами (монолитными/модульными), так и с оптическими или ленточными библиотеками. В отличие от первых, они имеют гораздо меньшую производительность, поэтому не могут использоваться для онлайновых приложений, а в целом отличаются (как от дисковых систем, так и ленточных/оптических библиотек) наличием встроенной функциональности управления (сортировка, поиск, удаление и др.) и обеспечением безопасности хранения контента.

EMC Centera

EMC Centera – самый "старый" продукт на рынке CAS-решений. С момента его доступности (апрель 2002 г.) в мире его приобрели более 3500 клиентов (общим объемом 150 Пбайт), и сейчас его поддерживают более 400 независимых поставщиков ПО.

Архитектура EMC Centera

Аппаратно Centera представляет (рис. 4) совокупность узлов, или кластер стандартных серверов, отвечающих за обработку запросов приложений (Access Node

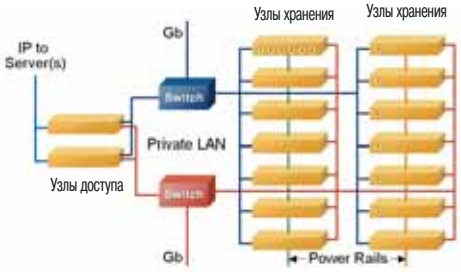

Рис. 4. Архитектурно Centera состоит из узлов доступа (Access Node) и узлов хранения (Storage Node), соединяемых между собой через два коммутатора.

– AN) и за хранение данных (Storage Node – SN), объединенных в RAIN-архитектуру (Redundant Array of Independent Nodes). В системе Centera используется не менее двух узлов для обработки запросов, причем количество таких узлов обычно увеличивается с ростом емкости Centera, что позволяет повышать производительность пропорционально росту емкости. Каждый узел хранения информации содержит 2 Тбайт незащищенного дискового пространства и соединен со всеми остальными узлами Centera через дублированную внутреннюю сеть Gigabit Ethernet, построенную на Layer 3 коммутаторах.

Минимальное число узлов в Centera – 4. В одном кабинете может быть установлено до 32 узлов с возможностью масштабирования до 1 Пбайт в составе одной системы хранения.

Обеспечение сохранности данных

В связи с тем, что Centera решает сразу задачи как хранения, так и управления данными, на принципиально другом уровне обеспечивается защита данных, как от аппаратных сбоев, так и от ошибок администратора или приложения, использующего систему Centera.

Каждый сохраняемый на Centera объект обязательно дублируется на двух различных узлах при использовании Content Protection – Mirroring (CPM). Причем, выбираются те узлы, которые наименее загружены и имеют больше свободного пространства. При защите Content Protection – Parity (CPP) объект разделяется на 6 час-

тей и записывается на 6 различных узлов с записью контрольной суммы (по аналогии с RAID 5) на седьмой узел, что так же, как и CPM, позволяет полностью защититься от сбоя любого узла.

В случае выхода из строя узла, остальные узлы, содержащие объекты, которые также хранились на отказавшем узле, автоматически сделают еще одну копию объектов. Таким образом, в процессе копирования 2 Тбайт данных участвуют максимальное количество узлов, что позволяет восстановить необходимую избыточность данных за минимальное время без заметного влияния на производительность хранилища.

При сохранении объекта приложение может указать минимальный период хранения (retention period). В этом случае объект не может быть удален приложением до окончания данного периода, что позволяет гарантировать сохранность информации в течение заданного времени даже при ошибках оператора, сбоях приложения или диверсии.

Дополнительную защиту обеспечивает проверка целостности данных, которая выполняется регулярно для всех хранимых объектов. При такой проверке сверяется содержимое объекта с контрольной суммой и с уникальным идентификатором. При искажении объекта на одном из узлов он автоматически восстанавливается при помощи CPM или CPP защиты.

Еще один уровень защиты обеспечивает возможность репликации данных между несколькими системами Centera, которые могут быть расположены в различных центрах обработки. Такая репликация, обеспечиваемая CentraStar, позволяет защитить данные от масштабных аварий и катастроф. При этом максимально упрощается процесс получения данных в резервном центре, так как они будут автоматически запрошены через интерфейс Centera API с резервной системы при недоступности основной системы Centera.

