Как современные СХД решают задачи информационной безопасности

Ни один бизнес не может работать спокойно, не будучи уверенным в сохранности и доступности своих данных. С этой задачей рано или поздно сталкивается проект любой сложности. В статье рассказывается о том, как обеспечить непрерывную доступность данных и защитить бизнес от информационных потерь.

Ключевые слова: горизонтальное масштабирование, отказоустойчивость, доступность данных, программно-аппаратный коплекс

Дмитрий Юрьевич Макушенко,
руководитель проектов
RCNTEC
dmitry.makushenko@rcntec.com

Только за последние пару лет человечество произвело информации больше, чем за всю историю своего существования. Соответственно, возрастают как потребность в системах хранения данных (СХД), так и технические требования к ним.

Многие компании при выборе СХД максимальное внимание уделяют ее производительности или цене, забывая при этом о главном. Самая же важная функция СХД вытекает из самого названия – система призвана ***сохранять*** данные, обеспечивать их максимальную доступность и ни в коем случае не потерять и малой толики хранимой информации. То есть в первую очередь следует оценивать ***надежность*** предлагаемой вендором системы.

Говоря о современных СХД, мы подразумеваем легко и неограниченно масштабируемые системы, обладающие высокой степенью отказоустойчивости и доступности данных.

Scale-out vs Scale-up

Мы, в RCNTEC, твердо уверены в том, что будущее СХД за системами с горизонтально масштабируемой архитектурой. Для нас горизонтальное масштабирование – это целая философия, которой мы придерживаемся в наших разработках, создавая решения, способные бесперебойно решать задачи, размеры которых растут с течением времени, пусть даже в геометрической прогрессии.

Несмотря на то что примерно 90 % российских компаний пользуется традиционными СХД с вертикально масштабируемой архитектурой, мы уверены, что большого и радужного будущего у таких систем нет, поскольку они всегда ограничены производительностью контроллеров. Емкость таких систем не превышает десятки петабайт и наращивается путем добавления дисковых полок, количество которых всегда лимитировано. При этом распределение информации между старыми и новыми массивами является ручной операцией, а процесс переноса данных сопровождается снижением производительности. Рано

En How Modern Data Storage Systems Solve the Problems of Information Security

D. Yu. Makushenko,
Project Manager
dmitry.makushenko@rcntec.com
RCNTEC

There is no business without full confidence in the safety and accessibility of work data. A project of any complexity sooner or later faces this problem. How to protect your business from data loss and provide continuous availability of data - find out in this article.

Keywords: horisontal scalability, fault tolerance, data accessibility, software-hardware complex

или поздно системы с вертикальной архитектурой неминуемо достигают своего «потолка», и тогда требуется приобретать новый, более мощный контроллер. Независимо от мощности контроллера, при росте объемов данных и увеличении интенсивности работы с ними, контроллеры, являясь единственной точкой входа-выхода, становятся «бутылочным горлышком» системы. Сама система получается совершенно разнородной, и неминуемо начинает «подтормаживать» из-за плохой стыковки компонентов.

Недавно Род Бэгг, вице-президент по аналитике и поддержке пользователей компании Nimble Storage, делясь результатами последних исследований, назвал основной причиной задержки при доступе к данным растущую сложность систем и, как результат, проблемы с конфигурацией и совместимостью.

Хранение данных в классических СХД с ростом объемов информации становится не только затруднительным, но и опасным, особенно если говорить о записях систем видеонаблюдения. Эти данные, нужны «редко, но метко», например, для проведения расследования чрезвычайных происшествий.

Концепция горизонтального масштабирования заключается в том, что СХД строится из унифицированных модулей хранения данных, каждый из которых выполняет одновременно функции хранения и взаимодействия с потребителями. Количество таких модулей может начинаться с трех единиц и достигать десятков тысяч. За счет этого по модулям распределяются не только данные, но и нагрузка. Это позволяет увеличивать производительность системы (с одновременным ростом объема) простым добавлением модулей. При этом производительность возрастает линейно – объему данных всегда соответствует вычислительная мощность, способная его обработать.

