

# Бэкап от NetApp

Обзор тенденций на рынке решений резервного копирования/восстановления данных с акцентом на технологии, предлагаемые компанией NetApp.



Солонин Сергей – руководитель проектного отдела группы компаний “Тетроникс”.

## Введение

Недавно агентство Vanson Bourne опубликовало результаты исследования *European Disaster Recovery Survey 2011*, посвященного проблемам резервного копирования и аварийного восстановления данных в европейских компаниях<sup>\*)</sup>. Результаты исследования говорят о недостаточно высоком уровне защищенности компаний от потери данных и перебоев в работе ИТ. Практически три четверти (74%) европейских компаний не уверены, что смогут полностью восстановить системы и данные после аварии, а более половины компаний (54%) теряли данные или сталкивались с проблемами в работе ИТ в течение последних 12 месяцев.

Для резервного копирования и восстановления данных по-прежнему широко распространены ленточные устройства (их используют 40% компаний). Однако 80% компаний, использующих ленту, хотели бы согласно результатам исследования, отказаться от нее. В списке основных причин для возможной миграции на альтернативные технологии назывались: низкая скорость восстановления данных с ленты (39% ответов); необходимость более быстрого резервного копирования и восстановления (33%); низкая надежность ленты (26%).

Эту тенденцию подтверждает и другое, недавно проведенное, исследование Gartner (*The Future of Backup May Not Be Backup, 22 September 2011, Dave Russell, Research Note G00218917*). В соответствии с ним,

\*) Исследование проводилось по заказу EMC независимым исследовательским агентством Vanson Bourne. Результаты базируются на интервью со 1750 руководителями ИТ-служб частных и правительственных организаций стран Бенилюкса, Великобритании, Германии, Испании, Италии, России и Франции. В этих организациях, представляющих различные секторы экономики, включая промышленность, розничную торговлю, финансовый и телекоммуникационный сектор, работает от 250 и до 3 тысяч и более сотрудников.

к 2014 г. около 30% организаций планируют заменить свои решения по резервному копированию/восстановлению данных (РКВ) на решения от других вендоров из-за стоимости, сложности и/или отсутствия необходимых возможностей. А к 2015 г. не менее 10% крупных компаний будут переходить от традиционных последовательных процедур РКВ на моментальные снимки с использованием технологий репликации.

В качестве основных драйверов таких перемен можно отметить:

- снижение общей стоимости процедур РКВ;
- упрощение управления процедурами РКВ;
- повышение надежности выполнения процедур РКВ;
- необходимость унификации процедур РКВ с возможностью поддержки виртуальных инфраструктур и распределенных локаций;
- повышение производительности процедур РКВ.

В соответствии с последним отчетом Gartner (*Magic Quadrant “Enterprise Disk-Based Backup/Recovery, January 2011” Dave Russell, Sheila Childs, Alan Dayley*), NetApp максимально приблизилась к группе лидеров. Сама NetApp во многом это объясняет: 1) удачной интеграцией собственных и ведущих решений по управлению процедурами РКВ от других разработчиков (поставляются NetApp по OEM-соглашениям) с собственными технологиями типа моментальных снимков (Snapshot) и disk-to-disk (D2D) процедурами РКВ; 2) гибкой лицензионной политикой; 3) гибкими возможностями по масштабированию решений РКВ.

## Семейства решений NetApp для управления процедурами РКВ

В настоящее время решения NetApp по резервному копированию/восстановлению (РКВ) данных представлены тремя линейками продуктов (табл. 1): NetApp SnapProtect, NetApp OnCommand и NetApp Syncsort Backup (NSB).

NetApp SnapProtect это OEM-версия решения организации резервного копирования семейства Commvault Simpana 9.

Ключевые его особенности:

- интеграция с приложениями Microsoft, Oracle, SAP, IBM;
- механизм каталога для снапшотов (что давно было нужно), как локально расположенных, так и реплицированных или на ленте;
- возможность индексации содержимого LUNов и VMware VMDK;
- резервное копирование на ленту, в том числе с дедупликацией;
- процедура Unified Restore как со снапшотов, так и с ленты или удаленной копии.

Такие семейства ПО, применяемые для создания резервных копий, позволяют максимально охватить все разнообразие задач РКВ и наиболее гибко организовать уникальный для каждой компании регламент РКВ.