Защита инвестиций и расширение емкости

В составе одной системы Centera могут одновременно использоваться все когда-либо выпущенные поколения узлов Centera. При этом CentraStar будет учитывать разницу в производительности и емкости различных узлов при размещении данных. Приложения защищены от технологических изменений благодаря тому, что работа Centera абсолютно не зависит от того, какие узлы в ней используются. Более того, даже в случае появления в будущем принципиально других узлов, использующих, например, твердотельную память, а не дисковые накопители, не потребуется вносить ни одного изменения в приложения, а эти новые узлы можно будет использовать совместно с уже имеющимися.

При добавлении узлов в кабинет или добавлении нового кабинета Centera автоматически определяет новое доступное пространство и начинает незамедлительно его использовать. Таким образом, полностью отсутствуют проблемы, связанные с расширением логических томов в системах хранения SAN или файловых систем в NAS-хранилищах.

Адресация данных

Система хранения EMC Centera является системой с адресацией данных по их содержимому, или CAS-системой (Content Addressed Storage).

При сохранении объекта система Centera вычисляет уникальный идентификатор объекта по алгоритму MD5 компании RSA Data Security с использованием содержимого объекта. При сохранении нескольких объектов с идентичным содержимым Centera будет содержать только одну копию объекта, что позволит сократить объем используемого пространства.

Для получения объекта или его удаления приложение использует уникальный идентификатор объекта. Очевидно, что при попытке злоумышленника незаметно исказить данные на системе хранения, приложение по-прежнему будет получать по своему идентификатору неискаженные данные, так как искаженному объекту будет соответствовать совершенно другой, незнакомый приложению идентификатор. Благодаря такой защите данных система Centera является на текущий момент единственной системой хранения, сертифицированной Комиссией по ценным бумагам США и Министерством обороны США для хранения данных, искажение которых не допускается (финансовая и секретная информация).

При сохранении объекта приложение также может сохранить в Centera дополнительные свойства в формате XML, по которым в дальнейшем может производиться поиск и фильтрация выдаваемых объектов, что особенно важно при восстановлении идентификаторов объектов, если они были по какой-то причине потеряны приложением.

Каждый идентификатор занимает 128 бит. Если средний размер объекта составляет, например, 1 Мбайт, то при хранении 1 Пбайт информации на Centera общий объем идентификаторов составит всего лишь 16 Гбайт. Только для этих данных нужно производить регулярное резервное копирование, что при таких маленьких объемах не составляет труда. Резервное копирование данных, хранимых на Centera, также может производиться при помощи протокола NDMP, но практической необходимости в этом нет, особенно при использовании минимального срока хранения объектов (retention period).

Производительность EMC Centera

Из-за возможности свободно определять количество узлов обработки запросов приложений производительность Centera может расти линейно при росте объема. При этом любой из хранимых объектов будет выдаваться приложению незамедлительно благодаря использованию дисковых накопителей для хранения данных.

Все потоки в Centera распределяются равномерно по всем доступным узлам, но для сбалансированности нагрузки между узлами доступа и хранения важно выдерживать правильное соотношение между ними:

- 2 узла доступа на 8 узлов Centera (6 SN, 2 AN);
- 4 узла доступа на 16 или 32 узла Centera;
- от 2 до 4 узлов доступа на каждый дополнительный кабинет в кластере;
- в целом – 1 узел доступа на 7 узлов хранения.

Добавление узлов доступа выше рекомендованных улучшает производительность Centera по чтению от 20% до 70% в зависимости от размера файла (объекта) и, чем меньше размер файла, тем меньше прирост производительности (рис. 5). Это объясняется тем, что вследствие одинакового объема накладных затрат независимо от размера передаваемого объекта (файла), общая пропускная способность снижается при уменьшении размера объекта. При этом следует учитывать то, что на каждый

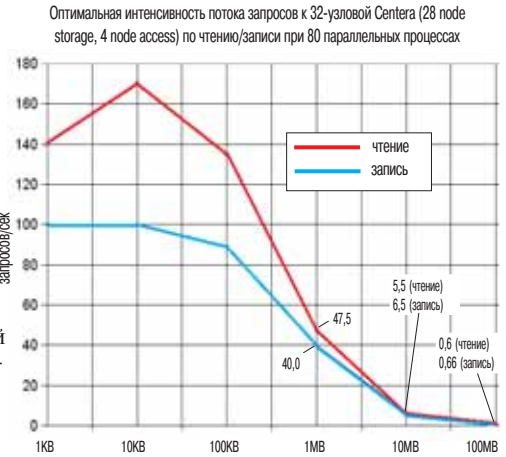

Рис. 5. Изменение пропускной способности Centera (файлов/сек) в зависимости от размера файла и типа операции.

