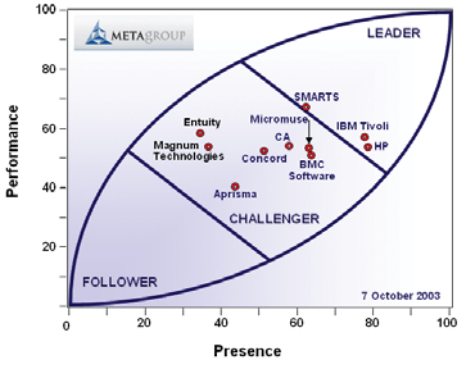
EMC SMARTS Storage Insight:

интеллектуализация диагностики SAN

В 2005 г. корпорация EMC приобрела компанию SMARTS Inc. и в апреле с.г. на основе технологии SMARTS анонсировала продукт EMC SMARTS® Storage Insight for Availability (SIA) – новый класс ПО – для автоматизированной "интеллектуальной" диагностики неисправностей инфраструктуры SAN. До конца 2006 г. EMC планирует сделать еще несколько важных объявлений для SIA в части расширения поддерживаемых им платформ и глобального интегрирования технологии SMARTS в концепцию ILM.

Введение

Несколько слов о предыстории семейства EMC SMARTS. Продукция компании SMARTS была представлена на рынке достаточно давно и относилась и относится в настоящее время к сектору продуктов для управления событиями (главным образом, в IP-сетях). Основные игроки, несмотря на уже устаревший последний публичный обзор (рис. 1), не изменились. При этом SMARTS была куплена EMC, Aprisma и Concord – CA, а Micromuse – IBM. По оценкам IDC на 2004 г., этот сектор рынка измерялся в $1,8 млрд. ПО этого класса относится к т.н. "fault management-системам", ориентированным в большинстве своем на протоколы IP, MPLS, ATM/FR и др. Такая "заточенность" данного ПО определялась значительно большей развитостью IP-сетей, чем SAN, и, соответственно, повышенной сложностью их диагностики.



Ист.: MetaSpectrum Event Management

Рис. 1. Распределение рынка управления и диагностики IP-сетей между вендорами по состоянию на октябрь 2003 г.

Но на настоящий момент ситуация "назрела" и в области управления и хранения данных. Как отмечают западные аналитики, за последние 3 года в "типовом" центре данных управление SAN намного усложнилось. В дополнение к гетерогенной среде хостов и систем хранения возрастает число различных типов HBA и FC-коммутаторов, используются все более сложные многопутевые схемы доступа к данным. При этом требования к доступности данных постоянно только возрастают. В этих условиях "традиционные" системы мониторинга могут "вываливать на голову" системного администратора гору сообщений – на поиск первопричины, ее породившей, могут уходить часы и даже дни.

В этой ситуации старый "ручной" подход с написанными индивидуальными правилами для каждой SAN-компоненты не пригоден – он является неполным и немасштабируемым. Альтернатива ему – подход, основанный на моделях (связи, взаимоотношения компонент SAN и их влияние на SLA) для анализа первопричины сбоя/отказа и позволяющий максимально автоматизировать этот процесс. Именно такой подход и используется в "fault management-системах".

Первая версия SIA из систем хранения поддерживает только Symmetrix и CLARiiON, но к осени с.г. EMC планирует обеспечить более полную гетерогенную поддержку.

Что "портит жизнь" системному администратору?

