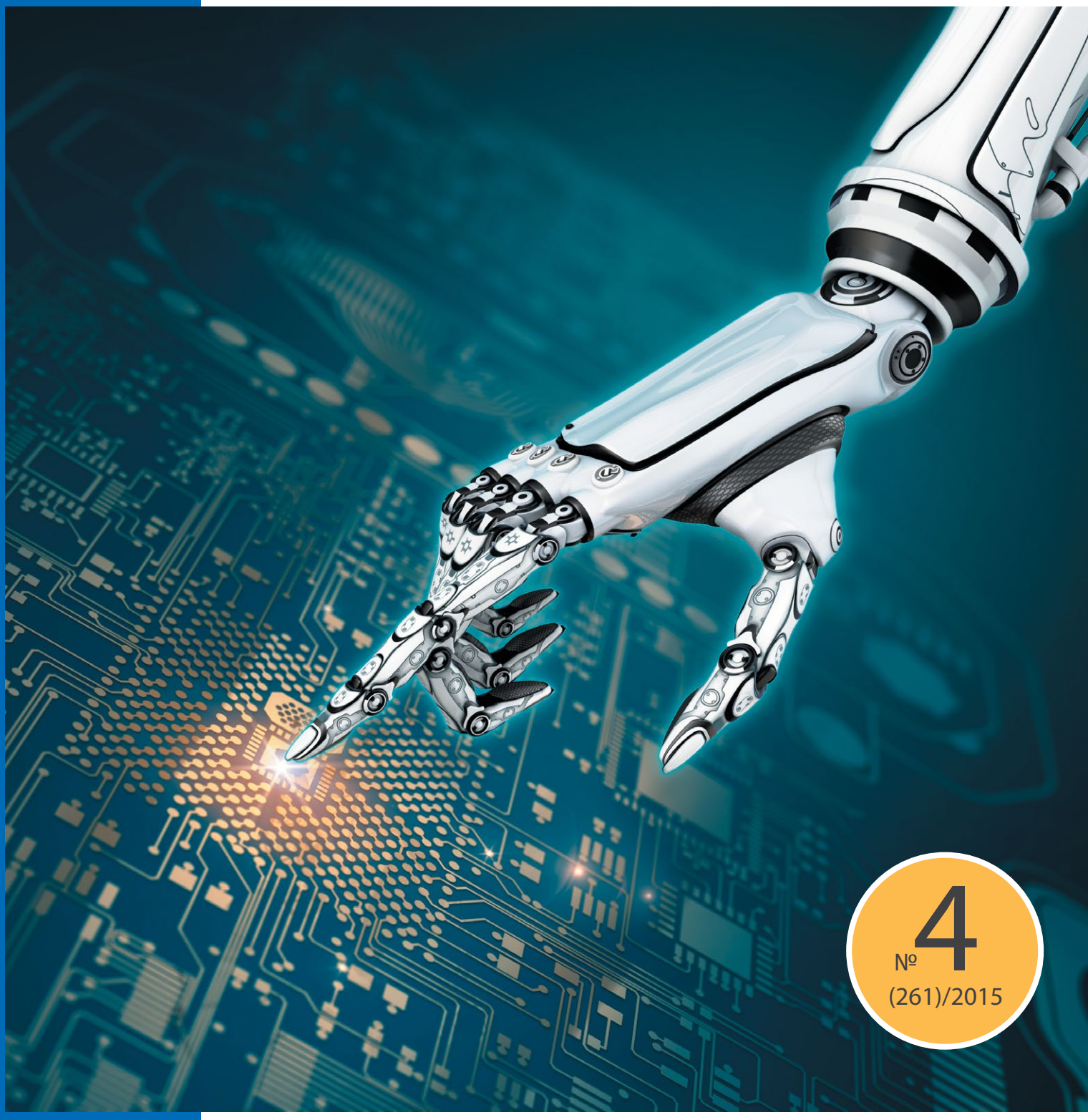
ИЗДАЕТСЯ КОМПАНИЕЙ «ИНФОСИСТЕМЫ ДЖЕТ»

Jet Info

WWW.JETINFO.RU

ТЕМА НОМЕРА

ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ



№ 4 (261)/2015

Jet Info

Издается с 1995 года

Редакция:
Дмитриев В.Ю.

Некрасова Н.А.

Шедова Е.Л.

Дискина А.Л.

Дизайн и верстка:
Саблина М.А.

Корректура:
Макеева Е.И.

