Игорь Берин
Константин Баканович

ОТКАЗОУСТОЙЧИВЫЕ СХД

НА БАЗЕ ОТКРЫТОЙ ПЛАТФОРМЫ ОТ STORUS

Решения, предлагаемые сегодня «гигантами» индустрии, обеспечивают сервисы только между массивами собственного производства, причем, зачастую, только между определенными моделями, так как сервисы обеспечиваются либо на уровне контроллеров дисковых массивов (Hitachi Data System), либо при помощи дополнительных аппаратно-программных модулей, по сути своей, являющимися мощными серверами (HP, EMC, IBM). По своей стоимости, такие решения сегодня недоступны для подавляющего большинства организаций в Восточной Европе, планирующих внедрение SAN с высокой доступностью и развертывание резервных центров данных.

ОТКРЫТАЯ ПЛАТФОРМА ОТ STORUS

Осознавая существующую проблему ограниченности бюджетов и актуальность совершенствования ИТ инфраструктур в государственном секторе и бизнесе в направлении повышения доступности и безопасности, Storus разработал открытую платформу для построения высоконадежных сетей хранения данных. Она обладает характеристиками решений корпоративного уровня, такими как ***виртуализация***, ***snapshot***, ***репликация***, ***миррорингиback-up (резервное копирование)*** данных как в рамках одного центра данных, так и между несколькими центрами, разнесенными территориально.

Открытая платформа состоит из трех уровней (рисунок на развороте). Уровень коммутации, включающий в себя адаптеры шины хоста (HBA) и коммутаторы Qlogic [4], уровень сервисов, которые обеспечиваются аппаратно-программным модулем IPStor производства компании FalconStor [5] и уровень хранилищ данных, состоящий из дисковых, ленточных и оптических систем различных производителей.

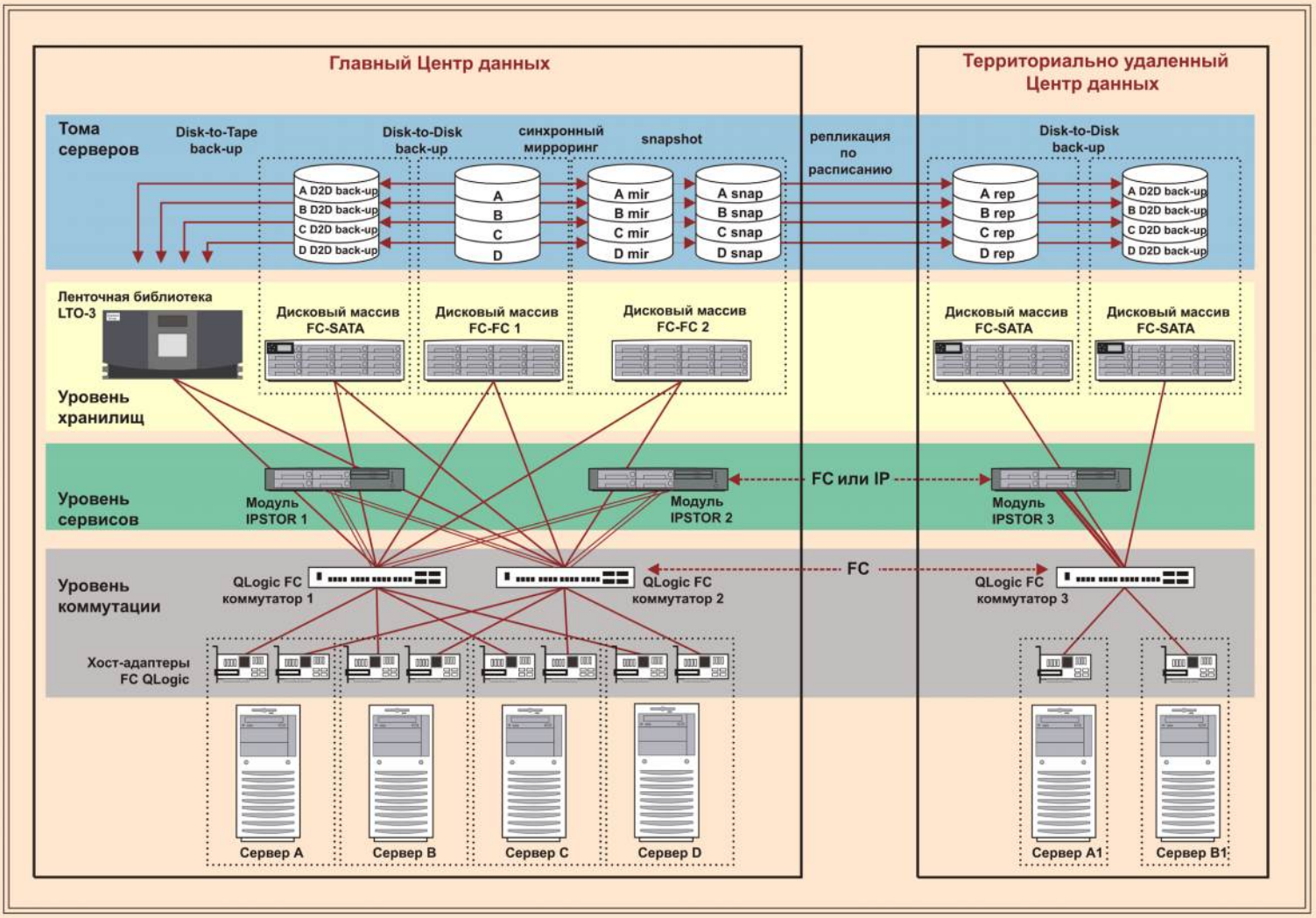
Уровень коммутации связывает хосты и хранилища по протоколу Fibre Channel. Этот уровень обеспечивает множественность путей доступа к данным в рамках сети хранения, позволяет достигнуть высокой доступности данных вне зависимости от отказа в одном из каналов передачи данных, так как управляющее программное обеспечение автоматически переключит пользовательские хосты на резервный путь передачи данных. Кроме этого, в случае необходимости возможно создание баланса на-