Рассмотрим типовые ситуации, с которыми приходится сталкиваться системному администратору, занимающемуся поддержкой IT-инфраструктуры и SAN, в частности. Первоочередная его задача – поддержка требуемого уровня доступности системы в целом, или максимально быстрое устранение возникающих и потенциальных ошибок/сбоев/отказов на поддерживаемых уровнях системы с минимальным влиянием на наиболее критичные бизнес-приложения. Особенности функционирования современных IT-систем таковы, что сбой/отказ в отдельной компоненте может вызывать целую цепочку "падений", связан-

ных с ним компонент/подсистем по принципу "домино". В результате, на консоли администратора – "море" красных предупреждений, выявить первопричину среди которых бывает крайне сложно. При этом часто "разбор" ситуации требует совместных усилий целой группы специалистов – администратора по системам хранения, сетевого администратора, менеджеров приложений, администратора СУБД. Это усложняется и тем, что даже схожие ситуации требуют индивидуального анализа, т.е. трудно стандартизуются и "разбираются" на основе правил. К этому можно добавить и то, что анализ ситуаций в большинстве компаний необходимо проводить с учетом приоритизации их влияния на бизнес, что при "традиционном" подходе также оказывается непросто. Исследования показывают, что от 80% до 90% времени простоя тратится только на анализ сбоя.

Общий результат при развитии IT-инфраструктуры – снижение доступности, возрастание IT-бюджета, рост "нервных заболеваний" у персонала.

Системы управления сбоями

Выходом из ситуации, описанной выше, является использование "fault management-систем", или систем управления сбоями. Существует 2 подхода к их построению: *правило-* и *моделеориентированный*.

Первый подход. Требуется определять правила сообщений того, как в случае сбоя каждый элемент инфраструктуры и его связи взаимодействуют друг с другом. При наличии большой сети большинство удаленных элементов правилами уже становится сложно охватить, к тому же любые изменения, сделанные к IT-топологии, будут требовать реорганизации правил, созданных ранее.

Второй подход. Автоматически строится модель топологии IT-инфраструктуры и затем также автоматически (на базе специализированного ПО) устанавливаются отношения между элементами. Для этого класса систем также появляется возможность объединения различных доменов, например, IP-сети, прикладной среды и инфраструктуры хранения в рамках единой архитектуры, и, соответственно, возможность анализа сбоев в рамках этой федерации. Это, в свою очередь, позволяет быстро устанавливать влияние сбоев на бизнес-процессы, что является существенным шагом вперед в сравнении с традиционным правилоориентированным подходом.

Еще одно преимущество второго подхода – возможность поэтапного расширения функциональности системы по мере развития IT-топологии и появления новых моделей компонент.

До недавнего прошлого "fault management-системы" использовались только для диагностики IP-сетей. С анонсированием EMC Smarts Storage Insight for Availability область их приложения

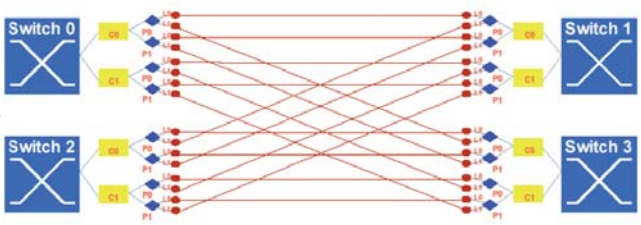


Рис. 2. Пример топологии SAN, состоящей из 4-х коммутаторов: по 2 карты в каждом (по 2 физических порта на каждую и с 2-мя логическими портами на физический порт).

впервые распространилась на SAN и их комбинацию (и с другими доменами).

Чтобы лучше понять концептуальные подходы, преимущества и проблемы, связанные с "fault management-системами", рассмотрим простой пример.

На рис. 2 представлена небольшая SAN с четырьмя коммутаторами (S0, S1, S2, S3), которые объединены в сеть для надежности. Каждый коммутатор состоит из 2-х карт, каждая из которых имеет 2 физических порта, каждый из которых, в свою очередь, поддерживает 2 логических порта.

В случае сбоя/отказа одной карты (C0) коммутатора (S1) генерируется 9 предупреждений на консоль администратора (рис. 3):

- 4 – от логических портов на отказавшей карте;
- 4 – от связанных логических портов на других коммутаторах;
- 1 – от коммутатора, на котором отказала карта (не для всех вендоров, при наличии поддержки).