объект записи в Centera пишется 4 объекта: (сам файл + его описание) x 2 (при зеркалировании).

Особенностью архитектуры Centera является то, что она поддерживает множество параллельных потоков, поэтому для увеличения общей пропускной способности важно использовать многопоточные приложения. Однако важно оптимизировать параллельные процессы в системе, чтобы существенным образом не росли задержки из-за конкуренции за ресурсы (рис. 6).

Все узлы доступа Centera могут быть подключены к коммутатору и работают параллельно. Centera с 28 узлами для хранения данных и 4 узлами обработки запросов позволяет получать более 0,5 млн документов объемом 100 Кбайт в час.

Следует учитывать и то, что при чтении сервер приложения посылает приложению только CAS-адрес, дальнейшее считывание объекта происходит уже без уча-

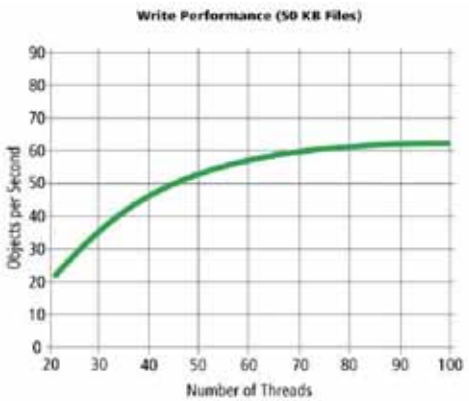

Рис. 6. Оптимальное соотношение между числом параллельных потоков и интенсивностью обращений на запись.

стия сервера, что в ряде случаев позволяет во многом снизить требования к серверу.

Управление EMC Centera

Система Centera самостоятельно осуществляет конфигурирование своих узлов, балансирует нагрузку между ними, при необходимости мигрируя данные между узлами хранения, автоматически восстанавливает необходимую избыточность при любых сбоях. Управление данными производится самими приложениями, которые в соответствии со своей логикой создают и удаляют объекты. Таким образом, администрирование системы Centera сводится лишь к мониторингу доступного свободного пространства и наблюдению за статистикой по аппаратным сбоям и производительности.

Интеграция с приложениями

На данный момент несколько сотен различных приложений поддерживают Centera API – от специализированных приложений по документообороту, хранению рентгеновских снимков, данных геологоразведки – до приложений для архивации данных SAP, Exchange, Lotus Notes и построения иерархических систем хранения данных. Несколько программных платформ EMC также поддерживают Centera: HSM-системы EMC Avalon и EMC DiskXtender, а также ECM-система Documentum. При этом "объект" системы Centera для каждого из приложений представляет собой именно те объекты, которыми оперирует приложение: фотография, документ, файл и т.д.

При использовании Documentum полностью реализуется функциональность Centera, включая возможность задания минимального периода хранения (retention period) для хранимых документов. Настройка интеграции осуществляется прямо из графического интерфейса Documentum при его первичной установке или при дальнейшем изменении конфигурации, что позволяет администратору Documentum использовать Centera без необходимости в дополнительном обучении. Для определения того, какие документы будут храниться на Centera, используются стандартные правила Documentum, что позволяет осуществлять гибкую настройку.

В случае использования приложения, которое не поддерживает EMC Centera API, существует несколько простых способов интеграции. Например, при помощи HSM-систем, когда приложение работает с огромными файловыми системами, большая часть которых на самом деле хранится на Centera. Или при помощи NAS-шлюза Centera Apllication Gateway, позволяющего осуществлять доступ к данным по протоколам NFS, CIFS, FTP и HTTP.