Над номером работали:
Бородин Д.А., Демарин А.В.,
Коляскин А.И., Шапошников А.Д.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01

info@jet.msk.su

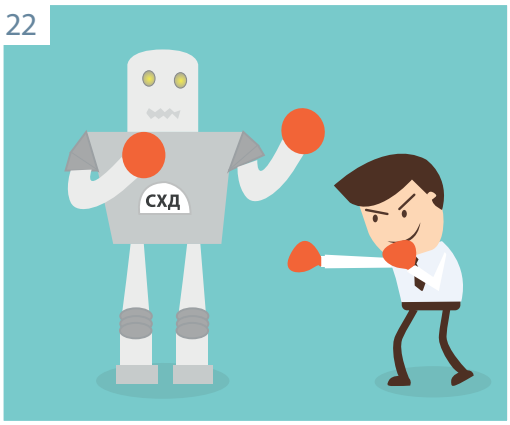
www.jetinfo.ru

Содержание

9

12

16



22

3 **От редакции**

5 **Новости**

8 **Наши проекты**

9 **Тема номера**
Как добиться единства противоположностей
АНДРЕЙ ШАПОШНИКОВ

12 **Тема номера**
Когда с SDN жить хорошо
АЛЕКСЕЙ КОЛЯСКИН

16 **Тема номера**
Диалектика виртуальных сетей: Cisco и VMware
ДМИТРИЙ БОРОДИН

22 **Тема номера**
Конкуренты железных СХД
АРТЕМ ДЕМАРИН

28 **Собеседник**
Василий Окулесский,
К. Т. Н., НАЧАЛЬНИК УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕПАРТАМЕНТА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ БАНКА МОСКВЫ

34 **В тему номера**

АНДРЕЙ ШАПОШНИКОВ,
заместитель директора
Центра проектирования
вычислительных комплексов
компании «Инфосистемы Джет»

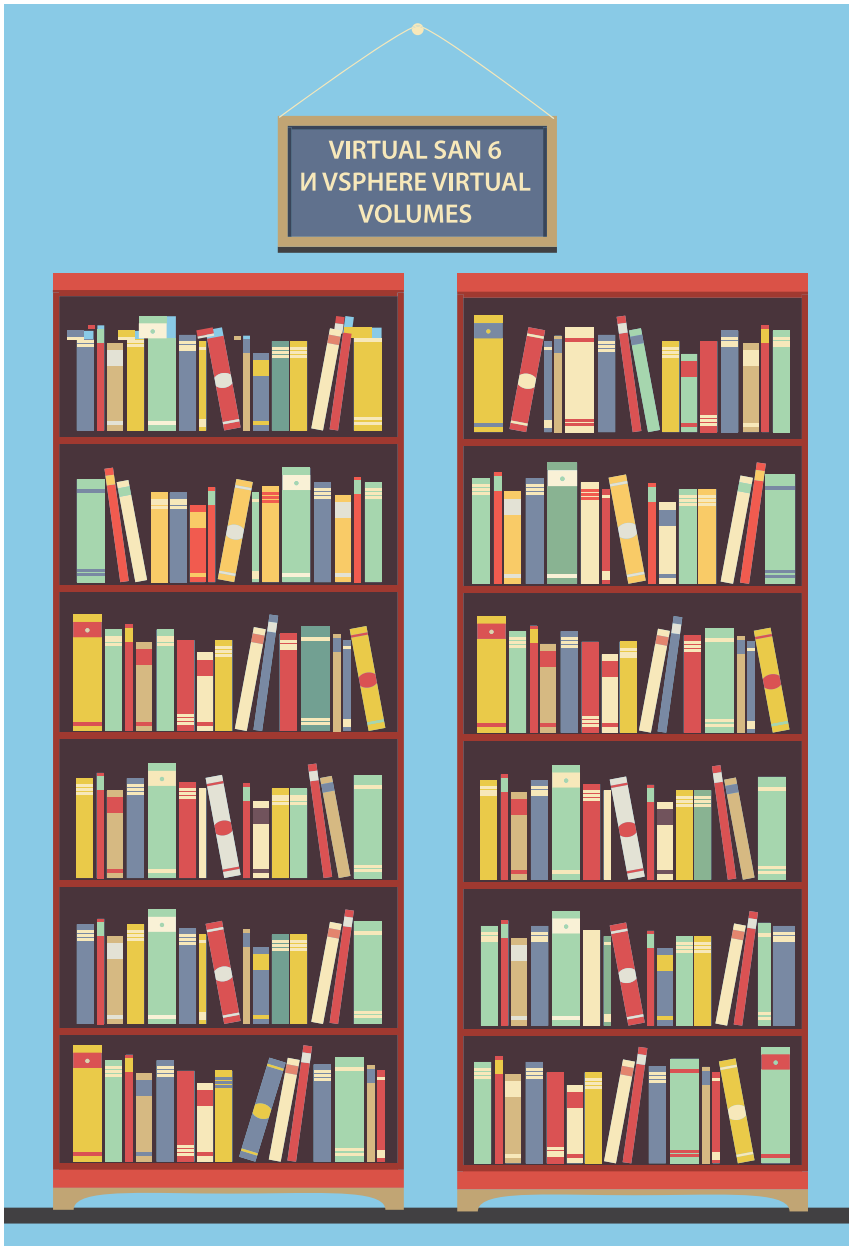
Совсем недавно мы выпустили номер, посвященный тематике программно-определяемых инфраструктур, – № 11, 2014. Но оказалось, что эта тема не исчерпана и в ней немало новых интересных поворотов. Например, с ней очень близко связана тема виртуализации. Фактически достаточно сложно провести грань между инфраструктурами виртуализованными и программно-определяемыми – что было вначале, в чем отличие между ними, как воспользоваться преимуществами таких решений? Попытаемся разобраться вместе!