Строительство такой СХД можно начать без значительных инвестиций, с нескольких стандартизированных юнитов. Разумеется, расширять емкость и производительность уже имеющейся системы выгоднее, чем менять ее на новую, более мощную, и это еще один плюс в пользу систем типа scale-out.

Отказоустойчивость систем

Отказоустойчивость – это способность системы работать в любой момент времени.

У каждой организации может существовать свое понимание этого термина. Для кого-то достаточно просто не потерять свои данные и не важно, что в какой-то момент времени они будут недоступны в связи со сбоями или неполадками в системе. А для другого недоступность данных пусть даже в течение нескольких минут может быть критичной и привести к огромным убыткам. Эти несколько минут в реальной жизни приводят к задержке самолетов, невозможности проведения срочных финансовых операций, а иногда препятствуют своевременному получению данных медицинских анализов, что может поставить под угрозу жизнь пациента.

Обеспечить отказоустойчивость в случае сбоя помогает резервирование. Допуская серьезное упрощение этого процесса, можно говорить о двух уровнях резервирования:

- на уровне аппаратных модулей, когда предусмотрено полное или частичное резервирование всех компонентов: блоков питания, путей доступа, процессорных модулей, дисков;
- на уровне программного обеспечения, когда «железо» изначально считается недостаточно надежным, а задачи резервирования решаются с помощью специального ПО, посредством которого создаются реплики данных, хранящиеся на физически разном «железе».

На software-уровне гораздо больше возможностей для оптимизации, поэтому будущее, конечно, за ним.

В качестве примера, рассмотрим как решен вопрос с резервированием в разработанной RCNTEC СХД «Полибайт» (международное название – Resilient Cloud Storage). Здесь информация по умолчанию хранится в трех репликах, размещенных в разных доменах отказоустойчивости. Благодаря этому система может выдерживать сбой целого домена отказоустойчивости (обычно – стойка либо серверное помещение), не теряя при этом в производительности. Если, вдруг, происходит сбой, система переключается на альтернативную реплику данных абсолютно незаметно для пользователей, продолжающих как ни в чем не бывало работать с системой.

Скорость восстановления

Помимо отказоустойчивости нам важна доступность данных в любой момент времени.

Традиционный подход к хранению данных подразумевает организацию единого виртуального пространства при помощи технологии виртуализации данных RAID (*redundant array of independent disks* – избыточный массив независимых дисков). Как это работает на практике, проще всего рассмотреть на примере RAID-массива из двух дисков. В случае сбоя или поломки одного из них, система продолжает работать с оставшимся, который на время сбоя становится уязвимым, так как на нем осталась единственная копия данных. Сколько продлится это состояние уязвимости – зависит от скорости восстановления. Чем быстрее система сможет восстановить нужное количество копий данных, тем меньше вероятность их потери.

Время, за которое данные «перельются» с рабочего диска на новый – и есть время восстановления. Скорость копирования примерно равна скорости чтения/записи, при условии, что контроллер не нагружен. Если в это время пользователи «грузят» систему извне, скорость будет в несколько раз ниже.

Аналогичная ситуация будет складываться независимо от количества дисков в RAID-массиве: в любом случае, восстановление будет осуществляться со скоростью, не превышающей скорости восстановления одного диска. Например, для восстановления 2 терабайт записей с камер видеонаблюдения понадобится около суток. Однако в реальной жизни этот показатель недосягаем, поскольку пользователи параллельно обращаются к доступным данным, уве-

личивая и без того повышенную нагрузку на систему.

Теперь представьте, что у нас есть система с несколькими тысячами жестких дисков, где выход из строя определенных элементов перестает быть вероятностью и становится статистикой.

Мы отказались от традиционных для систем хранения данных технологий RAID.

В СХД «Полибайт» реализован иной подход. Программное обеспечение позволяет распределить копии данных на физически отдельных модулях СХД. Софт разбивает данные на небольшие части и распределяет их по разным носителям. Восстановление происходит по принципу, сходному с торрентом, когда необходимые данные передаются маленькими частями из разных источников, что снижает нагрузку на систему в целом и обеспечивает избыточность данных. Быстродействие системы не снижается, а значит, отсутствуют задержки в доступе к информации.