Кроме того, Centera API поддерживает C/C++ и Java для операционных систем Sun Solaris, HP HP-UX, IBM AIX, Linux, SGI IRIX, Windows NT/2000/XP и IBM z/OS и может быть использован в самостоятельных разработках.

Одна система Centera может одновременно использоваться различными приложениями. Для каждого из приложений можно настроить соответствующий уровень доступа, что не позволит получить неавторизованный доступ к данным.

Одна из основных функций – выборка документов по запросу – реализуется с помощью ПО Centera Seek, которое является по сути встроенным поисковым сервисом. Поиск осуществляется по метаданным, которые хранятся XML-формате, и его результатом является XML-таблица элементов, удовлетворяющих критерию поиска. Для получения самого объекта требуется его уникальный идентификатор, и, таким образом, логика работы массива не нарушается. Centera Seek позволяет осуществлять поиск по всему архиву вне зависимости от количества приложений, которые используют архив.

Centera позволяет создавать виртуальные CAS-хранилища внутри одной системы, что при необходимости полностью изолирует объекты, хранимые различными потребителями.

Для обеспечения требований к данным, требующих особых подходов к хранению, имеются дополнительные опции, например: *"усиленный период хранения"* – в течение периода хранения (Retention Period) никто, даже системный администратор, не может удалить объект; *"Shredding"* – физическое удаление данных с дисков путем многократного перемагничивания секторов, на которых эти данные располагались, и др.

TCO

Общая стоимость обслуживания, или эксплуатационных затрат (Total Cost of Ownership – TCO) – один из основных факторов, определяющих выбор системы для долговременного хранения. Для Centera, по стандартным нормам, при отсутствии ее переполнения появление инженерного персонала для профилактических мероприятий требуется один раз в полгода (при гораздо меньшей реактивности персонала в случае возникновении неисправностей, поскольку даже многочисленные отказы приводят только к некоторой деградации системы, а не к ее отказу в целом).

За счет возможности одновременного использования нескольких поколений узлов отсутствует необходимость наличия склада запасных частей или необходимость приобретения у поставщика комплектующих, уже снятых с производства (которые, как правило, по своим характеристикам не только намного уступают последним релизам, но даже стоят больше).

Hitachi Content Archive Platform (CAP)

Доступность Hitachi CAP была анонсирована HDS в июне 2006 г. На момент объявления система была протестирована с возможностью масштабирования до 300 Тбайт и способностью поддерживать до 350 млн файлов в архиве. Архитектурно Hitachi CAP может масштабироваться до 2,5 Пбайт и поддерживать до 2 млрд файлов в одном архиве.

Конструктивно CAP строится на основе ячеек (рис. 7). Одна ячейка содержит 2 узла (стандартные серверы) с установленным Hitachi Content Archive ПО (на основе технологии Archivas®) и устройство хранения – WMS100, подключаемое к узлам по интерфейсу FC. Все ячейки в стойке объединяются на сете-

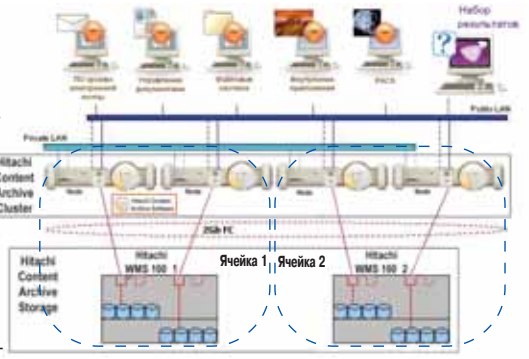

Рис. 7. Архитектура Hitachi Content Archive Platform.

вом коммутаторе. Базовая модель включает 2 ячейки с начальной полезной емкостью 4,8 и 9,6 Тбайт. Несколько ячеек можно объединять в более крупные системы с единым пространством имен архива (поддерживается до 40 ячеек).

Свою архитектуру Hitachi называет SAIN (SAN + Array of Independent Nodes). В сравнении с RAIN (EMC Centera), в SAIN элементы хранения контента отделены от архивных сервисов, которые обслуживаются узлами. По заявлениям разработчика, в перспективе это может упростить и удешевить масштабирование вследствие того, что вместо систем хранения от HDS могут использоваться и продукты от других вендоров.

