HA/DR-решения – работоспособность в условиях постоянных изменений

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

Алексей Чеканов – генеральный директор, компания Almitech

Введение

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

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

Тестирование HA/DR-систем

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

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

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

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

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

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

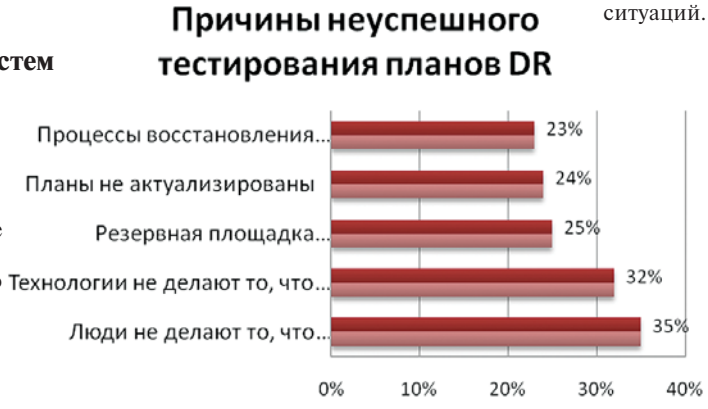

Рис. 1. Причины неуспешного тестирования планов послеаварийного восстановления

Основные причины неработоспособности DR-решений

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

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

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

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

Новый термин – Disaster Recovery Management

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

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

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

Рынок решений DRM

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

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

Заключение

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

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

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

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

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

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

видим достаточно широкое поле для внедрения новых технологий.

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

Алексей Чеканов,
компания Almitech

HDCS выбирает 3PAR

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

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

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

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

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

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