УДК 004.05

ОБЕСПЕЧЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ IT-СЕРВИСОВ

Акамова Н.В.[1], Голяев С.С.[1], Правосудов Р.Н.[1]

[1]АНОО ВО ЦС РФ Саранский кооперативный институт (филиал) Российский университет кооперации, Саранск, Россия (430027, г. Саранск, ул. Транспортная, 17), e-mail: wakamow@yandex.ru

В настоящее время все большую роль вдеятельности крупных предприятий, компанийприобретает надежность и бесперебойность работы IT-сервисов, на основе специализированных программно-аппаратных платформ.Экономические потери от снижения их эффективности или полного отказа как результата ненадежного функционирования очевидны. В зависимости от размера компании финансовые потери могут быть значительными. От ИТ-подразделений требуется обеспечение минимальных показателей времени восстановления (RTO) и допустимого объема потери данных (времени точки возврата– RPO). В статье рассматриваются основные мероприятия по повышению уровня надежности комплексных централизованных систем, обеспечивающих автоматизацию бизнес-процессов. Дан анализ схем “холодного” и “шахматного” резервирования. Рассмотрены технические решения для создания резервных центров обработки данных.Обращается внимание на то, что наивысший уровень безопасности IT-сервисовможет дать система хранения данныхреализующая единое виртуальное пространство путем объединения основного и резервного центров обработки данных.

Ключевые слова: центр обработки данных, резервирование, резервный центр обработки данных.

THE FAULT-TOLERANCE MAINTENANCE OF IT–SERVICES

Akamova N.V.[1], Golyev S.S.[1], Pravosudov R.N.[1]

[1]The Saransk Cooperative Institute (branch) Russian University Cooperation, Saransk, Russia (430027, Saransk, str. Transportnaya, 17), e-mail:wakamow@yandex.ru

Nowadays, the reliabilityand continuityof IT-servicesbased on specialized hardware and software platforms play an increasing role in the activities of large enterprises and companies. Economic costs of reducing their efficiency or total failure as a result of unreliable operation are obvious. Depending on acompany size the financial loss can be substantial. From IT departments need to ensure minimum performance recovery time (RTO) and the allowable amount of data loss (time point of return - RPO) rare needed to be ensured. The article discusses the main measures to improve the reliability of complex centralized systems to automate business processes. The analysis of the schemes of "cold" and "chess" redundancy is given. The technical solutions for creating backup data centers. Attention is drawn to the fact that the highest level of security IT-services can be provided bystorage system implementing a single virtual space by combining the primary and backup data centers.

Keywords: data center, reservation, backup data center.

Значительное увеличение количества, многообразия и сложности информации является отличительной чертой современного общества. Существующая в настоящее время тенденция передачи функций управления электронно-вычислительным машинам требует ответственного подхода их создателей к вопросам обеспечения надежности управляющих машин.Прямые экономические потери от снижения эффективности подобных систем (вплоть до полного отказа в результате их ненадежного функционирования) очевидны. Поэтому возникает необходимость в дополнительных затратах на повышение надежности информационных систем (ИС) в процессе эксплуатации, которые могут составлять десятки миллиардов рублей [2].

Во всем мире в настоящее время возрастает интерес к вопросам построения эффективных центров обработки данных (ЦОД) – отказоустойчивых комплексных

централизованных систем, обеспечивающих автоматизацию бизнес-процессов с высоким уровнем производительности и качеством предоставляемых сервисов. В России рынок услуг ЦОД-ов (дата-центов) начал формироваться в 2000 году [4]. Основными владельцами локальных ЦОД являются банки, страховые компании, финансовые институты, интернет-провайдеры, операторы связи, крупные проектные институты, научно-исследовательские центры и другие организации, использующие в своей деятельности высоко критичные IT – сервисы и/или обработку больших массивов данных. Основными технологиями при построении ЦОД на данный момент являются: виртуализация, кластеризация, горизонтальное масштабирование, резервирование. Основная задача при этом – обеспечение отказоустойчивой работы ИС, обеспечивающих бизнес-процессы компании. Развитие облачных сервисов выдвигает новые возрастающие требования к построению ЦОД[5], и соответственноих отказоустойчивости.