Среди основного функционала – возможность полнотекстовой индексации и поиска. Другие базовые особенности:

- доступ к объектам строится на основе файловой системы WORM ("однократная запись/многократное считывание");
- автоматическое восстановление и настройка конфигурации;
- автоматическое выравнивание нагрузки;
- возможность репликации данных на удаленный архив;
- возможность поддержания от 2 до 4 внутренних копий в зависимости от ценности данных;
- аутентификация:
  - периодически рассчитывается цифровая подпись, которая сравнивается со значением, сохраненным в момент архивации файла;
  - пользователь может выбрать различные алгоритмы формирования хэш-кода (цифровой подписи), в том числе SHA-1 (256, 384 или 512 бит), MD5 и RIPEMD-160;
- возможность хранения всех типов контента (структурированного, полуструктурированного, неструктурированного);
- стандартные интерфейсы интеграции (NFS, CIFS, HTTP и WebDAV). CAP поддерживает стандартные шлюзы файловых систем, может хранить стандартные форматы файлов, такие, как XML и HTML. Всего поддерживается 370 форматов файлов и 77 языков;
- гарантируется, что после удаления файла нельзя будет извлечь с диска

никаких его следов (соответствие стандарту Министерства обороны США 5520-М).

HP StorageWorks Reference Information Storage System (RISS)

Архитектура и функциональные особенности RISS

Первая реализация HP RISS доступна с середины 2004 г. Хотя RISS имеет IP-интерфейс для взаимодействия с любым приложением, он в основном ориентирован на работу с почтовыми системами по протоколам SOAP, HTTP, HTTPS, IMAP4 и SMTP, в списке которых поддерживаются следующие почтовые серверы: Exchange 5.5/2000/2003, Lotus Domino V5/V6, Sendmail, а также почтовые клиенты: Outlook 2000/2002-XP/2003. Из поддерживаемых ОС для управления документами – Windows 2000/XP.

Среди файлов, которые автоматически индексируются по ключевым словам, позволяя впоследствии осуществлять поиск по содержанию документа, следующие: MS Office (.doc, .ppt, .xls), MS Access (с различными расширениями), MS Outlooks personal folder (.pst), Adobe Public Distribution Format (.pdf), Rich text format (.rtf), Outlook encapsulated .rtf (TNEF), Hypertext Markup Language (.html), Text files (.txt), ASCII files (.asc). Файлы других типов, не содержащие информации для индексирования, например, TIFF, MPEG, GIF, JPEG, WAV, могут записываться в RISS, но их поиск будет осуществляться только по атрибутам (тип файла, имя файла, время создания файла, автор файла).

Основные функциональные особенности определяются непосредственно самой системой хранения, реализованной в виде множества двуразмерной grid-сети связанных ячеек (рис. 8) – Grid Computing Architecture (архитектура вычислительной сети). Каждая ячейка в такой сети представляет собой полнофункциональный сервер стандартной архитектуры с несколькими SCSI-дисками по 146 Гбайт. В базовой комплектации (при 4 Тбайт полезной емкости) таких ячеек без зеркалирования несколько десятков. Наличие компьютера в каждой ячейке сети дает широкие возможности по "манипулированию" объектом хранения, управлению доступом к нему и поисковым возможностям системы, когда поиск некого подмножества документов (документа) осуществляется на множестве параллельно работающих серверов. Для этого применительно к почтовой системе каждая ячейка имеет индексацию по атрибутам письма и по ключевым словам содержимого письма, а также непосредственно по самому контенту.

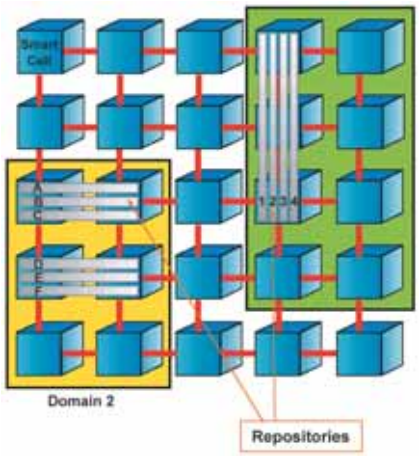

Рис. 8. Архитектура HP RISS представляет собой множество связанных IP-интерфейсом ячеек, каждая из которых является стандартным сервером. Каждая из ячеек содержит контент, индексы и обеспечивает все сервисы по ее контенту. В целях удобства управления RISS может быть разделен на домены, внутри которых выделяются репозитории.