VMWARE ПРЕДСТАВИЛА НОВУЮ ПЛАТФОРМУ ХРАНЕНИЯ

VMware выпустила новое поколение решений для хранения данных Virtual SAN 6 и vSphere Virtual Volumes.

Разработанное для повсеместного распространения программно-определяемых хранилищ, VMware Virtual SAN 6 обеспечит значительный рост производительности и масштабируемости решения для хранения данных с конвергенцией на уровне гипервизора. VMware vSphere Virtual Volumes предложит новые уровни интеграции хранения для виртуальных машин, обеспечивающие прямую поддержку системами хранения данных от сторонних производителей.

VMware Virtual SAN 6 гарантирует двухуровневую поддержку архитектуры all-flash, когда флеш-накопители используются как для кэширования, так и для постоянного хранения данных. Новая архитектура all-flash обеспечивает прирост скорости ввода/вывода более чем в 4 раза на один узел по сравнению с VMware Virtual SAN 5.5, обеспечивая прогнозируемые задержки в доли миллисекунды.



Кластер VMware Virtual SAN из 64 узлов гарантирует пропускную способность до 7 миллионов операций ввода/вывода в секунду (IOPS), что практически соответствует идеальному линейному масштабированию.

VMware Virtual SAN 6 обеспечивает интеллектуальное распределение объектов виртуальных машин между серверами для обеспечения повышенного уровня доступности приложений, даже в случае полного выхода одной стойки из строя.

VMware vSphere Virtual Volumes представляет собой набор библиотек API для хранения данных, которые обеспечивают более тесную интеграцию между самим хранилищем и VMware vSphere на уровне отдельных виртуальных машин. Такой подход позволяет дисковому массиву динамически выделять ресурсы и сервисы работы с данными для каждой виртуальной машины. Благодаря этому инфраструктура хранения становится более динамичной и экономически эффективной, также упрощается процесс управления. Массивы хранения с VMware vSphere Virtual Volumes будут управляться через единую систему управления. Это расширение видения VMware в сфере программно-определяемого хранения данных для работы приложений с автоматизацией гетерогенного хранилища на основе политик.

ВИРТУАЛИЗАЦИЯ СЕТЕВЫХ ФУНКЦИЙ ОТ VMWARE

Компания VMware представила VMware vCloud for NFV, интегрированную платформу для виртуализации сетевых функций (NFV), сочетающую надежную и проверенную временем платформу виртуализации и управления вычислительными и сетевыми ресурсами, ресурсами хранения и интегрированную поддержку OpenStack. Благодаря возможностям работы с более чем 40 различными виртуальными функциями сетей (VNF) от более чем 30 поставщиков VMware vCloud for NFV сегодня является единственной платформой, которая позволяет запускать виртуализированные сетевые функции от разных производителей в единой унифицированной облачной среде. С помощью vCloud for NFV операторы связи смогут внедрять решения NFV на проверенной платформе и быстрее выводить на рынок новые услуги, значительно снижая при этом расходы.

VMware vCloud NFV включает решение для виртуализации вычислительных ресурсов VMware vSphere, полнофункциональную систему виртуализации сетей VMware NSX, которая обеспечивает программное представление всей сети и систем безопасности на уровнях L2–L7. Кроме того, в состав решения входят программно-определяемая система хранения VMware Virtual SAN, которая помогает снизить капитальные и операционные затраты на хранение данных; расширенное решение для управления эксплуатацией облачной среды VMware vRealize Operations, позволяющее использовать специально разработанные модули расширения, оптимизированные для решения задач операторов связи. Совместимость платформы с OpenStack обеспечивается за счет дистрибутива VMware Integrated OpenStack.

КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ» – СЕРВИСНЫЙ ПАРТНЕР HUAWEI

Компания «Инфосистемы Джет» получила статус авторизованного сервисного партнера компании Huawei – Russia Certified Service Partner Program, Server & Storage (Four-Star). Он подтверждает высокий уровень компетенций специалистов компании, соответствие всем сертификационным требованиям и предоставляет право на инсталляцию и сервисное обслуживание дисковых массивов и серверов Huawei. Получение сервисного статуса дает нам право на предоставление услуг первой и второй линий поддержки решений Huawei.

