Методы защиты данных: обзор решений

Публикация рассматривает различные технологии, обеспечивающие доступность, целостность и сохранность данных, а также методологию выбора решений по защите данных на базе нескольких основных показателей применительно к разным секторам рынка на основе продуктов компании HDS.

Введение

Цель любой компании, чей бизнес строится на IT – минимизировать потери при возможных сбоях/отказах/проблемах/катастрофах, связанных с IT-инфраструктурой. При этом чем бóльшую доступность необходимо обеспечить, тем, как правило, требуется и более дорогое решение. Общая стратегия в подобных случаях сводится к задаче выравнивания возможных потерь (финансовых) от простоя со стоимостью самого решения (рис. 1).

На практике число параметров, которые необходимо учитывать при построении подобных решений, как и самих вариатов решений (даже одного класса) – гораздо выше. В больших центрах данных оценка показателей доступности отказоустойчивых систем – тема отдельного проекта. Задача публикации – дать общее представление всего семейства решений, используемых для повышения защиты данных, а также возможных диапазонов основных показателей, достигаемых при этом.

Рис. 1. Наиболее оптимальным IT-решением, обеспечивающим восстановление после сбоев, является то, которое по стоимости сопоставимо с убытками от самого простоя.

Классификация технологий построения отказоустойчивых решений

Выбор того или иного решения определяется на основании четырех основных показателей, это:

- *доступность* – доля времени на протяжении года (обычно), в течение которого система может простаивать;
- *RPO (recovery point objective)* – средний период времени, в течение которого можно позволить потерю данных, или как часто должны выполняться резервные копии/снимки работающих приложений;
- *RTO (recovery/recall time objective)* – максимально допустимое время восстановления работоспособности приложения;
- *стоимость* решения,

а также дополнительных требований, например, условием катастрофоустойчивости – способностью решения противостоять форс-мажорным обстоятельствам, или сценарием, в соответствии с которым происходит восстановление системы в случае сбоя/отказа/непредвиденных обстоятельств.

В целом, классификацию всех технологий для построения отказоустойчивых решений можно производить исходя из ценности данных, целостность которых необходимо поддерживать (рис. 2, *в классификации HDS – прим. ред.*). И данный подход с соответствующей таксономией (за исключением технологических особенностей) един для основных поставщиков решений по защите данных.

Рис. 2. Классификация используемых технологий для построения отказаоустойчивых решений в соответствии с ценностью данных.

Табл. 1. Пять технологических уровней поддержания отказоустойчивости

Technology Tier	RPO Range[1)]	RTO Range[1)]	Minimum # Disk Copies	Distance	Regional Disaster Support
Tier 1–Tape Backup	24–168 hours	48–168 hours	N/A	Any	возможно
Tier 2–Disk Point-in-time copies	4–36 hours	4–24 hours	3 [2)]	Any	возможно
Tier 3a–Sync	0–2 minutes	1–8 hours	2 [2)]	Limited	No
Tier 3b–Sync w/failover	0–2 minutes	5–60 minutes	2 [2)]	Limited	No
Tier 4a–Async	0–5 minutes [3)]	1–8 hours	2 [2)]	Any	Yes
Tier 4b–Async w/failover	0–5 minutes [3)]	30–90 minutes	2 [2)]	Any	Yes
Tier 5–Three data center	0–2 minutes	1–8 hours	3-7 [2),4)]	Any	Yes

1) оценки RPO и RTO представляют исследования HDS, основанные на реальном опыте клиентов в корпоративных средах
2) лучшая практика – одна дополнительная копия, для того чтобы не повлиять на сеанс реплицирования
3) сетевые проблемы увеличивают RPO
4) зависит от вендора и метода развертывания

Обобщенно, все решения по используемым технологиям условно подразделяются на 4 класса: 1) на основе/эмуляции ленточных технологий (близко к пониманию т.н. традиционного резервного копирования); 2) на локальных копиях логических томов данных (LUN); 3) на основе поддержания удаленных копий LUN; 4) кластерные удаленные решения.

В соответствии с требованиями доступности, отказоустойчивые решения подразделяют на 5 уровней (с соответствующими подуровнями) – табл. 1.

Рассмотрим основные базовые компоненты от компании Hitachi Data Systems для построения отказоустойчивых решений в соответствии с приведенной классификацией.