Используя бесплатные компоненты от NetApp, можно организовать простую в настройке и эксплуатации, но довольно функциональную РКВ для небольших компаний.

В то же время платные компоненты позволяют разрабатывать многоуровневые схемы с постепенной миграцией резервных копий на более медленные и дешевые уровни хранения.

## Базовые компоненты решений NetApp по защите данных

В качестве основных компонент, используемых в решениях по защите данных, можно выделить следующие:

- **Snapshot-konuu** – создает моментальные снимки данных (томов, файлов и др.), работает на базе ОС Data ONTAP и поставляется бесплатно со всеми СХД NetApp;
- **SnapVault** – ПО (работает на базе ОС Data ONTAP) – обеспечивает миграцию моментальных снимков с одной

Табл. 1. Сравнительные особенности трех линеек решений РКВ NetApp.

	NetApp SnapProtect	NetApp OnCommand	Syncsort (NSB)
Management app	SnapProtect™	OnCommand*	BEX
Manages NetApp® Snapshot® copies	да	да	нет
Virtualization and application aware	да	да	да
Create and manage NetApp replication	да	да	да
Single DP interface	да	нет	да
Catalog	да	нет	да
Manage tape	да	нет	да
Supports systems with third-party storage	Not at initial release	Files and SQL Server Limited with OSSV	Files and apps

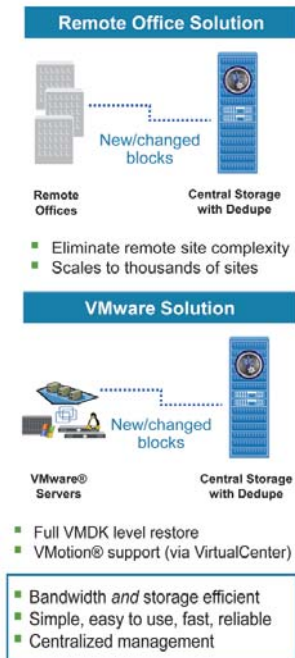


Рис. 1. Open Systems SnapVault поддерживает масштабируемость до тысяч удаленных сайтов и обеспечивает полное восстановление на VMDK-уровне.

СХД NetApp на другую, а также восстановление данных. RPO (Recovery Point Objective – определяет период времени, в течение которого можно позволить потерю данных, или как часто должны выполняться резервные копии/снимки работающих приложений) составляет 1 час и более;

- **Open Systems SnapVault** – агент для бэкапирования может быть установлен на Windows®, Linux®, UNIX®, VMware® ESX. Работает на блочном уровне, обеспечивает передачу измененных блоков данных с любой СХД на СХД NetApp, снижает нагрузку на сеть, поддерживает полное восстановление на уровне VMDK-файлов (рис. 1) и др.;
- **SnapMirror** – ПО для поддержки катастрофостойчивости, обеспечивает низкий RTO (Recovery/recall Time Objective – максимально допустимое время восстановления работоспособности приложения), поддерживает IP- и FC-соединение (табл. 2);
- **SyncMirror** – ПО для создания реплик между контроллерами одной системы хранения;
- **SnapManager** – агент и ПО управления бэкапированием (локальные и DR-инфраструктуры) для виртуальных инфраструктур, интегрируется с

Табл. 2. Сравнительные характеристики РКВ-компонент SnapVault и SnapMirror.

SnapVault	SnapMirror
Предназначение - всегда только read-only	Предназначение - может быть read-write
RPO - 1 час и более	RPO - может выполняться каждую минуту
Long-term retention - сохранение множественных версий файла	True mirroring technology - deletions reflected in mirror
Множество точек онлайн-восстановления (CIFS/NFS доступны)	Низкий RTO, поддержка failover/failback
Только один способ передачи - IP-соединение	Двухнаправленная передача, поддержка IP- и FC-соединения

SnapMirror®, SnapVault®, Protection Manager. С помощью SnapManager администратор виртуальных машин через ряд специализированных продуктов – SnapManager for Exchange, SnapManager for Oracle, SnapManager for SAP, SnapManager for SQL и SnapManager for SharePoint может самостоятельно управлять всеми функциями, связанными с поддержанием доступности приложений;

- **Protection Manager** – ПО управления приложениями, интегрировано с SnapMirror®, SnapManager®, SnapVault®, Open Systems SnapVault. Автоматизирует управление на основе политик: автоматически обнаруживает новые данные, автоматически распределяет (provisions) вторичное хранение, автоматически выполняет политики по защите данных. Упрощает управление и мониторинг процедурами РКВ на базе единой консоли.