STORUS

На заре развития технологий хранения данных преобладали решения, такие, как дисковые массивы с технологией RAID (1994), непосредственно подключаемые к серверам по Parallel SCSI (Direct Attached Storage, DAS), и специализированные файл серверы для обеспечения доступа к файловым ресурсам по сетям Ethernet (Network Attached Storage, 1998). С ростом количества серверов и дискового пространства в организациях требовалось все больше ресурсов для администрирования ИТ инфраструктур, а надежность последних и доступность данных в них снижались в обратной пропорции. В то же время, основным препятствием на пути вывода ресурсов хранения за рамки отдельных серверов и перевода их в коллективное пользование являлись ограничения по адресному пространству и расстояниям протокола Parallel SCSI, служившего основным протоколом доступа приложений к данным.

С началом использования протокола Fibre Channel (1995) [1], а в дальнейшем iSCSI (2001) [1] для организации последовательной передачи команд SCSI, открылись возможности сетевого доступа к коллективным дисковым и ленточным ресурсам на уровне физического блока данных на больших расстояниях и с высокой степенью надежности. Настала эра сетей хранения данных (SAN).

В настоящее время актуальность решений с использованием сетей хранения данных не вызывает сомнений. Такие сети развертываются там, где присутствуют высокие требования к производительности, надёжности и управляемости информацией. В своем классическом исполнении технология SAN позволяет "нарезать" емкость дискового массива на доли и раздать их серверам. Причем эти доли могут иметь различные уровни RAID. Вне зависимости от используемого протокола в SAN, сервер видит свою долю как свой внутренний SCSI диск. Хотя это и решает некоторые проблемы администрирования и ИТ инфраструктуры в целом такие, например, как избыток персонала, низкая доступность данных, неэффективное использование дискового пространства, зависимость хранилища от конкретного сервера. Но в целом, ряд вопросов все еще остается открытым. Как при ограниченном бюджете построить отказоустойчивую SAN? Как обеспечить сервисы дублирования данных и back-up [2] в разнородных SAN, сохраняя открытость архитектуры и независимость от одного производителя? Как развернуть резервный центр данных [3], не затрачивая на это баснословные суммы?



грузки, т.е. одновременное использование двух или более альтернативных путей в сети передачи данных, что позволяет добиться требуемого уровня пропускной способности и обеспечить более равномерную загрузку каналов передачи данных.

Уровень сервисов обеспечивает дублирование данных в виде создания полной копии рабочего тома, snapshot, репликации, синхронного либо асинхронного миррорингa и back-up на ленту и/или диск через FC или iSCSI.

Уровень хранилищ представляет собой дисковые и ленточные хранилища, поставляемые Storus (*www.storusint.com*) либо любые другие, предпочитаемые заказчиком.