Домены и репозитории

В целях упрощения управления RISS может быть разделен на домены или на несколько меньших объектов (рис. 9). Например, администратор может создать отдельные домены – каждый с собственными политиками – для отдельных подразделений внутри большой организации. В частности, домены могут быть полезны в сервисных бюро или для сегрегации "регулируемых" и "нерегулируемых" документов, а также почтовых сообщений.

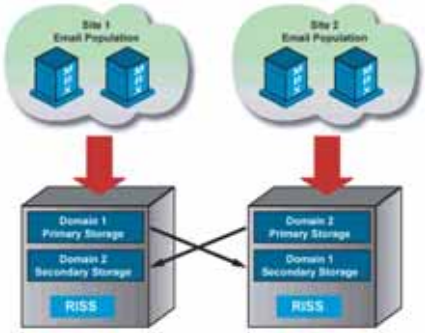

Рис. 9. Реплицирование данных на удаленный RISS может быть двунаправленным.

Каждый домен содержит не менее двух ячеек, которые физически отделены от других, и может иметь собственные backup политики, разрешения на доступ к ячейкам и управляться собственным администратором.

Внутри каждого домена можно выделить один или несколько репозиториев (архивов). Каждый репозиторий – логический объект, который физически строится не менее чем на двух ячейках хранения (storage SmartCell). Репозиторий, например, может представлять почтовый ящик одного пользователя. Домен может содержать множество почтовых ящиков пользователей. Списки контроля доступа определяют, кто имеет доступ к специфическому домену или репозиторию.

"Регулируемые" и "нерегулируемые" сообщения

RISS хорошо подходит для хранения как "регулируемых", так и "нерегулируемых" сообщений в течение многих лет. В регулируемой среде, почтовые сообщения немедленно направляются к системе хранения; в нерегулируемой – система хранения сама периодически "перемещает" или "собирает" сообщения от Exchange серверов.

Например, благодаря типовой политике система может собирать все почтовые сообщения по истечении 7 дней. В этом заданном режиме архивирования RISS становится расширением сервера Exchange и сгружает всю электронную почту, которая получена 8 дней назад и более, таким образом сокращая размер сервера Exchange. Электронные письма могут также выборочно собираться на основании других критериев (например, отправитель, получатель, тема и т.д.).

Все собранные сообщения (и их вложения) хранятся RISS и удаляются с сервера Exchange. После этого пользователи в почтовом ящике видят только немного измененный заголовок сообщения со специальной иконкой, которая свидетельствует, что данные были успешно сохранены на RISS. Чтобы восстановить сообщения, пользователи просто дважды щелкают на значке: сообщения восстанавливаются с RISS и посылаются напрямую Outlook клиенту (не на сервер Exchange).

Почтовые сообщения, к которым предъявляются повышенные требования – неизменности и сохранности в течение многих лет – могут снабжаться цифровыми подписями с целью верификации их целостности.

Правила хранения контента могут определять различные уровни доступа к его содержимому для различных групп или отдельных пользователей.

Устранение хранения дублированных сообщений

Хранение одинаковых сообщений может в ряде случаев быть достаточно дорогостоящим. Например, сохранение множественных копий единственной презентации PowerPoint на несколько мегабайт может излишне уничтожить многие мегабайты ресурсов хранения. Поэтому высокоэффективные архивные системы почтовых сообщений должны устранять или уменьшать эту избыточность. RISS обнаруживает одинаковые сообщения двумя способами: 1) по анализу полей письма (когда письмо посылается множеству получателей); 2) путем сравнения уникальной цифровой подписи, создаваемой для каждого хранимого в RISS сообщения. Таким образом устраняется дублирование сообщений, поступающих даже с разных почтовых серверов.

Поиск сообщений

RISS, как уже отмечалось, – не только хранилище данных, но и мощная поисковая машина. Сообщения могут отыскиваться в соответствии со многими критериями поиска, включая: дату сообщения, имя получателя и отправителя, тему или текстовую строку в пределах сообщения.