В свою очередь, это может вызвать целую волну сообщений 2-го уровня – от подсоединенных к портам систем и приложений.

При правилоориентированном подходе – возможны 3 сценария анализа первопричины. Самый простой (1) – "снизу–вверх" ("bottom-up"), который подходит только для анализа простых статических сетей. В этом случае анализируются все события – тревоги, предупреждения, SNMP-traps, пороговые нарушения и т.д., которые могут произойти в системе, и затем пишутся правила (зависящие от конкретной сети), обрабатывающие каждое из этих событий, когда они происходят. Более эффективный (2) подход, основанный на правилах, обрабатывающих комбинацию признаков. Например, правило, идентифицирующее сбой карты 0 в коммутаторе 1 (см. рис. 3), выглядит следующим образом ("если все логические порты на S1C0 выдают *"down"* и все подсоединенные порты также выдают *"down"*, то S1C0 является первопричиной сбоя"):

IF

S1C0P0L0 *down* ***AND***

S1C0P0L1 *down* ***AND***

S1C0P1L0 *down* ***AND***

S1C0P1L1 *down* ***AND***

S0C0P0L0 *down* ***AND***

S0C0P1L0 *down* ***AND***

S2C0P0L1 *down* ***AND***

S2C0P1L1 *down* ***AND***

THEN CONLUDE S1C0 *failure*

Поскольку даже в такой небольшой сети (см. рис. 2) существует не менее 60 возможных сбоев/отказов (каждого выключателя, карты, физического и логического порта), то, соответственно, потребуется и написание не менее 60 правил, подобно представленному выше. Но это только начало. В случае одновременного возникновения более одного сбоя потребуются дополнительные правила. Что случается, если сетевая проблема вызывает задержку или потерю данных? Как отличить проблемы, которые могут немедленно привести к снижению доступности от тех, которые автоматически дублируются системой и могут "подождать"? В подобных ситуациях число правил экспоненциально возрастает с ростом сети, а при наличии уже сотен элементов в сети число правил может легко достигать нескольких миллионов. При изменениях в сетевой топологии правила необходимо изменять и т.д.

В некоторых "fault management-системах" используется т.н. "downstream event suppression-технология", которая позволяет значительно сократить число предупреждающих сообщений при анализе иерархических IP-сетей. Она работает следующим образом: poller периодически опрашивает (пуллирует) IP-устройства, чтобы проверить их работоспособность. Когда устройство не в состоянии ответить, делается следующее:

- игнорируются отказы от устройств "вниз по течению" (дальше от пуллируемого от первого устройства);
- определяется устройство, наиболее близкое к пуллируемому, которое выбирается в качестве первопричины сбоя.

Однако эта техника требует, чтобы сеть представляла собой простую иерархическую структуру, что в современных условиях практически недостижимо.

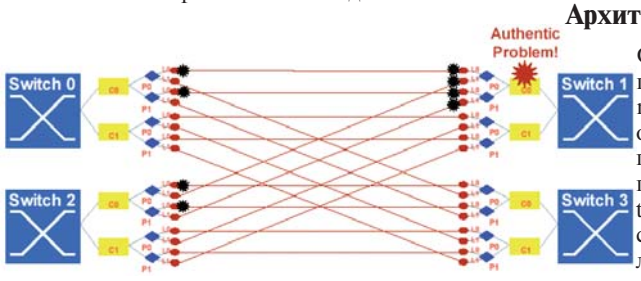


Рис. 3. Сбой/отказ одной (C0) карты коммутатора (S1) вызывает 9 предупреждений на консоль администратора.

Архитектура SMARTS

Семейство продуктов SMARTS представляет собой "fault management-систему", построенную на основе моделеориентированного подхода, в основе которого лежит патентованная Codebook Correlation Technology (CCT). Все семейство продуктов SMARTS поставляется с библиотеками моделей поведения объектов (*InCharge* Common Information Model™), ориентированными на соответст-

вующие инфраструктуры сетей: IP, Multi Protocol Label Switching (MPLS), сетевые протоколы, SAN.