В компании «Инфосистемы Джет» функционирует демонстрационный стенд, позволяющий изучать продукты Huawei и моделировать различные задачи заказчиков. Несколько специалистов интегратора прошли необходимое обучение и получили сертификаты HCNA (Huawei Certified Network Associate) и HCNP (Huawei Certified Network Professional).

HITACHI VSP G1000 – ЛИДЕР ПО ПРОИЗВОДИТЕЛЬНОСТИ СРЕДИ СХД КОРПОРАТИВНОГО КЛАССА

Платформа Hitachi Virtual Storage Platform G1000 в конфигурации полностью на основе флэш-памяти заняла первое место в группе лидеров по производительности среди систем хранения данных корпоративного класса. Результаты независимого теста SPC-1 показали, что решение Hitachi VSP G1000 с модулями Hitachi Accelerated Flash имеет пропускную способность более чем на 60% выше, а время отклика в условиях полной загрузки втрое меньше, чем даже у специализированных нишевых систем на базе DRAM.

Конфигурация Hitachi VSP G1000 полностью на основе флэш-памяти создана специально для работы в самых требовательных с точки зрения нагрузки автономных и конвергентных производственных средах. Она позволяет организациям обеспечить максимальную рентабельность инвестиций в использование технологии флэш-памяти и при этом повысить эффективность приложений, полностью задействовать возможности виртуализации серверов и упростить развертывание частных облачных инфраструктур высокой производительности.

БОЛЬШЕ, ЧЕМ ИТ

3D-ПРИНТЕР ВВЕРХ ТОРМАШКАМИ

Инженеры объединились с химиками и создали новую технологию трехмерной печати. Для этого они буквально перевернули с ног на голову обычный 3D-принтер и в конечном итоге добились увеличения скорости печати в 100 раз.

Есть несколько технологий трехмерной печати, суть которых заключается в послойном создании объекта нужной формы. Одна из них – лазерная стереолитография. Изделие создается из жидкого фотополимера – специального вещества, которое затвердевает под действием ультрафиолетового лазера. Лазерный луч обегает контур детали, засвеченные им участки становятся твердыми, а незасвеченные остаются жидкими. Создаваемое изделие погружается слой за слоем в ванну из жидкого полимера. Когда процесс закончился, готовую деталь достают из ванны, удаляют непрореагировавший полимер и проводят заключительную обработку. Технология применяется по всему миру. Но у нее есть недостаток – скорость, которая не превышает нескольких миллиметров в час.

Самая медленная стадия во всем процессе – это отвердевание полимера. Дело тут в кислороде воздуха. Молекулы этого газа растворяются в верхнем слое жидкого полимера и тормозят его отвердевание. Лазерное излучение создает активные молекулы, которые начинают связывать молекулы полимерного материала друг с другом так, что он становится твердым. Кислород же активно мешает этому процессу, в результате полимер твердеет намного дольше, чем мог бы.

Как не допустить кислород к активным молекулам полимера? Проводить печать не на поверхности ванны с жидким фотополимером, а на глубине. Например, сделать у ванны прозрачное дно и светить лазером не сверху, а снизу. Тогда можно было бы печатать деталь, постепенно вытаскивая ее из-под слоя жидкого полимера. Вариант хороший, за исключением одного – полимер начнет отвердевать прямо в месте его контакта с прозрачным дном, и создаваемая деталь просто приклеится к ванне. Вот тут-то и заключается все ноу-хау изобретения. Разработчиком удалось сделать так, чтобы изготовляемая деталь не «пригорала» к поверхности ванны. И помог им в этом, как ни странно, тот самый «плохой» кислород.

Дно ванны для жидкого полимера изготовили из специального тефлонового материала, через который почти свободно могут проникать молекулы кислорода, но в то же время он прозрачен для ультрафиолетового излучения лазера. Молекулы кислорода проникают сквозь такую мембрану и растворяются в придонном жидком слое. Лазерный луч, светящий сквозь мембрану, активирует молекулы фотополимера, и те начинают связываться друг с другом, но прилипнуть ко дну им мешает тонкий слой, насыщенный кислородом. Толщина такого «антипригарного» покрытия всего несколько десятков микрометров. Найдя баланс между проницаемостью мембраны, свойствами фотополимера и мощностью лазера, можно сделать весь процесс 3D-печати необычайно быстрым.

В своих экспериментах разработчики технологии добились скорости в 500 миллиметров в час, что в 100 раз превосходит скорость печати методом обычной лазерной стереолитографии. А напечатанное изделие эффектно появляется из ванны, наполненной жидким полимером.