СЕРВИСЫ В ОТКРЫТОЙ ПЛАТФОРМЕ ОТ STORUS

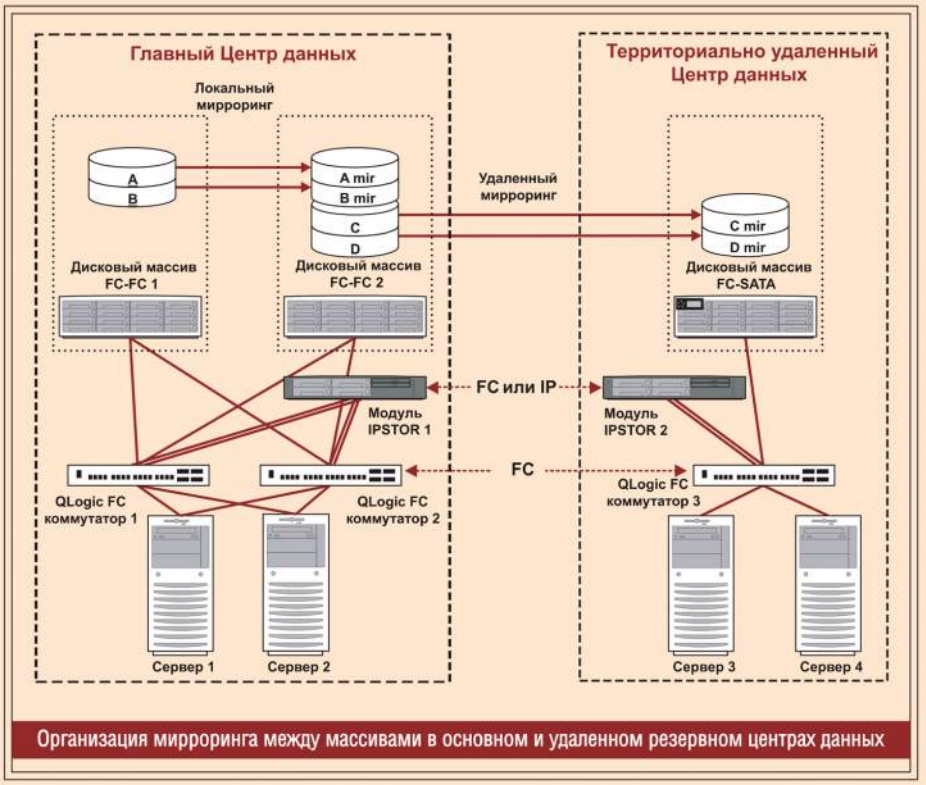
Миррорингг – выполняемый на уровнях дисков, виртуальных устройств, LUNов или хранилищ сервис зеркалирования, обеспечивает высокий уровень доступности данных и увеличивает защищённость от программных и аппаратных сбоев, которые могут возникнуть непосредственно в хранилищах, в каналах передачи данных и т.п. При реализации миррорингa данные, записанные на первичном объекте хранения, одновременно записываются на вторичный объект, где, таким образом, обеспечивается хранение точной копии данных. В случае невозможности доступа к первичному объекту хранения пользовательский запрос на запись/чтение данных автоматически адресуется к вторичному объекту хранения данных. Существуют решения как аппаратной реализации миррорингa, например, на уровне коммутаторов [6], так и с использованием программно/аппаратных решений. Миррорингг может выполняться в синхронном или в асинхронном режиме. При работе в синхронном режиме физический блок не будет записан на первичный массив до тех пор, пока контроллер резервного массива не пришлёт подтверждения успешной записи. Асинхронный миррорингг предполагает запись на первичный массив сразу же, без ожидания подтверждения успешности записи на резервном массиве. При использовании синхронного миррорингa рекомендуется использовать

массивы, обладающие примерно равными характеристиками производительности, так как в противном случае общая производительность системы будет определяться менее производительным устройством.