Технология CCT – математически обоснованный подход нового поколения средств автоматизации корреляций событий в системах, требующих гарантированного сервисного обслуживания. CCT имеет следующие уникальные особенности:

- автоматический анализ любого типа проблемы в любом типе физического или логического объекта для любой сложности инфраструктуры;
- возможность встраивания интеллектуального анализа в имеющиеся решения;
- автоматическая адаптация интеллектуального анализа при изменении топологии сети;
- высокое быстродействие.

Концепция CCT проста: каждая проблема в сетевой системе имеет уникальную сигнатуру (подпись) или признаки, которые ее вызывают. Эта сигнатура – ключ к идентификации проблемы.

Сигнатура обычно содержит много признаков (симптомов): в дефектном компоненте, где проблема происходит, и в связанных компонентах, которые затрагивает первоначальная проблема. Поскольку признаки различных проблем пересекаются, это приводит к уникальной комбинации признаков, которые отличают одну проблему от другой.

CCT диагностирует проблемы в режиме реального времени. Проблема, чья сигнатура наиболее близко соответствует множеству поступающих данных, идентифицируется как первопричина. На рис. 4 представлена вся совокупность возможных проблем для сети, представленной на рис. 2, каждая из которых идентифицируется соответствующей сигнатурой, или комбинацией уникальных признаков. Принцип диагноза в CCT подобен медицинскому, при котором врач по соответствующей комбинации симптомов заболевания, устанавливает диагноз пациенту.

Корреляция первопричины производится из простого сравнения признаков с

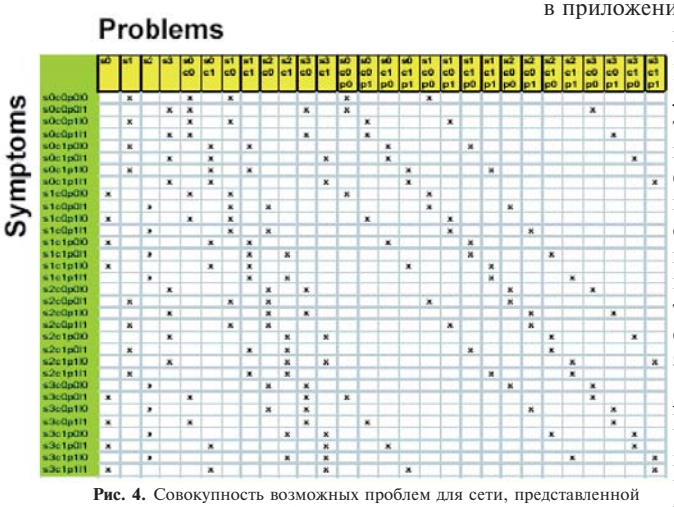


Рис. 4. Совокупность возможных проблем для сети, представленной на рис. 2, идентифируемых соответствующей сигнатурой или совокупностью уникальных симптомов.

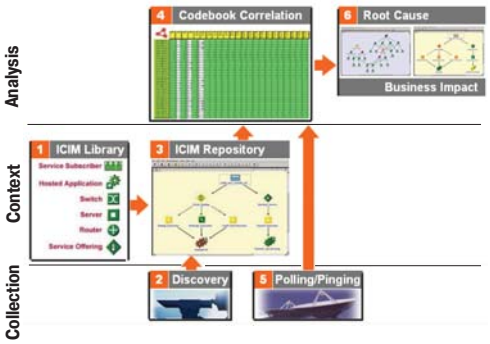


Рис. 5. Общая схема функционирования SMARTS.