МОДЕРНИЗАЦИЯ ИТ-ИНФРАСТРУКТУРЫ ИНТЕРНЕТ-МАГАЗИНА «М.ВИДЕО»

Компания «Инфосистемы Джет» построила модульную виртуализованную ИТ-инфраструктуру для работы новой программной платформы интернет-магазина «М.Видео».

АЛЕКСАНДР СКОРОБОГАТОВ, начальник отдела корпоративных решений Центра проектирования вычислительных комплексов компании «Инфосистемы Джет»

ИТ-инфраструктура состоит из нескольких типовых модулей, решающих разные задачи: предоставление статической информации, динамическая генерация контента, обработка поисковых запросов, обращение к базам данных и др. Разделение по функциональным ролям позволяет выявлять узкие места в части производительности и масштабировать только конкретные проблемные участки. Ускорить этот процесс помогают шаблоны развертывания, преднастроенные для каждого модуля. Большая часть ИТ-сервисов размещена в виртуальной среде и зарезервирована по схеме N+1. Сервисы, наиболее требовательные ко времени отклика (обработка поисковых запросов и обращений к базам данных, запросы в кэш), расположены на физических серверах. Их отказоустойчивость обеспечивается кластерной конфигурацией.

Целостность сессий обеспечивается сетевыми балансировщиками, которые также кластеризованы. Например, отложив товар, покупатель может продолжить поиск по сайту – статус его корзины не изменится.

Помимо продуктивного ИТ-ландшафта, созданы среды разработки, тестирования и нагрузочного тестирования. При этом в течение нескольких дней все вычислительные мощности могут быть переведены в продуктивный режим – для непосредственного обслуживания онлайн-покупок.

Компания «Инфосистемы Джет» осуществляет аутсорсинг сопровождения ИТ-инфраструктуры, включающий, в том числе, мониторинг доступности сайта, аппаратной среды и системного ПО.

«Покупатель редко сообщает о неполадках в работе интернет-магазина – он просто сразу переходит на другой ресурс. Наша задача – заранее учитывать возможность резких скачков трафика, принимать проактивные меры на случай сбоев при обновлении ПО, четко соблюдая параметры SLA», – поясняет **Александр Скоробогатов, начальник отдела корпоративных решений Центра проектирования вычислительных комплексов компании «Инфосистемы Джет».**

> Модернизация упростила обслуживание ИТ-комплекса и обеспечила высокую скорость масштабирования его компонентов. Добавление новых вычислительных ресурсов не требует изменений на прикладном уровне и может быть произведено в течение 1,5–2 часов (ранее на это требовалось 2–3 месяца).

«Интернет-магазин – ресурс бизнес-критичный. Его недоступность приводит к репутационным потерям и упущенной выгоде, – рассказывает **Дмитрий Постников, руководитель группы архитектуры и контроля качества web-разработок компании “М.Видео”.** – Теперь наш интернет-магазин справляется с пиковыми нагрузками в высокие сезоны, а ИТ-платформа может гибко трансформироваться под изменения трафика. Показательным стал период новогодних праздников, когда наблюдался 3-кратный наплыв пользователей. Благодаря гибкой архитектуре и быстрой реакции специалистов службы поддержки работоспособность интернет-магазина была обеспечена даже в этих условиях».

В ближайших планах – тестирование новых релизов прикладной системы и их установка в продуктивную среду, а также реализация мониторинга интернет-магазина «глазами пользователя». Это позволит в реальном времени контролировать скорость выполнения различных пользовательских сценариев: от загрузки главной страницы и поиска товара до оформления заказа и проведения оплаты.

КАК ДОБИТЬСЯ ЕДИНСТВА ПРОТИВОПОЛОЖНОСТЕЙ

АНДРЕЙ ШАПОШНИКОВ,
заместитель директора Центра проектирования вычислительных комплексов компании «Инфосистемы Джет»

Мы живем в мире, пронизанном идеями дуализма. Что первично – курица или яйцо? Что определяет бытие – дух или материя? Что важнее – вера или знание? Такого дуализма не избежала и наша профессиональная область – информационные технологии.

Можно обозначить первую пару противоположных и не сводимых друг к другу начал, относящихся к теме нашего номера, – инфраструктура физическая и инфраструктура виртуальная. Виртуализация проникла уже на все уровни ИТ-ландшафтов – в сети передачи данных, в сети и системы хранения данных, в серверные системы и комплексы. Дошло до того, что, хотим мы того или нет, но, используя современное оборудование, мы уже фактически не можем говорить о нем только как о физическом объекте. Всё его внутреннее устройство, точнее, логика работы, является виртуальным (пример – современные дисковые массивы, зачастую не дающие непосредственно управлять размещением данных на дисках). Дальше – больше: мы уже всерьез говорим о следующей стадии виртуализации – о приходе программно-определяемых инфраструктур.