В качестве ключевых преимуществ, которые достигаются при внедрении РКВ-технологий NetApp на основе моментальных снимков, можно назвать следующие:

- ускорение процедур РКВ:
  - уменьшение окна резервного копирования до 98%;
  - полное восстановление в течение минут;
  - ускоренная защита приложений и виртуальных машин;
- простота и гибкость процедур РКВ:
  - возможность использования единого интерфейса для всех операций;
  - поддержка множественных уровней на дисках и лентах;
  - возможность использования повторяющихся процессов на множестве приложений;
- снижение стоимости и увеличение эффективности:
  - уменьшение до 90% используемой емкости хранения;
  - уменьшение утилизации сети;
  - легкость добавления к другим сервисам по защите данных;
  - масштабируемость на множестве приложений, платформ и локаций.

### Ускорение процедур РКВ

В качестве базовой технологии в процедурах РКВ NetApp используются моментальные снимки – Snapshot-копии, кото-

- создают моментальную копию тома на конкретный момент времени;
- обеспечивают запись только измененных блоков данных с момента создания предыдущего моментального снимка, требуя минимальных ресурсов для хранения;
- имеют близкое к нулю влияние на производительность хоста;
- позволяют выполнять бэкап так часто, как это необходимо;
- позволяют выполнять самые жесткие требования по RTO (Recovery Time Objectives), используя только одну команду при восстановлении.

После создания моментальных снимков они могут быть реплицированы на другое СХД или удаленную локацию/сайт, включая облако. Поддерживаются различные платформы и модели, например, FAS -> V-Series, FAS6080 -> FAS 2040. За счет того, что производится репликация только измененных данных, возможна запись/восстановление данных за месяцы и даже годы.

При репликации моментальных снимков не требуются какие-либо серверы резервного копирования, а за счет того, что запись данных осуществляется в формате оригинальных данных, допускается анализ реплицированных данных и восстановление, управляемое администратором. С помощью Volume SnapMirror данные реплицируются автоматически в дублированном виде.

Технологии дедупликации NetApp работают на блоковом уровне и изначально интегрированы с Data ONTAP и WAFL файловыми структурами, за счет чего удается существенно повысить эффективность механизмов дедупликации. При этом, например, не требуются сложные алгоритмы хэширования и таблицы поиска. Дедупликация применима как к основным данным, так и к архивным данным, а также для резервных копий и дополняет другие технологии NON-DUP в массивах NetApp, в частности, SnapVault, SnapShot, FlexClone, Thin Provisioning, Space Reclamation и т.д.

Особенностью РКВ-процедур NetApp является то, что все технологии, используемые для продуктивных данных, в полной мере применяются и для данных РКВ-процедур, включая HA, DR, бэкапирование и архивирование данных (рис. 2), что позволяет увеличить эффективность используемой емкости до 90% и более.

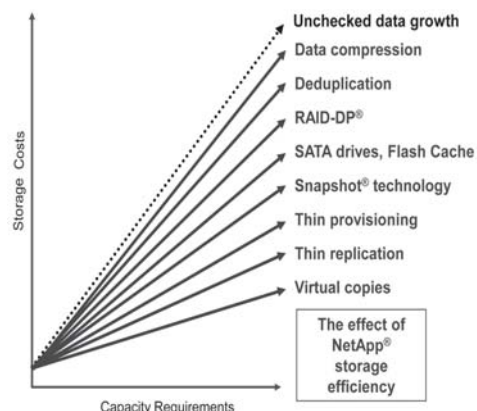
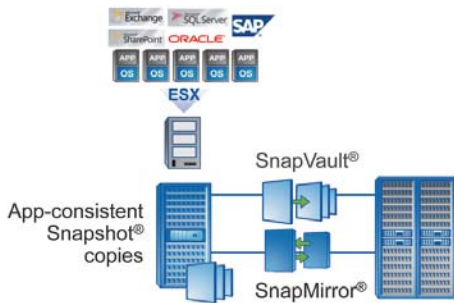


Рис. 2. Особенностью моментальных снимков NetApp является то, что все технологии, используемые для продуктивных данных, в полной мере применяются для данных РКВ-процедур.