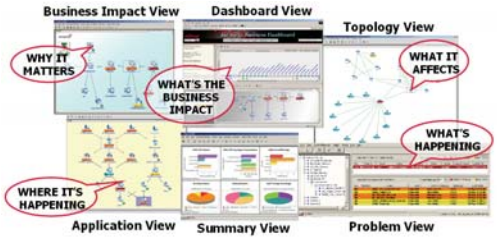


Рис. 6. SMARTS обеспечивает и полноту и глубину влияния диагностируемой проблемы.

сигнатурами, что происходит достаточно быстро. При этом устанавливается самое близкое совпадение – и не обязательно точное. Сами сигнатуры к каждой проблеме генерируются в CCT автоматически на основе т.н. моделей поведения (Behavior Model) компонент и не требуют вмешательства IT-персонала.

Сами объектноориентированные модели поведения описываются классами объектов и ассоциируемыми с ними проблемами. Ключевым моментом описания классов объектов и их поведения является их независимость от топологии инфраструктуры.

Модели поведения описываются двумя типами признаков. Признаки, непосредственно связанные с дефектным объектом, упоминаются как *местные* признаки. Например, "недоступность сервера" является местным признаком, связанным с сервером, который "упал". Признаки, которые появляются в объектах, связанных с дефектным объектом, упоминаются как *размноженные* (вторичные) признаки. Например, "недоступность приложения" является размноженным признаком, который появляется в приложениях, выполнявшихся на сервере, который "упал".

Пример моделей, представленный ниже, дает описание трех классов объектов SAN, показанных на рис. 2: карт, физических и логических портов. Поскольку пример ориентирован на управление доступностью, набор первопричин для каждого типа объекта содержит единственную проблему, названную "down".

Card **Behavior Model**
Problem *Down* **Causes** *PortDown*
Propagated symptom *PortDown* **To** *Physical Ports in the Card Down*

Physical Port **Behavior Model**
Problem *Down* **Causes** *PortDown*
Propagated symptom *PortDown* **To** *Logical Ports Layered over the Port are Down*

Logical Port **Behavior Model**
Problem *Down* **Causes** *OperationallyDown, ConnectedPortDown*
Local symptom *OperationallyDown*
Propagated symptom *ConnectedPortDown* **To** *Connected Logical Ports Down*

Общая схема функционирования "fault management-системы" на основе технологии SMARTS представлена на рис. 5,6.

Реализация SMARTS SIA

Продукт Smarts Storage Insight for Availability стал доступен с конца апреля с.г. и представляет по сути набор моделей поведения объектов в определении SMARTS для SAN.

Общая структурная схема использования SIA в составе существующей IT-инфраструктуры дана на рис. 7.

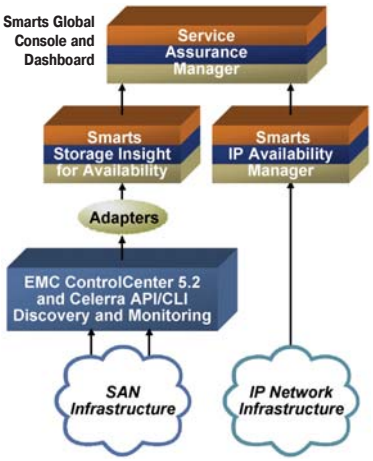


Рис. 7. Структурная схема использования SIA в существующей IT-инфраструктуре.

Открытие и мониторинг источников в среде SAN осуществляется на базе EMC ControlCenter 5.2 и Celerra API/CLI, в среде IP-сети – SNMP traps.

Анализ событий в среде IP-сети делается на базе SMARTS IP Availability Manager. Корреляция событий между storage и сетевым доменами осуществляется через Celerra Gateway с обеспечением единой точки интеграции всех инструментов анализа SMARTS.

Объекты (которые анализируются), типы первопричин сбоев (которые для них

Табл. 1.