Но стала ли современная ИТ-инфраструктура с приходом виртуализации проще? Нет, напротив – при определенном упрощении физического уровня (используется меньшее разнообразие аппаратных архитектур) мы наблюдаем существенное усложнение уровня логического, усугубляемое взаимопроникновением технологий. Например, на серверной платформе с использованием средств виртуализации можно реализовать и SAN с СХД, и виртуальную сеть передачи данных, наладить предоставление других сервисов, ранее доступных только в физическом исполнении (например, сервисов ИБ). При этом в работе остаются и физические устройства со сходным функционалом.

Вторая пара противоположных начал все последнее десятилетие, по сути, служила драйвером развития инфраструктурных технологий, в том числе виртуализации. Речь, с одной стороны, об объединении, с другой – о разделении. Как многие, наверное, помнят, первые «открытые системы», как и их родоначальники – «мейнфреймы», были «одиночками», не связанными даже сетевым взаимодействием. Но постепенно, вначале, как водится, неспешно, а потом все быстрее и быстрее сетевые интерфейсы и протоколы стали объединять разрозненные локальные компьютеры в локальные, а позже и в глобальные сети.

С увеличением размера сетей и стандартизации протоколов встали два вопроса – как сохранить производительность и обеспечить безопасность? Ответом в локальных сетях, основанных на протоколе Ethernet, стала первая ласточка сетевой виртуализации – технология VLAN, в скором времени стандартизированная. Затем появились другие технологии и стандарты, призванные обеспечить необходимую пропускную способность для высококритичного трафика и вместе с тем изолировать друг от друга сегменты сети с различными требованиями.

Сходным образом в свое время развивалась виртуализация и на других уровнях ИТ-ландшафта – объединяя ресурсы в единые общедоступные «пулы» и изолируя разнородные по тем или иным признакам (разные виды, категории, профили нагрузки и т.п.) ресурсы друг от друга.

Таким образом, современная виртуализованная инфраструктура включает не только сложно-скомбинированные физические и виртуальные сущности, но и целый набор разнородных связующих и разделяющих технологий.

С учетом этого третья, более драматичная, дилемма лежит в области эксплуатации современных виртуализованных инфраструктур. Мало построить такую инфраструктуру – надо уметь решать актуальные бизнес-задачи с ее помощью: масштабировать инфраструктуру прикладных систем в соответствии с потребностями бизнеса, разворачивать под новые проекты, обеспечивать необходимую доступность приложений и данных. Важно также решать эти задачи эффективно – в срок, качественно и в рамках бюджетов.

В чем же тут дилемма? В том, что обещающие такой инфраструктуре максимальную эффективность средства автоматизации управления облачного типа (портал самообслуживания, оркестрация и т.п.) либо сложны и дороги во внедрении и обслуживании, либо работают «из коробки» на очень ограниченном, однородном (в идеале – от одного вендора) системном ландшафте. При этом привычные методы управления физической инфраструктурой с использованием узких специалистов в разных тематических областях, выстроенных в жесткую организационно-штатную структуру, уже не могут обеспечить необходимую эффективность.

Есть ли выход из этой дилеммы? На наш взгляд, выходом является применение в создании и эксплуатации виртуализованной инфраструктуры сервисного подхода. Он заключается в том, что каждая инфраструктурная система – сеть передачи данных, СХД, серверный комплекс и т.д. – предоставляет типовые сервисы определенных классов, из которых, в свою очередь, формируется ИТ-инфраструктура, обеспечивающая работу соответствующих классов прикладных систем. Классы инфраструктурных сервисов формируются в зависимости от требований прикладных ИС и функциональных особенностей конкретной инфраструктурной системы.

Параметрами, по которым проводятся классификация и типизация сервисов, могут быть, например, тип аппаратной платформы, требования по производительности, времени хранения и восстановления данных, необходимость обеспечения высокой доступности (HA) и катастрофоустойчивости (DR) сервиса.

В состав предоставляемой прикладной системе ИТ-инфраструктуры должны также входить определенные схемы обслуживания и программы технической поддержки, соответствующие заданному классу.

Понятно, что применение сервисного подхода к существующему ИТ-ландшафту потребует определенного объема организационно-методических работ. Надо систематизировать информацию по эксплуатирующимся прикладным системам, определить требования к их функционированию со стороны бизнес-подразделений (критичность, время восстановления) и, соответственно, сформулировать требования к инфраструктурным сервисам. Кроме того, после проведения необходимых технических работ по проектированию и настройке необходимых классов инфраструктурных сервисов потребуются разработка и ввод в действие пакета стандартов, регламентов и инструкций, определяющих действия ИТ-службы по выбору и настройке ИТ-инфраструктур по требованиям прикладных систем.