Иногда кроме отказоустойчивости рассматривается понятие катастрофоустойчивости [3] ЦОД, в котором речь идет о полном или частичном физическом разрушении технологической площадки дата центра и полной потери данных. Однако катастрофоустойчивость можно считать частным случаем общего определения отказоустойчивости ИС. Потеря данных компанией в результате разрушения ЦОД является событием маловероятным, но, в тоже время, для большинства коммерческих компании решающим для существования бизнеса. Основным способом защиты от подобного рода рисков является построение территориально разнесенных вычислительных площадок с функцией резервирования. В идеальном случае они имеют тождественное по составу и функционированию оборудование. Задача, возлагаемая на резервный центр обработки данных (РЦОД) – иметь актуальную копию данных основного центра (ОЦОД) и резервные сервера, обеспечивающие полномасштабное функционирование основных сервисов системы[1]. Кроме того, для защиты от локальных неисправностей в оборудовании, сбоя в программном обеспечении и прочих причин, способных привести к недоступности системы, на локальной площадке также используются локальные средства защиты, такие как кластеризация, средства резервного копирования и т.д.

На данный момент наиболее применяемыми в реализации РЦОД являются схемы “холодного” или “шахматного” резервирования. “Холодное” резервирование заключается в наличие резервных дублирующих схем в РЦОД, не участвующих в продуктивной эксплуатации. “Шахматное” резервирование аналогично “холодному”, но обеспечивает распределение продуктивных информационных систем (ИС) по основному и резервному ЦОД-ам для уменьшение (вдвое) количества восстанавливаемых систем в случае необходимости.

Схемы “холодного” и “шахматного” (active-passive) резервирования базируются на технологиях автоматического создания актуальной копии данных ИС и поддержания симметричного состояния вычислительного комплекса в резервном ЦОД. Для создания и поддерживание в актуальном состоянии копий данных в РЦОД в основном применяются следующие технологии:

– Oracle Data Guard (Stand By копия БД Oracle) и подобные от других производителей СУБД;
– Синхронная или асинхронная репликация средствами дисковых массивов;
– Синхронная или асинхронная репликация программными средствами;
– Создание и автоматизированное восстановление данных в РЦОД средствами резервного копированияи т.д.

Основные недостатки данных схем резервирования заключаются в применении технологий, требующих значительного времени на восстановление за счет необходимости выполнения обязательных вспомогательный действий, таких как:

– проверку доступности комплекса к восстановлению;
– подключения копий данных к целевым серверам;
– проведения проверки целостности данных;
– активизации бизнес процессов;
– проверки взаимодействия ИС со смежными системами.

Время переключения работы ИС компании в РЦОД составляет время восстановления (RTO), размер потерянных данные составляют точку восстановления (RPO). Для большинства коммерческий компаний простой бизнес-критических систем или потеря данных приводит к потере прибыли или, в некоторых случаях, убыткам. В зависимости от размера компании финансовые потери могут быть значительными. Например, в апреле 2000 года на восемь часов (почти всю торговую сессию) были парализованы торги на Лондонской фондовой бирже из-за ошибок в работе программного обеспечения. Убытки оценили в несколько миллионов фунтов[3]. В связи с этим бизнес-менеджеры компании требуют от ИТ-подразделений обеспечения минимальных показателей RTO/RPO в случае чрезвычайной ситуации. Соответственно одним из решений является использование РЦОД. В таблице 1 представлены преимущества использования резервирования уровня ЦОД.

Таблица 1 – Преимущества использования резервирования уровня ЦОД

Функционирование ИС без РЦОД			Функционирование ИС с РЦОД	
Сценарий	RTO/ RPO	Особенности восстановления сервисов и данных.	RTO/ RPO	Особенности восстановления сервисов и данных.
Потеря ОЦОД	месяц/ веч-ность	Закупка оборудования. Поиск датацентра. Восстановление систем. Данные потеряны	1 час/ 0 час	Оборудование уже есть. Данные актуальны. Потерь данных нет.

Потеря массива	месяц/ 8 часов	Закупка оборудования. Восстановление систем. Данные из резервной копии прошлого дня	0 час/ 0 час	Оборудование уже есть. Данные актуальны. Потерь данных нет.
Потеря критических каналов доступа	месяц/ 0 часов	Вероятно, можно будет собрать времянку из существующего граничного оборудования	0 час/ 0 час	Оборудование уже есть и работает.
Логическое повреждение БД	4 часа/ 8 часов	Восстановление базы данных из резервной копии прошлого дня	30 мин/ 0 час	Оборудование уже есть. Все изменения данных за сутки записаны на отдельные тома
Потеря сервера Баз данных	1 час/ 0 час	Ручное переключение на резервную копию БД	0,2 час/ 0 час	Автоматическое переключение на резервную копию БД
Потеря сервера приложений	0 час/ 0 час	Есть резервные серверы, балансировка задач обеспечена средствами приложений	30 мин/ 0 час	Оборудование уже есть. Данные актуальны. Потерь данных нет.