Защита данных

RISS обеспечивает несколько уровней защиты данных. *Первый* уровень: каждая ячейка SmartCell зеркалируется к другой ячейке в пределах одного репозитория. Во время записи правильность сохраняемых данных как на основной ячейке, так и ее зеркале, проверяется через верификацию циклического кода избыточности (CRC), прежде чем операция записи закончится.

Зеркальное отражение в пределах RISS защищает от отказов самих ячеек, но не защищает данные от отказа первичного центра данных в целом. Для обеспечения катастрофоустойчивости данные первич-

ного RISS могут копироваться дистанционно на вторичную RISS-систему по IP, T3, OC3/12 или по DC3 соединению – *второй* уровень. Удаленное реплицирование происходит на уровне доменов и может быть двунаправленным (см. рис. 9). Например, домен 1 в первичном RISS 1 может копироваться на удаленный RISS 2, в то время как домен 2 в RISS 2 – в RISS 1.

Для пользователей, которые не имеют второго центра данных, есть возможность копирования данных и цифровых подписей на носители с однократной записью (WORM – Write-Once Read-Many), т.е. на WORM-ленту или оптический диск. При этом устройство, обеспечивающее запись, может располагаться локально или соединяться через IP WAN сеть.

Пользовательский интерфейс

Два различных интерфейса предлагаются конечному пользователю для поиска и получения любого контента, который сохранен в RISS. Пользователь может осуществлять поиск и извлечение сообщений и документов из почтового клиент-ориентированного приложения или через web-интерфейс.

Web-интерфейс позволяет пользователю иметь доступ к контенту из любого web-браузера и любого местоположения. Пользователь может выбрать тип искомого контента (e-mail сообщение или документ) и запускать простой или расширенный поиск в RISS. Оба варианта поиска предоставляют поля, соответствующие типу искомого контента.

Основные характеристики RISS

В базовой комплектации (для 4 Тбайт полезной емкости) RISS конструктивно исполнен в двух 19" стойках общей высотой 42U. Основные показатели RISS:

- внешний интерфейс для взаимодействия с RISS – 1 Gigabit Ethernet;
- максимальная емкость – 350 Тбайт (более 7 млрд сообщений емкостью 50 Кбайт);
- максимальная производительность входящих сообщений – 2 млн в сутки для базовой комплектации;
- максимальная производительность восстанавливаемых сообщений – 40 документов в секунду, до 500 одновременных запросов – для базовой комплектации;
- автоматическое перемещение данных от старой ячейки к новой;
- возможность записи данных в режиме WORM (Write Once Read Many);
- поддержание цифровой подписи данных, обеспечивающей идентификацию целостности данных;
- автоматическое удаление данных по истечении заданного срока.

Sun StorageTek 5800 System

Это последнее из недавно (май 2007 г.) представленных на рынке CAS-решений, разработанное Sun Microsystems в рамках проекта Honeycomb. Система Sun StorageTek 5800 построена на симметричной кластерной архитектуре (рис. 10). Все управление хранением, данными, путями метаданных распределено через кластер, обеспечивая как надежность, так и масштабируемую производительность. Каждый 1U узел представляет стандартный сервер под управлением ОС Solaris и состоит из 1U socket 939 AMD Opteron процессора, server management board и 4 SATA-дисков (по 500 Гбайт). Все узлы не зависимы друг от друга и полностью (аппаратно и программно) симметричны. Минимальная конфигурация системы состоит из 8 узлов хранения (по 2 Тбайт), двух балансировщиков нагрузки и одного Sun Fire x2100 сервера в качестве сервисной панели. В максимальной конфигурации число узлов хранения может составлять 16 (всего 32 Тбайт при SATA-дисках 500 Гбайт).

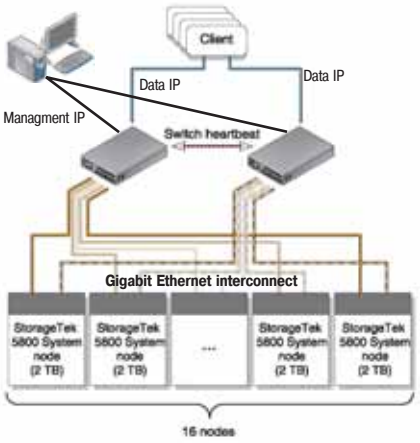

Рис. 10. Архитектура Sun StorageTek 5800.