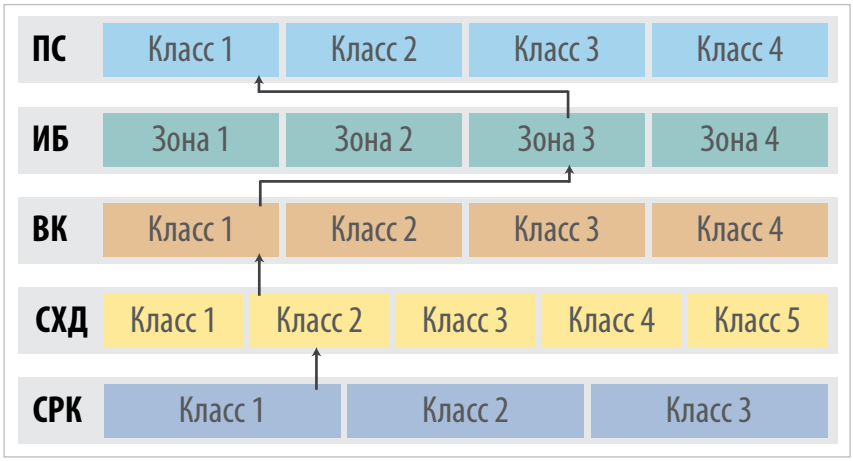


Рис. 1. Схема формирования ИТ-инфраструктуры для прикладной системы из различных инфраструктурных сервисов

Еще одной особенностью сервисного подхода является то, что он дает возможность создать модель стоимости предоставляемой конкретной прикладной системе ИТ-инфраструктуры, а значит, закладывает основу для более эффективного финансового управления ИТ-активами компании.

Далее в нашем номере мы подробно рассмотрим технологии, позволяющие в той или иной степени реализовать описанный нами подход и эффективно использовать его для решения бизнес-задач.

КОГДА С SDN ЖИТЬ ХОРОШО

АЛЕКСЕЙ КОЛЯСКИН,
заместитель директора по работе с операторами связи
Центра сетевых решений компании «Инфосистемы Джет»

На протяжении последних двух лет тема программно-конфигурируемых сетей (SDN) остается в центре внимания профессионалов ИТ-индустрии и производителей оборудования и программного обеспечения. Тем не менее говорить о каких-либо масштабных внедрениях этой технологии в корпоративном или операторском секторе пока не приходится. Наша статья является попыткой ответить на вопрос «когда технология SDN придет и в нашу сеть?».

НЕМНОГО ИСТОРИИ

За десятилетия, прошедшие с момента создания используемых и по сей день сетевых технологий, таких как Ethernet и IP, изменилось довольно мало. Базовые принципы, заложенные в основу сетей с коммутацией пакетов, долгое время оставались неизменными. Но в середине 2000-х годов группа американских ученых решила пересмотреть сами основы, составляющие фундамент современных сетей. Так на свет появились технология SDN и протокол OpenFlow, являющийся ее неотъемлемой частью.

Основная идея, на которой базировалась новая технология, – нужно убрать любую «интеллектуальную» составляющую с сетевого оборудования, делегировав процесс принятия решения об обработке трафика выделенному серверу (контроллеру). В качестве средства взаимодействия между сетевыми элементами и контроллером предлагалось использовать стандартизованный протокол – OpenFlow. Единицей планирования информационного обмена стал поток (Flow). Поток определяется оборудованием на основании значения полей 2-го, 3-го и 4-го уровней каждого отдельного пакета, а также их произвольных комбинаций. Именно количество одновременно поддерживаемых потоков (Flow) является главной характеристикой SDN-коммутатора.

В настоящий момент развитием и стандартизацией протокола OpenFlow, который, по сути, является краеугольным камнем технологии SDN, занимается международная организация Open Networking Foundation. На ее сайте представлены открытые спецификации протокола и другая полезная информация по теме.

ДЛЯ ЧЕГО ЭТО НУЖНО?

Итак, для чего же создавалась эта технология? Какие преимущества она дает по сравнению с традиционной сетевой инфраструктурой? Чтобы она прижилась и пошла в массы, должны иметь место существенные плюсы от ее применения. Безусловно, такие плюсы есть, это:

+ единый механизм управления всеми сетевыми устройствами (протокол OpenFlow);
+ возможность самостоятельно определять логику коммутации внутри сети.

Если по первому пункту выгоды от внедрения вполне очевидны (стандартизация и, как следствие, автоматизация и упрощение управления сетью), то по второму все далеко не так просто. Да, безусловно, реализация собственной логики коммутации – это интересно, но какие выгоды она дает конечному потребителю?

На самом деле фундаментальных выгод всего две:

1. возможность организации виртуальных сетей (Virtual Tenant Networks);
2. создание сервисных цепочек (Service Chaining).