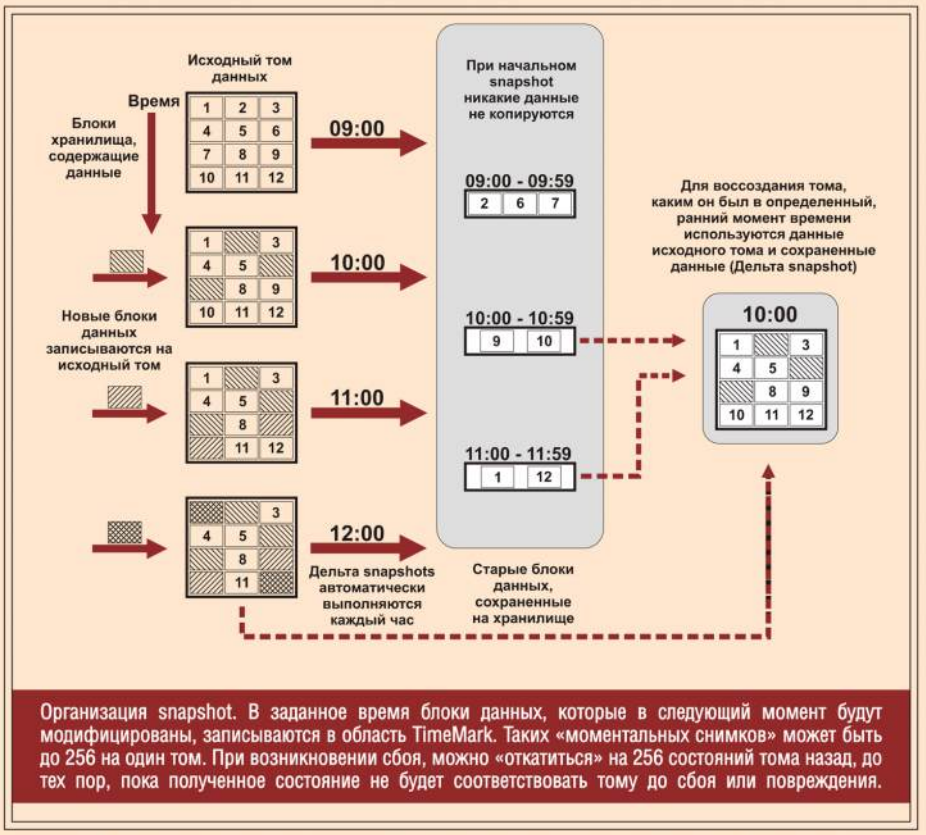
Репликация – сервис, обеспечивающий защиту от катастроф посредством создания удалённой копии данных. После первоначальной синхронизации данных очередные обновления передаются от первичного массива к реплике либо по заранее заданному расписанию, либо по достижению измененными данными порогового объёма. При возникновении сбоя и потере доступа к первичному объекту хранения в течение короткого времени пользовательские запросы могут быть перенаправлены к реплике. Так как при синхронизации первичных данных и реплики и непосредственно во время репликации передаются только изменения, а не весь объём данных, для связи между центрами данных возможно использование каналов передачи данных с достаточно невысокими характеристиками, в частности WAN/IP.

Репликация данных может выполняться как на уровне блоков, так и на файловом уровне. При файловой репликации можно непосредственно указывать, какие именно каталоги и файлы необходимо копировать. Блочная репликация использует в качестве копируемых объектов логические единицы (logical units, LUNs). В этом случае процесс репликации становится независимым от используемых типов файловых систем.

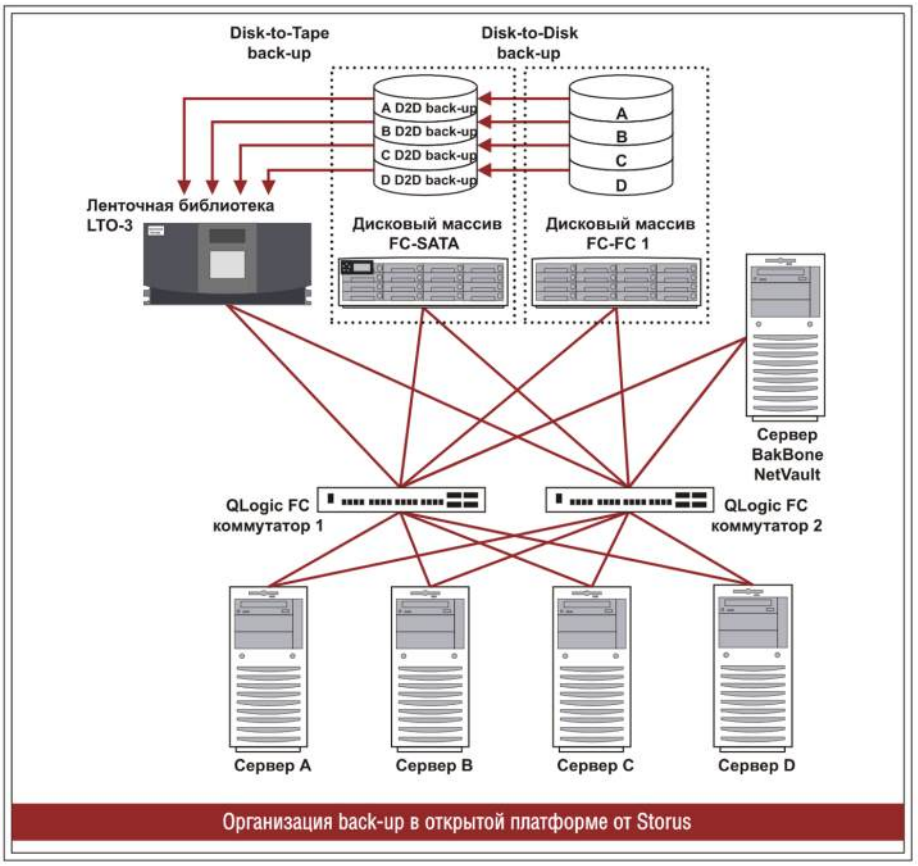
Snapshot Copy. Сервисы создания мгновенных снимков данных позволяют обеспечить быстрое восстановление данных после сбоев, большей частью программных, таких как вирусные атаки, ошибки в ПО и т.п. или вызванных человеческим фактором. При реализации подобных сервисов автоматически по расписанию или по иным правилам создаются копии данных, привязанные к определённым точкам во времени. При этом возможно необходимо создание только одного полной копии данных в первоначальный момент (Snapshot Copy). В дальнейшем копируются только данные, которые будут изменены, что позволяет снизить как общий объём хранимых данных, так и требования к пропускной способности каналов передачи данных (TimeMark™) [7].