Компоненты построения отказоустойчивых решений

ПО для создания локальных реплик томов

Hitachi ShadowImage In-System Replication (SiSR) ПО

SiSR создает и поддерживает копию конкретного тома в пределах одной и той же системы хранения. Эта копия – полноразмерный дубль копируемого тома и занимает то же самое количество дискового пространства, как оригинал (рис. 3). ShadowImage-копии могут быть сделаны на любом типе RAID при любом размере тома и имеют полностью идентичные характеристики с оригиналом. Модульные системы класса Thunder поддерживают одну копию на первичный том и до 2047 пар томов – на систему хранения в целом.

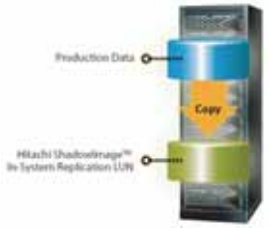

Рис. 3. В пределах системы хранения ПО ShadowImage In-System Replication создает и поддерживает полную копию LUN, которая занимает столько же места, как и оригинал.

ПО Copy-on-Write Snapshot

ПО Copy-on-Write Snapshot (ранее – QuickShadow) создает копии в виде снимков (snapshot) для конкретных точек во времени (point-in-time) специфицированных томов (рис. 4). Как и в случае с ShadowImage, Copy-on-Write Snapshot позволяет серверу продолжать

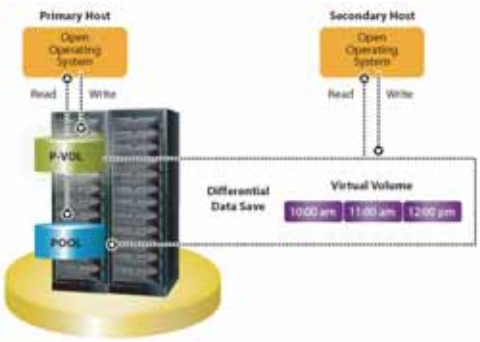

Рис. 4. ПО Copy-on-Write Snapshot при создании копии записывает только изменения к данным и указатели к первоначальным, что позволяет значительно уменьшить объем дискового пространства для копии в сравнении с ShadowImage-копированием тома..

"писать" на оригинальный том, в то время как система хранения поддерживает копирование "указателей" на измененные блоки данных в таблицу ссылок. Поскольку сохраняются только изменения в дополнение к сохраняемым указателям на первоначальные данные, количество дискового пространства, используемого снимком, значительно меньше, чем ShadowImage-копия полного тома. При снижении требований к размеру копии возрастают требования к процессорной мощности системы хранения для поддержания и обработки указателей, обеспечивающих доступ к данным оригинального тома. Серия Thunder позволяет делать до 14 snapshot-копий любого тома и до 1022 пар копий в пределах системы хранения.

ПО для создания удаленных реплик томов

ПО Hitachi TrueCopy Remote Replication

ПО TrueCopy Remote Replication подобно ShadowImage ПО в создании и обслуживании полной копии данных тома. Однако вторичная копия поддерживается на отдельной системе хранения, как показано на рис. 5. Поэтому ПО TrueCopy известно как "внешний" (удаленный) метод реплицирования в противоположность "внутреннему" (локальному) методу реплицирования ShadowImage ПО. Поскольку TrueCopy ПО работает в синхронном режиме и требует подтверждения каждой записи данных на удаленном томе перед ее продолжением, рекомендуется, чтобы резервный сайт находился в пределах 35–50 км, в зависимости от допуска на время ответа и некоторых других факторов. Системы хранения серии Thunder поддерживают до 2046 TrueCopy пар томов в одной системе.

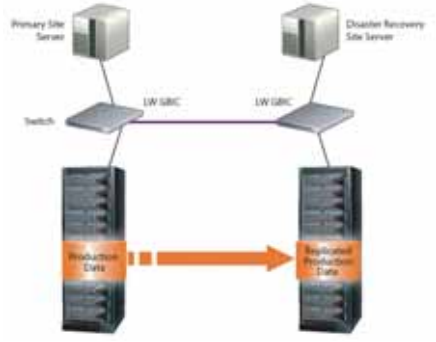

Рис. 5. ПО TrueCopy функционирует на удалении двух сайтов в пределах 35-50 км и требует подтверждения каждой синхронной записи перед продолжением.

Для монолитных систем хранения старшего класса – серии Lightning – TrueCopy используется для построения решений как в синхронном, так и асинхронном режимах, для систем серии Thunder – только в синхронном режиме.