Восстановление системы начинается сразу же после выхода диска из строя. Данные перераспределяются на оставшееся в системе свободное пространство автоматически. После замены вышедшего из строя диска запускается процесс балансировки, который распределит данные максимально равномерно. Даже если не произойдет оперативной замены диска, избыточность данных будет восстановлена и риск потери данных сведется к нулю.

Перспективы развития

Призвание эффективного руководителя – делать правильный выбор. Это касается в равной степени и подписания контрактов, и подбора персонала, и построения ИТ-инфраструктуры. В этой статье мы затронули только несколько наиболее важных аспектов, на которые стоит обратить внимание.

Рынок СХД развивается головокружительными темпами, и, заглядывая вперед, можно с высокой долей уверенности сказать, что в ближайшие годы они снижаться не будут, причем будущее – за горизонтально масштабируемыми системами! ■

НОВОСТИ

Защита персональных данных в облаке

Эксперты облачного проекта M1Cloud компании Stack Group – высоконадежной виртуализированной ИТ-инфраструктуры корпоративного класса, построенной на базе двух центров обработки данных в России, а также в Амстердаме и Франкфурте, – рассказали о новых возможностях для защиты персональных данных.

Если рассматривать средний и крупный бизнес, то сегодня в дополнение к требованиям высокого качества сервиса и уровня ответственности добавились требования по соответствию российским законам, которые относятся к защите персональных данных. Безусловно, профессиональный сервис-провайдер будет использовать только надежные и проверенные решения корпоративного класса для создания ИТ-услуг, в том числе он сможет предложить решение, отвечающее требованиям по безопасности персональных данных.

За последние несколько лет существенно пересмотрен подход к аутсорсингу в области защиты данных и к концепции облачных сервисов. С точки зрения аутсорсинга функций информационной безопасности сейчас предъявляются требования по разделению ответственности за обработку и защиту данных между заказчиком и провайдером.

В настоящее время возможно «приземлить» облачную инфраструктуру в конкретный дата-центр и рассматривать ее как распределенную информационную систему, выстраивая защиту в соответствии с моделью угроз такого объекта защиты. Для этого сервис-провайдером должны быть выполнены требования законодательства о лицензировании отдельных видов деятельности и об установлении специальных требований по информационной безопасности относительно различных категорий защищаемой информации, то есть различных видов тайн, персональных данных и т. д.

Основное преимущество подобной защищенной среды – возможность значительного (в ряде случаев – до 80 %) снижения стоимости владения средствами защиты информации (СЗИ) при потреблении равного по возможностям их функционала. Инфраструктура ЦОД реализует защиту от угроз с использованием промышленных периметровых СЗИ: сред виртуализации, анализа защищенности, предотвращения и обнаружения вторжений, защиты от распределенных атак отказа в обслуживании, антивирусной защиты, криптографической защиты каналов связи. Причем все эти функции дублируются для обеспечения SLA провайдера. При этом заказчик должен реализовать самостоятельно лишь защиту клиентских рабочих мест и серверов на уровне ОС и выше в виртуальной среде.

Преимущество отечественных решений – это, прежде всего, соответствие требованиям российского законодательства, возможность поставки сертифицированных российскими регуляторами решений, которые могут применяться в системах, обрабатывающих защищаемую законом информацию, или в отношении которых должна быть проведена оценка соответствия тем или иным требованиям нормативных документов и выдан аттестат соответствия. «Неподвластность» санкциям и русскоязычная техподдержка также является серьезным преимуществом российских производителей по сравнению с иностранными компаниями.

Для эффективной защиты облаков требуются новые средства защиты, эволюция которых только стала набирать ход, так как обеспечить защиту данных на выделенных серверах и на разделяемом серверном оборудовании – далеко не одно и то же. Кроме того, повышение утилизации серверного оборудования в облаке диктует более жесткие требования к потребляемым СЗИ вычислительным ресурсам.