Организация миррориинга между массивами в основном и удаленном резервном центрах данных



Организация snapshot. В заданное время блоки данных, которые в следующий момент будут модифицированы, записываются в область TimeMark. Таких «моментальных снимков» может быть до 256 на один том. При возникновении сбоя, можно «откатиться» на 256 состояний тома назад, до тех пор, пока полученное состояние не будет соответствовать тому до сбоя или повреждения.



Организация back-up в открытой платформе от Storus

Кроме защиты от сбоев, рабочую копию тома удобно использовать для организации с нее back-up, миррорингa или удаленной репликации.

Back-up в сетях хранения данных [8]

Открытая платформа от Storus решает три основные проблемы выполнения back-up и восстановления данных, с которыми организации сталкиваются сегодня. Во-первых, разгрузка трафика локальной сети путем "убирания" трафика back-up в сеть хранения данных. Во-вторых, разгрузка серверов приложения, путем осуществления централизованного back-up. В третьих, сужение окна back-up до минимума путем использования иерархического метода (сначала back-up на диск, затем с диска на ленту). Back-up может осуществляться как на уровне файловой системы или записей баз данных, так и на блоковом уровне, когда ПО back-up видит данные не виде файлов, а в виде физического тома. В последнем случае, файловая система серверов приложений "не знает" когда происходит back-up. Поэтому, агенты открытых файлов и баз данных на серверах не требуются. Для блокового back-up рекомендуется использование рабочей копии тома (snapshot copy).

В качестве ПО для back-up в решении от Storus используется продукт NetVault компании BakBone [9].

ЗАКЛЮЧЕНИЕ

Основным преимуществом открытой платформы от Storus является независимость от одного производителя. Она позволяет использовать разнородное оборудование и осуществлять сервисы между хранилищами с различными типами носителей (SCSI U320, FC, SAS, sATA, sDLT, LTO, DVD, UDO). Это значительно сокращает инвестиции в инфраструктуру и ускоряет их возврат. Данное решение - это гибкий инструмент для разработчика стратегии ИТ. Оно призвано ускорить внедрение отказоустойчивых сетей хранения данных с высокой доступностью и развертывание резервных центров данных в организациях и на предприятиях. Это, несомненно, является главным условием безопасности и эффективности ведения государственной и хозяйственной деятельности.

Специалисты Storus всегда готовы предоставить вам квалифицированные консультации и решения (www.storusint.com)!

STORUS

ССЫЛКИ:

[1]. http://www.storusint.com/articles/protocols.htm
[2]. http://www.storusint.com/articles/rk.htm
[3]. http://www.storusint.com/articles/san.htm
[4]. http://www.storusint.com/products/connectivity_san.htm
[5]. http://www.storusint.com/vendors/falconstor.htm
[6]. http://www.falconstor.com/solutionsforcisco.asp
[7].http://www.falconstor.com/disasterrecovery.asp
http://www.storusint.com/solutions/disaster_recovery.htm
[8]. http://www.storusint.com/solutions/backup_recovery.htm
[9].http://www.storusint.com/products/software_bakbone.htm

Тел/факс: +7 (095) 775-33-76
e-mail: info@storus.ru
121609, Москва,
Рублевское шоссе, д. 36,
корпус 2, офис 248