При реализации систем с разнесенными сайтами на расстояние не более 35–50 км, как уже отмечалось, используется прямое подключение по Fibre Channel. Для асинхронного режима и расстояниях более 50 км используются протоколы (с помощью расширителей): Internet Protocol (IP), Dense Wavelength Division Multiplexer (DWDM), T1/E1, T3/E3, Synchronous Optical Network (SONET), Asynchronous Transfer Mode (ATM) и ESCON.

ПО для создания удаленных реплик томов в асинхронном режиме с расширенными возможностями

ПО Hitachi Universal Replicator for TagmaStore Universal Storage Platform

Universal Replicator – флагманское ПО в семействе продуктов HDS, позволяющее создавать отказоустойчивые географически разнесенные на любые расстояния системы с расширенными возможностями поддержания целостности данных.

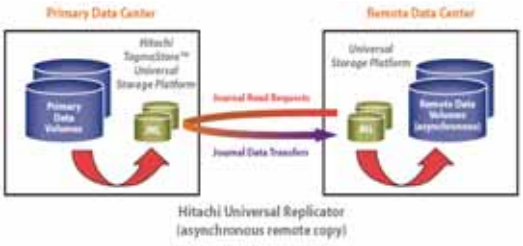

Рис. 6. Репликация под управлением Universal Replicator происходит на основе журналов записей, содержащих данные и метаданные, при поддержании всей процедуры передачи, в основном, удаленной системой хранения.

В секторе среднего бизнеса такие системы доступны, прежде всего, на базе Network Storage Controller – модели NSC55.

С целью снижения потребляемой мощности ресурсов, общей стоимости процессов и повышения эффективности Universal Replicator использует 2 ключевые технологии: журналирование (поддерживаемое на дисках) и т.н. pull-style механизм реплицирования.

Иллюстрация этих технологий представлена на рис. 6. Перед тем, как, например,

OLTP-том начинает реплицироваться на резервную удаленную USP-платформу, первичная USP-платформа записывает все записи в специальные журнальные тома на дисках.

Запись на диски вместо использования для этого кэша позволяет снять некоторые ограничения, свойственные более ранним асинхронным методам реплицирования. В дополнение к реплицируемым записям журнал содержит метаданные каждой записи с целью гарантии целостности и последовательности процесса реплицирования. Каждый передаваемый набор записей включает временную метку (только для мэйнфреймов) и информацию о порядковом номере записи, давая возможность механизму реплицирования на удаленном сайте осуществлять контроль за получением записей в правильном порядке.

Первичный сайт не посылает данные вторичному, пока не получает от него запрос. Вследствие того, что все процессы, которые управляют асинхронным реплицированием, расположены на удаленной системе, меньше ресурсов используется на основной системе, повышая таким образом ее производительность.

Все процедуры основываются на доказанных алгоритмах ПО TrueCopy и также поддерживают одновременную множественность передачи томов.

Universal Replicator позволяет повысить эффективность удаленной репликации и сделать ее более доступной. На рис. 7 представлены 3 конфигурации (одна – для сравнения, на основе TrueCopy) решений на основе использования Universal Replicator. Основные отличительные особенности:

- *2DC Asynchronous:* снижение бизнес-рисков за счет наличия удаленного сайта;
- *3DC Cascade:* синхронное реплицирование поддерживает текущую копию промышленных данных локально. Промежуточный сайт также обеспечивает удаленное реплицирование;
- *3DC Multitarget.* Синхронное реплицирование поддерживает текущую копию промышленных данных локально с возможностью восстановления.

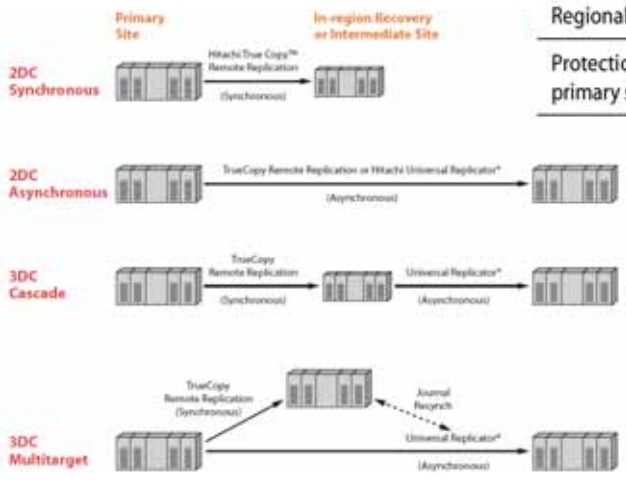

Рис. 7. Основные конфигурации построения отказоустойчивых центров на основе использования ПО Universal Replicator и TrueCopy.