Владимир Колганов – руководитель направления систем хранения данных компании "КРОК"

Сегодня многие государственные и коммерческие организации вынуждены оперировать большим и быстро растущим объемом информации и баз данных. При этом важно, чтобы доступ к информации был простым и быстрым, а срок ее хранения – не ограничен или задавался на основе политик работы с данными. Эти и сопутствующие им задачи помогают эффективно решать CAS-системы, которые позволяют одновременно хранить неструктурированные данные, обеспечивать к ним эффективный доступ, определять с помощью политик жизненный цикл данных, автоматически архивировать или уничтожать устаревшие данные, а также применять дифференцированный подход к выбору среды хранения в зависимости от степени актуальности данных.

Среди представленных в настоящий момент на рынке аналогичных систем EMC Centera, на мой взгляд, выгодно отличает возможность интеграции с уже используемым заказчиком программным обеспечением. Это позволяет не только экономить средства, но и значительно упростить управление большими объемами разнородной информации. Немаловажно, что система EMC Centera наряду с неструктурированными данными также позволяет управлять значительными объемами фиксированных данных при существенно более низких затратах. Так, один штатный сотрудник может управлять пулом фиксированных данных общим объемом до 350 Тбайт.

Как показывает наш опыт внедрения CAS-решений, чаще всего они используются для архивного хранения больших объемов информации почтовых и файловых систем. Гибкость решения позволяет также ее использовать для решения отраслевых задач. К примеру, для банков актуальна возможность хранения финансовых документов и транзакционных файлов от платежных систем. Телекоммуникационным компаниям Centera позволяет хранить большие объемы биллинговой информации. Перспективным является использование CAS-систем в тех отраслях, где необходимо хранение очень больших объемов информации без изменения длительное время. К ним относятся страхование, архивы, в том числе государственные, метеорология, медицина и др.

Отдельно стоит отметить возможности отраслевых решений на базе EMC Centera для государственных, областных и муниципальных организаций, обеспечивающих хранение архивированных данных, существенное сокращение административных затрат, упрощение консолидации и совместного использования данных, а также повышение уровня обслуживания.

Работающий в "КРОК" первый в России Авторизованный центр компетенции EMC позволяет нашим специалистам выполнять интересные и подчас уникальные проекты на базе Centera. Их основную долю составляют сегодня электронные архивы для почтовых систем, где в качестве рабочего решения используется программное обеспечение EMC EmailXtender, DiskXtender или Symantec Enterprise Vault, интегрированное с EMC Centera. Особое место занимают решения для электронных архивов служебных документов на базе EMC Documentum и Centera. Встроенная интеграция Centera и Documentum позволяет нам строить для заказчиков законченные решения корпоративного электронного документооборота с расширенным функционалом архивирования, управления жизненным циклом документов и эффективным механизмом работы с огромными объемами неструктурированных данных. Настроенные в нашем центре компетенции решения на базе технологии EMC DatabaseXtender и Centera позволяют распространить методы и подходы ILM на всевозможные базы данных, что особенно востребовано банковской системой.

На примере решения EMC Centera становятся очевидными причины, по которым CAS-технологии получили мировое признание. Перспективность этого абсолютно нового подхода в операциях с данными обусловлена надежностью их хранения, широкими и простыми возможностями масштабирования, прозрачной поддержкой устройств разных поколений и предоставляемыми инструментами для работы с огромными массивами разнородной информации.

Заключение

Интерес к CAS-решениям в России в последнее время значительно вырос. По результатам 2006 г., было реализоавано около двух десятков подобных проектов. В текущем году эта цифра должна удвоиться и тому, как уже было сказано, есть объективные предпосылки. Принятие же уже в ближайшее время XAM-стандарта (eXtensible Access Method) по унификации и стандартизации доступа к данным для контентных хранилищ позволит в значительной степени упростить и еще больше активизировать продвижение CAS-решений на рынке.