	Entity	Root Cause
Symmetrix	Disk	Down
	Front-end port	Down, unstable
	Front-end director	Down
	Unit	Down
	Service processor	Down, disabled
CLARiiON	Disk	Down
	Unit	Down
	Storage processor	Down, disabled
FC switches	Port, cable, unit	Down
Host	HBA port, cable, card	Down, unstable

Impacted Elements	
Host devices	Celerra Data Movers
File systems	Celerra Client File Shares
Logical volumes	PowerPath paths

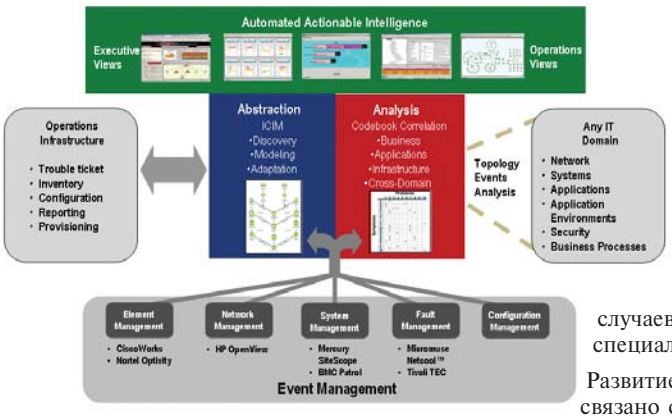


Рис. 7. Интеграция инструментов SMARTS в существующую IT-инфраструктуру.

могут устанавливаться), а также связываемые с ними элементы инфраструктуры, представлены в табл. 1. SIA, в частности, и весь пакет продуктов SMARTS легко интегрируются с ПО класса Event Management – CiscoWorks, Nortel Optivity, HP OpenView, Mercury SiteScope, BMC Patrol, Micromuse Netcool, Tivoli TEC и др. (рис. 7). Также обеспечивается простая корреляция между различными доменами инфраструктуры (см. рис. 7).

Применение и дальнейшее развитие семейства SMARTS

Как показало внедрение в одном из самых крупных банков – Citigroup (*США, Нью-Йорк, имеет более 3000 отделений в США и Канаде, а также более 1500 подразделений в 100 странах мира – прим. ред.*), сокращение числа выдаваемых событий составило от 20 до 100 раз, и в большинстве случаев администратор сразу получал информацию о первоисточнике проблемы, что дало возможность значительно более эффективно использовать IT-персонал. Второй фактор экономии – существенное сокращение затрат на поддержание установленного ПО и инфраструктуры вследствие резкого уменьшения числа случаев, требующих обращения к специалистам вне штата банка.

Развитие SIA, как уже отмечалось, связано с его расширением в область гетерогенной поддержки систем хранения, которое планируется на осень с.г. В целом семейство SMARTS будет расширяться в сторону анализа бизнес-приложений и охвата всей ILM-инфраструктуры. Объявление в конце апреля с.г. EMC Smarts® Application Discovery Manager (ADM) является первым шагом на этом пути.

ADM позволяет в реальном времени создавать интерактивную модель законченной инфраструктуры бизнес-приложений, обеспечивая пользователей необходимым пониманием поведения приложений при возникновении различных событий/ситуаций/проблем с учетом всех их взаимозависимостей с компонентами IT-инфраструктуры.

Основные особенности ADM:

- поддержка до 500 приложений;
- автоматическая модификация модели поведения при изменениях конфигурации/структуры приложений, а также их модернизации;
- информация о конфигурации сервера включает данные о: BIOS, CPU, DNS, файловых системах, установленных приложениях, IP-адресах, память, сетевые устройства и операционные системы;
- информация о конфигурации ПО включает данные о: компонентах приложений, конфигурационных файлах, инсталлированных приложениях, установленных каталогах, а также информацию о вендорах и версиях;
- легко устанавливается, по архитектуре – безагентный, развертывается в течение 60 минут.