Табл. 2. Сравнение основных показателей различных конфигураций отказоустойчивых решений (см. рис.7)

Data Center Strategy	1DC*	2DC		3DC	
Remote Replication Configuration	Local	Sync with Failover	Async out of Region	Cascade	Multitarget
Technology					
Synchronous Replication	n/a	TC	n/a	TC	TC
Asynchronous Replication	n/a	n/a	TC/A, UR	UR	UR
Characteristics					
Recovery locations supported	0	1	1	2	2
In-region site failover	No	Yes	No	Yes	Yes
Out-of-region site failover	No	No	Yes	Yes	Yes
"No data loss" available	No	Yes	No	Yes	Yes
Minimum # of logical full-volume copies **	1	2	2	3	3
Primary Site Failure					
RPO	24–168 hours	0–2 minutes	0–5 minutes	0–2 minutes	0–2 minutes
RTO***	48–168 hours	5–60 minutes	1-8 hours	5–60 minutes	5–60 minutes
Regional Disaster					
RPO	24–168 hours	24–168 hours	0–5 minutes	0–5 minutes	0–5 minutes
RTO	48–168 hours	48–168 hours	1–8 hours	1–8 hours	1–8 hours
Impact of single failure outside primary site					
Recovery/intermediate site failure (primary still up)	n/a	No DR	n/a	No DR	OK
Remote out-of-region site failure (primary still up)	n/a	n/a	No DR	OK	OK
Link failures only—primary to in-region	n/a	No DR	n/a	No DR	OK
Link failures only—primary to out-of-region remote	n/a	n/a	No DR	n/a	OK
Link failures only—intermediate to remote	n/a	n/a	n/a	OK	n/a

Табл. 3. Качественное сравнение различных конфигураций отказоустойчивых решений (см. рис.7)

Data Center Strategy	1DC	2DC		3DC	
Replication Configuration	On-site	Sync Near	Async Far	Cascade	Multitarget
Primary Site Failure/failover					
Speed of recovery (RTO)	bad	better	good	better	better
Data currency (RPO)	bad	better	good	better	better
Regional disaster (RTO)	bad	bad	good	good	good
Protection after failure outside primary site	n/a	bad	bad	depends	better

Отдельный асинхронный процесс реплицирования копирует данные от первичного сайта до удаленного сайта восстановления по отдельной сети. Данная конфигурация также поддерживает реплицирование и катастрофоустойчивость промежуточного сайта к удаленному асинхронно от первичного. До сих пор 3DC многоцелевые решения были развернуты только в самых критичных бизнес-инфраструктурах. При использовании Universal Replicator такие конфигурации доступны и для более широкого диапазона компаний и приложений.

Общее сравнение конфигураций дано в табл. 2, качественное сравнение – в табл. 3.

ПО управления репликами томов для поддержания непрерывности бизнеса

Hitachi Business Continuity Manager (BCM) ПО

ПО Hitachi Business Continuity Manager (*ранее – CopyCentral*) позволяет умень-

шить сложность и упростить управление отзазоустойчивыми системами и их компонентами на базе единого централизованного инструментального средства. BCM поддерживает: Hitachi TrueCopy, Hitachi ShadowImage, Hitachi Universal Replicator, Universal Storage Platform (USP), а также дисковые системы класса Lightning, Thunder и TagmaStore AMS/WMS.

ПО управления резервным копированием/восстановлением

ПО Hitachi HiCommand Backup Services Manager (BSM)

Данное ПО представляет собой нижний класс продуктов (см. рис. 2), используемых для поддержания целостности бизнеса, но в то же время может использоваться как дополнительная компонента во всех решениях более высокого уровня.

Как показывают исследования Enterprise Strategy Group, около 35% всех операций резервного копирования/восстановления (РКВ) по разным причинам не завершаются успешно. Другие исследования, проведенные InfoStor, выявили следующую классификацию проблем, связанных с РКВ. 36% респондентов заявили, что они достоверно не знают, копировали ли они соответствующие данные. Для 24% опрошенных восстановление было самой большой проблемой, для 25% – большой трудностью было управление множественными устройствами резервного копирования/восстановления, а 15% – заявили, что им трудно было "вписаться" в выделенное окно для резервного копирования.

BSM с включенной в пакет функциональностью от компании APTARE во многом позволяют избежать этих сложностей и практически добиться 100%-го выполнения всех операций, связанных с РКВ.