Технология SnapShot прозрачно интегрируется со всеми ведущими гипервизорами для стандартных серверов: VMware ESX, Microsoft Hyper-V, Citrix и др., а также ключевым прикладным ПО – Oracle, SAP, Microsoft Exchange/SharePoint/SQL Server и др., предотвращая потерю: данных записанных в памяти, обрабатываемых транзакций, VM или файлов VM (рис. 3), а также поддерживая специфические прикладные опции восстановления, например, восстановление отдельного почтового ящика.



**Рис. 3.** РКВ-технологии NetApp прозрачно интегрируются со всеми ведущими гипервизорами для стандартных серверов: VMware ESX, Microsoft Hyper-V, Citrix и др., а также ключевым прикладным ПО — Oracle, SAP, Microsoft Exchange/SharePoint/SQL Server и др.

### Гибкость управления

Все множество способов резервного копирования администрируются при помощи единого инструмента — NetApp OnCommand, — который может быть использован с любыми системами и ПО от NetApp.

NetApp OnCommand позволяет создавать многоуровневые схемы хранения резервных копий, при этом реализуется это на основе уже существующих шаблонов или вновь создаваемых сегментов. Во время создания сложных схем визуально можно проследить схему миграции резервных копий и при необходимости внести изменения. Одной из особенностей использования данного ПО является хранение всех заданий по созданию резервных копий, синхронной и асинхронной репликации, что позволяет отказаться от использования выделенного сервера резервного копирования и получить возможность управления схемами РКВ с любого места по IP-сетям.

### Заключение

В ноябре 2011 г. компания NetApp анонсировала новые системы семейства FAS — FAS2240. Также компания объявила о том, что системы FAS2020 снимаются с произ-

**Табл. 3.** Розничные цены на преконфигурные бандлы FAS2020.

Bundle *)	Цена USD
FAS2020, 12X1TB, base sw, 36M SSP NBD-Part-Shippment	7450
FAS2020, 12X2TB, base sw, 36M SSP NBD-Part-Shippment	10950
FAS2020A, 12X1TB, Windows Bundle sw, 36M SSP NBD-Part-Shippment	12950
FAS2020A, 12X600GB, Complete Bundle sw, 36M SSP NBD-Part-Shippment	13950

\*) В бандлы включена фиксированная конфигурация на 1/2 контроллера и 12 дисков разной емкости, набор лицензий на функциональность, гарантия на 3 года с доставкой замены в режиме Next Business Day, а также трехлетняя подписка на обновления ПО (SSP — Software Subscription Program) и сопровождение систем.

В состав лицензий входят:

- все доступные протоколы доступа: CIFS, NFS, iSCSI, FCP;
- Base pack (Snapshots — до 255 снапшотов на том; Thin provisioning не зависящий от хост-OS; дедупликация; SyncMirror — синхронная репликация как внутри, так и между системами по IP);
- Windows bundle это Base pack плюс: SnapRestore, SnapVault, SnapMirror, SnapManager, SnapDrive, NetApp DSM.
- Complete bundle это все перечисленное выше, плюс еще несколько лицензий: FlexClone, Multistore — создание независимых "виртуальных систем хранения" внутри одной физической, SnapLock — средство неизменяемого хранения данных (WORM — Write-once, Read-many).

водства, а на системы данной модели, находящиеся на складах дистрибьюторов, до конца года ввела дополнительные скидки с новыми рекомендованными ценами для конечного пользователя на 4 конфигурации этих систем (табл. 3).

Несмотря на невысокую производительность данных систем (ввиду их относительного большого возраста), они полностью соответствуют концепции компании NetApp и являются полноценными Unified Storage. Такое обстоятельство подразумевает, что все описанные выше функции и опции присутствуют и на этих системах, а в свете новых скидок такая система становится идеальной back-end системой для долговременного хранения резервных копий. При этом система позволяет не только хранить резервные копии, но и при необходимости подключить к этой системе серверы напрямую и обслуживать запросы пользователей, хотя и с потерей производительности.