Заключение

Появление продукта Smarts Storage Insight for Availability является знаковым событием перехода от "дриллинговых" систем логического, во многом "ручного", "поштучного" анализа событий SAN к более потоковым и более интеллектуальным моделеориентированным системам диагностики. В этих условиях даже такие гиганты ПО, как Microsoft, начинают предлагать своим клиентам для анализа и поддержки IT-инфраструктуры интегрированные платформы, например, своего базового продукта – Microsoft Operations Manager 2005 совместно со SMARTS, поставляемого по OEM-соглашению.

Глобальное расширение семейства SMARTS в область всей ILM-инфраструктуры будет еще более привлекательным для потребителей событием.

И, безусловно, рынок не останется в стороне и уже к концу 2006 г. последует еще ряд интересных анонсов.

Storage Expo Russia 2006

4–6 сентября 2006 г. в Экспоцентре на Красной Пресне (Москва, Краснопресненская наб., 14, павильон 2) пройдет Storage Expo Russia 2006 *(www.storage-expo.ru)* – единственная в России выставка-конференция, полностью посвященная решениям и технологиям в области хранения данных.

На 3-дневной конференции Storage Expo Russia 2006 будут обсуждаться: тенденции и направления развития рынка систем хранения; виртуализация в системах хранения; технологии гарантированного долговременного хранения данных и вопросы регулирования; обеспечение непрерывности бизнес-процессов и технологии защиты от катастроф; отказоустойчивость инфраструктуры систем хранения; ILM – практические шаги; альтернативные технологии доступа к данным; технологии резервного копирования; вопросы архивирования корпоративных данных; взаимосвязь и взаимовлияние бизнес- и storage-решений.

Организатором выставки являются Выставочное Объединение "Рестэк" совместно с британской компанией "Reed Exhibitions".

Одновременно со Storage Expo пройдут выставки Infosecurity Russia 2006 *(www.infosecuritymoscow.com)* и Documation Russia 2006. На соседней площадке 4–5 сентября состоится еще одна выставка-конференция: Linux-World Russia 2006 *(www.linuxworldexpo.ru)*.

Новые системы EMC CLARiiON CX3 UltraScale

Май 2006 г. – Корпорация EMC анонсировала новое семейство дисковых систем – CLARiiON CX3 UltraScale. Внутренние контроллеры семейства CLARiiON UltraScale реализованы на компьютерах, поддерживающих шинную архитектуру на базе PCI Express и имеющих до 16 Гбайт оперативной памяти. Сами системы хранения имеют полную поддержку (включая диски, хост- и дисковые интерфейсы) протокола 4 Гбит/с FC. За счет этого, а также высокоскоростных контроллеров, производительность новых систем практически удваивается.

Также на новых системах быстрее работает и "старый" софт – так, репликация на основе EMC SnapView, EMC MirrorView, EMC SAN Copy (как сказано в пресс-релизе) выполняется на 30% быстрее.

Одновременно новые системы могут поддерживать комбинации 2-х типов дисков: высокоскоростных (2/4 Гбит/с FC) и высокоемких (2Gb/s Low-Cost Fibre Channel – LC/FC) с целью оптимизации различных ILM-стратегий.

Новые системы имеют дополнительную избыточность (n+1+1) для блоков питания/вентиляторов и надежность. Семейство CLARiiON UltraScale построено на EMC UltraPoint технологии (введена в августе 2005 г.), дающей расширенные возможности по диагностике всех компонент.

Новые системы могут конфигурироваться для DAS- и SAN-развертывания. Возможность их соединения по iSCSI и в коммутируемых публичных сетях на основе NEBS (Network Equipment Building System) будет доступна осенью с.г.

Новое семейство представлено тремя моделями: CX3-20 – масштабируемость от 365 Гбайт до 59 Тбайт, поддержка – до 128 высокодоступных хостов; CX3-40 – масштабируемость до 119 Тбайт, поддержка – до 128 высокодоступных хостов; CX3-80 – масштабируемость до 239 Тбайт, поддержка – до 256 высокодоступных хостов.