Это достигается за счет полной визуализации текущего и прогнозируемого состояния всех процессов РКВ, а также носителей информации (по длительности хранения, использованию картриджей, взаимосвязи с приложениями и т.д.) с возможностью доступа к данным через web-браузер (рис. 8). С помощью задания правил управления РКВ администратор может добиваться максимального соответствия процедур РКВ, требуемым SLA.

Администратор также имеет простую визуализацию последовательности своих действий при самых разнообразных возможных вариантах восстановления (приложения, файла, восстановление на дату/время и т.д.). В целом, за счет использования BSM достигается повышение доступности, управляемости, снижение затрат (на управление, материальное обеспечение и др.).

BSM интегрируется с другими пакетами данного класса, в частности, с VERITAS NetBackup и IBM Tivoli Storage Manager.

Примеры дополнительных решений

Пример 1. Бессерверное резервное копирование на ленту

С помощью ShadowImage ПО (в составе системы хранения HDS) и поддерживающего ПО, например Symantec NetBackup 4.5, можно организовать процедуру бессерверного резервного копирования рабочего тома данных на ленту с нулевой задержкой для активных приложений. Общая схема решения представлена на рис. 9.

Процедура состоит из следующих шагов:

- мастер-сервер дает команду для выполнения копии рабочего тома;
- Hitachi ShadowImage делает вторичную копию (S-VOL);
- по LAN клиент посылает информацию медиа-серверу о готовности и местоположении копии;

Рис. 8. С помощью одного взгляда на окно "my.Backup Services Manager home page" администратор может быстро определить состояние ("успешно", "аварийно") завершения процессов резевного копирования.

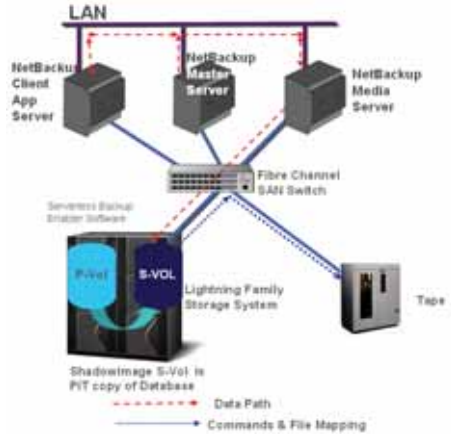

Рис. 9. Структурная схема решения с использованием ShadowImage ПО (в составе системы хранения HDS) и поддерживающего ПО – Symantec NetBackup 4.5 для организации процедуры бессерверного резервного копирования рабочего тома данных на ленту с нулевой задержкой для активных приложений.

- медиа-сервер посылает SCSI-команду дисковой системе Lightning о выполнении бессерверного резервного копирования;
- ПО Serverless Backup Enabler читает S-VOL и записывает его через SAN на ленту.

Пример 2. Автоматическое восстановление работоспособности системы в случае отказа

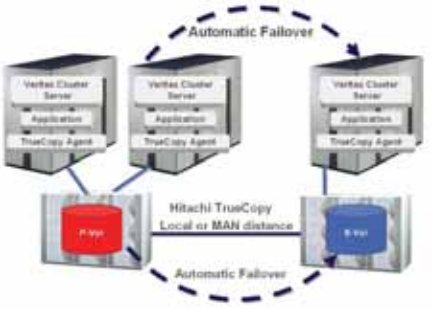

Рис. 10. Организация отказоустойчивой географически разнесенной системы с автоматическим переключением на резервный центр в случае чрезвычайных обстоятельств.

С помощью TrueCopy, Veritas Cluster Server, а также Hitachi TrueCopy Agent for Veritas Cluster Server организуется отказоустойчивая географически разнесенная система с автоматическим переключением на резервный центр в случае чрезвычайных обстоятельств (рис. 10).

Заключение

Современный бизнес во многом уже напрямую стал зависеть от IT и возможностей центров данных обрабатывать огромные и постоянно увеличивающиеся объемы данных, а, соответственно, и от возможностей IT-персонала поддерживать непрерывность и целостность бизнес-процессов.

Примеры представленных продуктов от Hitachi Data Systems позволяют строить подобные решения и поддерживать высокий уровень их доступности, а также оптимизировать работу приложений, одновременно улучшая работу IT-персонала путем автоматизации задач управления и технического обслуживания.

Александр Гончаров,
компания VERYSELL Distribution