Для примера, схема с системой FAS2240 (на front-end) для хранения оперативных данных и системой FAS2020 (на back-end) для долговременного хранения резервных копий позволит не только организовать полноценную единую систему оперативного хранения и РКВ, но и основательно сэкономить.

Сергей Солонин,  
компания Tetroniks

## Intel продолжает погружать технологии ИБ на уровень ядра

Октябрь 2011 г. — В 2009 г. компания Intel ввела поддержку опций AES-NI в своих процессорах, а в октябре 2011 г. объявила о доступности еще ряда ИБ-технологий в своих процессорах: McAfee Deep Defender и McAfee ePO™ Deep Command. Два новых решения были представлены на конференции McAfee FOCUS 11.

Первое решение McAfee Deep Defender предназначено для защиты рабочих станций и использует технологию McAfee DeepSAFE для обнаружения почти любого вредоносного ПО на уровне ядра, что позволяет защитить все данные между процессором и операционной системой, а также находящиеся в оперативной памяти системное программное обеспечение. McAfee DeepSAFE обеспечивает беспрецедентный уровень безопасности благодаря тому, что он может работать даже без операционной системы (ОС).

Выпуск такого решения, которое задействует аппаратное обеспечение, стал возможен благодаря совместной работе McAfee и Intel. Новое решение способно блокировать руткиты и атаки формата АРТ. С повышением числа угроз, возникновением целенаправленных атак, проводимых до получения результата, необходим новый подход к защите персональных данных. Это стало причиной объединения McAfee и Intel, чья совместная работа направлена на изменение

принципов защиты информации — путем объединения программного и аппаратного обеспечения в единый комплекс, способный более эффективно противостоять атакам и обеспечивать защиту каждого участка вычислительного континуума.

Также McAfee Deep Defender предлагает:

- мониторинг ОЗУ и ЦП в реальном времени. Технология McAfee DeepSAFE позволяет McAfee Deep Defender выявлять труднообнаруживаемый вредоносный код, предоставляет администраторам информацию об использовании памяти и запущенных процессах и позволяет выполнять блокировку и ограничение;
- обнаружение неизвестных вирусов. McAfee Deep Defender не нужно знать руткит для того, чтобы его найти;
- защита от известных и неизвестных угроз. McAfee Deep Defender будет сообщать, блокировать, помещать в карантин и удалять известные и неизвестные и невидимые вирусы при их попытке попасть в ОЗУ. При обнаружении подозрительных объектов или неизвестных угроз McAfee Deep Defender отправит копию кода в сеть McAfee Global Threat Intelligence и предпримет заданные ему действия: блокирование, лечение или помещение карантина.

Централизованное управление McAfee Deep Defender осуществляется с помощью универсальной консоли McAfee ePolicy Orchestrator, которая используется и в других продуктах McAfee для защиты. Таким образом, пользователи получают возможность удобного централизованного управления и протоколирования.

“Совместная работа McAfee и Intel позволила создать абсолютно новое решение, способное обеспечить безопасность будущих поколений вычислительных систем, — заявил президент McAfee Тодд Гебхарт (Todd Gebhart). — Злоумышленники придумывают новые способы, как сделать вредоносный код незаметным и сложным для обнаружения, но они не могут теперь сделать его невидимым, если взаимодействуют с аппаратным обеспечением, памятью или операционной системой. Теперь мы можем отслеживать такое взаимодействие, полностью блокировать новые угрозы и обеспечивать наших клиентов беспрецедентным уровнем защиты. McAfee Deep Defender олицетворяет полностью новый подход к обеспечению безопасности и показывает то, какие продукты могут стать результатом объединения McAfee и Intel”.

Второе решение McAfee ePO™ Deep Command делает возможным управление безопасностью оконечных устройств/персональных компьютеров даже без использования операционной системы, которые могут быть отключены от питания или даже повреждены. McAfee ePO™ Deep Command использует аппаратные функции, встроенные в ноутбуки и настольные ПК с процессорами Intel® Core™ i5 vPro™ и Intel® Core™ i7 vPro™. Используя технологию Intel Active Management Technology (AMT), McAfee ePO Deep Command помогает обеспечить удаленный доступ к ПК вне зависимости от