Достижение минимальных показателей RTO/RPO возможно при построении равноправно активных (active-active) ЦОД-ов с функцией резервирования. При данном построении предусматривается возможность расположения продуктивных экземпляров информационной системы на любом из ЦОД и прозрачная миграция между ними с отсутствием или минимальным автоматизированным прерыванием работы системы.Равноправно активная работы ИТ систем должна обеспечиваться на всех уровнях ИС:

I. Уровень доступа. Обеспечивается средствами сетевой инфраструктуры с применением динамического или постоянного доступа к сетевым ресурсам обоим ЦОД. Например, на счет использования сетевых маршрутизаторов с функцией отслеживания месторасположения запрашиваемых ресурсов.

II. Уровень вычислительных сред. Обеспечивается средствами прикладных средств кластеризации вычислительных ресурсов (например, распределенных отказоустойчивых ферм виртуализации, Stretched HA Clusters) или приложений (например, разнесенный комплекс Oracle RAC) между технологическими площадками.

III. Уровень хранения данных. Обеспечивается средствами дисковых систем хранения с применением дублирования данных между технологическими площадками.

Основной проблемой построения равноправно активных ЦОД является обеспечение актуальных целостных данных одновременно на основном и резервном ЦОД-ах с возможностью одновременного доступа к данным с обеих технологических площадок.

Производители решений для дисковых подсистем хранения в настоящий момент имеют в своем портфолио решения, которые позволяют решить или минимизировать вышеуказанные проблемы. Примерами таких решений являются:

1. Комплекс дисковой виртуализации EMC VPLEX;
2. Комплекс дисковой виртуализации IBM SVC;

3. Распределенный режим работы (MetroCluster) системы хранения NetApp FAS-series.

Данные продукты предназначены для абстрагирования используемых дисковых ресурсов от их физического размещения и количества резервируемых копий. Т.е.системы обеспечивают наличие резервируемых копий данных в основном и резервном ЦОД с предоставление ресурсов в виде единого тома данных. Обобщенная схема представления данных в данном случае представлена на рисунке 1:

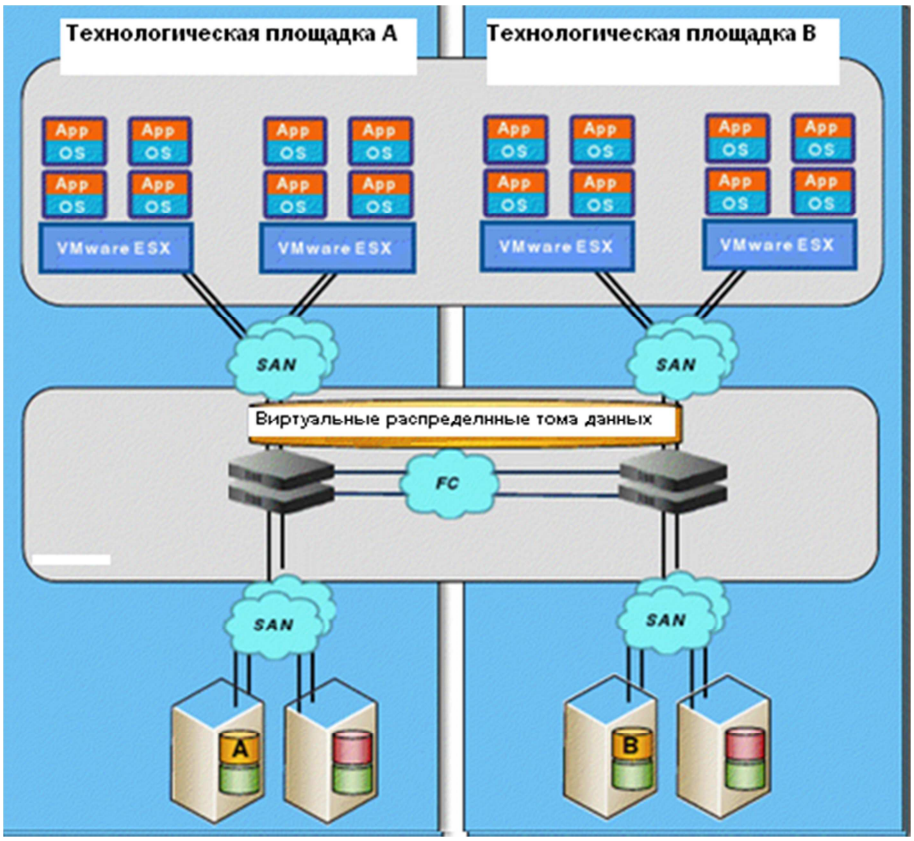

Рисунок 1 –Обобщенная схема представления данных

Применение данных продуктов в совокупности с программными механизмами резервирования вычислительных мощностей, таких как распределенные отказоустойчивые или равноправные кластеры для аппаратных и виртуальных сред и программных средств, позволяют исключить или свести к минимуму показатели RTO/RPO в случае чрезвычайной ситуации.

Таким образом, создание резервного ЦОД, отвечающего требованиям компании по уменьшению показателей RTO/RPO, предполагает построение единой отказоустойчивой инфраструктуры на всех уровнях работы ИС.

Программно-аппаратные решения подобного класса не являются гарантированным решением обеспечивающим отказоустойчивость и быстрое реагирование на чрезвычайные ситуации. Обеспечение непрерывности IT – сервисов бизнес-ориентированных ИС является

комплексной задачей включающей в себя создание внутренних процессов компании ориентированных на:

1. Создание и развитие программно-аппаратных комплексов (ПАК);
2. Эксплуатацию ПАК;
3. Разработку и поддержание комплекса действий при устранении чрезвычайной ситуации.
4. Мониторинг работы ПАК и оперативное реагирование на чрезвычайную ситуацию.

Однако, в совокупности затраты на построение и обслуживание РЦОД могут превысить возможные риски и потери компании от чрезвычайной ситуации. В связи с этим необходимо, при проработке подобных решений, руководствоваться принципом “от бизнеса к бизнесу”, который заключается в формировании требований к резервированию работы ИТ-системы, исходя из требований обеспечения доступности бизнес-сервисов и оценки целесообразности данного решения по финансовой признаку.

Наивысший уровень безопасности для предприятия может дать система хранения данных реализующая единое виртуальное пространство путем объединения ОЦОД и РЦОД предприятия. Данная схема обеспечивает возможности дальнейшего масштабирования ИС за счет добавления новых ресурсов без существенных изменений в архитектуре комплекса. Она не требует разработки планов восстановления для информационных систем входящих в область действия единого виртуального пространства основного и резервного ЦОД.

Список литературы

1. Мелешенко, А.В. /Рациональный подход к проектированию современного ЦОД // [Электронный ресурс] // «Журнал сетевых решений/LAN», № 07, 2009.URL:http://www.osp.ru/lan/2009/07/9600114 (дата обращения: 23.11.2014).

2. Тынчеров, К.Т. Основы теории и принципы построения отказоустойчивых вычислительных структур на основе нейронных сетей: автореферат дис. ... доктора технических наук : 05.13.15 / Тынчеров Камиль Талятович; [Место защиты: Моск. гос. авиац. ин-т]. - Москва, 2012. – 34 с.

3. Куперман М., Аверьянов Д. / Резервный центр обработки данных. Оценка надежности // [Электронный ресурс] // «Электроника НТБ», № 04, 2010.URL:http://www.electronics.ru/journal/article/75(дата обращения: 27.11.2014).

4. Харатишвили Давид/Дата-центры в цифрах и фактах // [Электронный ресурс] //КомпьютерПресс, № 8, 2009. URL:http://compress.ru/article.aspx?id=20687(дата обращения: 27.11.2014)

5. Герасимов Александр /Корпоративные и облачные дата-центры в России: перспективы конвергенции // [Электронный ресурс] // Журнал ИКС, № 08-09,2014. URL:http://www.iksmedia.ru/articles/5116648-Korporativnye-i-oblachnye-datacentr.html(дата обращения: 27.11.2014)

Рецензенты:

Свешников В.К., д.т.н., профессор, ФГБОУ ВПО «МордГПИ им. М.Е. Евсевьева», г.Саранск.

Федоренко А.С., д.т.н., профессор, ФГБОУ ВПО "МГУ им. Н.П. Огарева", г.Саранск.