Стоит упомянуть также такие «встроенные» возможности сетей на базе SDN, как баланси-

	Матрица коммутации	Интерфейсы	Количество Flow	Количество на рынке
Core switch	От 1 Тбит/с	1G, 10G, 40G, 100G	От 1 млн	< 5
ToR switch	1–2 Тбит/с	1G, 10G, 40G	8–500 тыс.	< 30
Access switch	До 200 Гбит/с	10/100/1000, 1G, 10G	2–4 тыс.	< 15

Табл. 1. Основные характеристики коммутаторов различных групп, представленных на рынке

ровка трафика и использование произвольных сетевых топологий, но все же определяющими являются именно первые два преимущества.

АППАРАТНАЯ ПОДДЕРЖКА SDN

Любой технологии, претендующей на существенную долю рынка, необходима поддержка со стороны производителей аппаратного обеспечения. В случае SDN это прежде всего коммутаторы с поддержкой протокола OpenFlow. В настоящий момент на рынке представлено некоторое количество таких устройств от различных производителей. Их условно можно поделить на три группы:

- большие модульные коммутаторы (Core switch);
- коммутаторы уровня Top of the Rack для ЦОД (ToR switch);
- коммутаторы доступа (Access switch).

Какие выводы можно из нее сделать?

✓ На рынке наблюдается существенный дефицит в сегменте коммутаторов доступа. При этом их текущие характеристики в части количества Flow оставляют желать лучшего. Прибавив к этому весьма скромные возможности по модификации трафика у подавляющего числа моделей, можно сделать неутешительный вывод – в этом сегменте практически нет устройств, пригодных для практического использования. Более того, скорее всего, достойных коммутаторов и не появится, так как производители вряд ли будут вкладывать деньги в выпуск новых гигабитных моделей.

✓ Наиболее полноценный сегмент рынка на настоящий момент – коммутаторы класса ToR (Top-of-the-Rack). Изначально этот класс оборудования предназначался для ЦОД, но такие коммутаторы могут быть успешно использованы на уровне агрегации корпоративной сети или сети оператора связи. Такое положение дел обусловлено тем, что коммутаторы построены на современных чипсетах, которые обладают значительными объемами памяти и широкими возможностями по модификации трафика. Более того, модельный ряд данного сегмента активно расширяется, поэтому стоит ожидать появления гораздо более продвинутых в части SDN коммутаторов.

✓ Что же касается коммутаторов уровня ядра, то достойных представителей этого семейства можно пересчитать по пальцам одной руки. Тем не менее такое положение нельзя назвать катастрофическим: коммутаторы подобного класса, как правило, строятся на базе весьма умных чипсетов либо сетевых процессоров, что позволяет производителям в случае необходимости реализовать полноценную поддержку SDN в уже существующих моделях.

ЕСТЬ ЛИ ВЫХОД?

Да, безусловно, выход есть всегда. Если в настоящий момент не получается использовать SDN на аппаратных коммутаторах ввиду их малого распространения, можно рассмотреть возможность использования оверлейных сетей и виртуальных коммутаторов.

Отметим, что использование оверлейных сетей возможно далеко не во всех случаях. Ту же корпоративную сеть невозможно полностью построить, используя наложенные сети. Но в центрах обработки данных или в распределенных сетях (WAN) использование технологии представляется весьма уместным.

В настоящий момент среди протоколов инкапсуляции, используемых для построения наложенных сетей, определились 2 основных лидера – это всем знакомый GRE (Generic Routing Encapsulation) и новый протокол VxLAN. Они оба, по сути, являются инкапсуляцией, позволяющей организовать общение виртуальных коммутаторов на втором

уровне через традиционную L2/L3 сетевую инфраструктуру. Таким образом, использование оверлейных сетей позволяет совместить в рамках одной сетевой инфраструктуры как традиционный подход, так и технологию SDN.

SDN + NFV

Другим трендом последних лет является виртуализация всего и вся. Как следствие, виртуализация добралась и до сетевых функций – маршрутизации, NAT, фильтрации и исследования трафика и т.д. Многие производители, выпускающие аппаратные решения в этой области, либо уже выпустили, либо готовят к выпуску виртуализованные версии своих продуктов.

Этот бум обусловлен двумя обстоятельствами – существенным увеличением производительности x86-серверов и появлением большого числа SDN-подобных технологий. За первым фактором, помимо закона Мура, стоят усилия многих компаний по существенному увеличению производительности платформы x86 в задачах обработки трафика. В частности компания Intel, специализирующаяся на аппаратном обеспечении, вкладывает значительные средства в разработку библиотек для высокоскоростной обработки трафика и разработки сетевых приложений. Разработанная ею библиотека Intel DPDK (Data Plane Development Kit) используется в продуктах очень многих компаний и позволяет сетевым приложениям достигать производительности от 20 до 40 Гбит/с на один процессор в зависимости от сложности задачи.

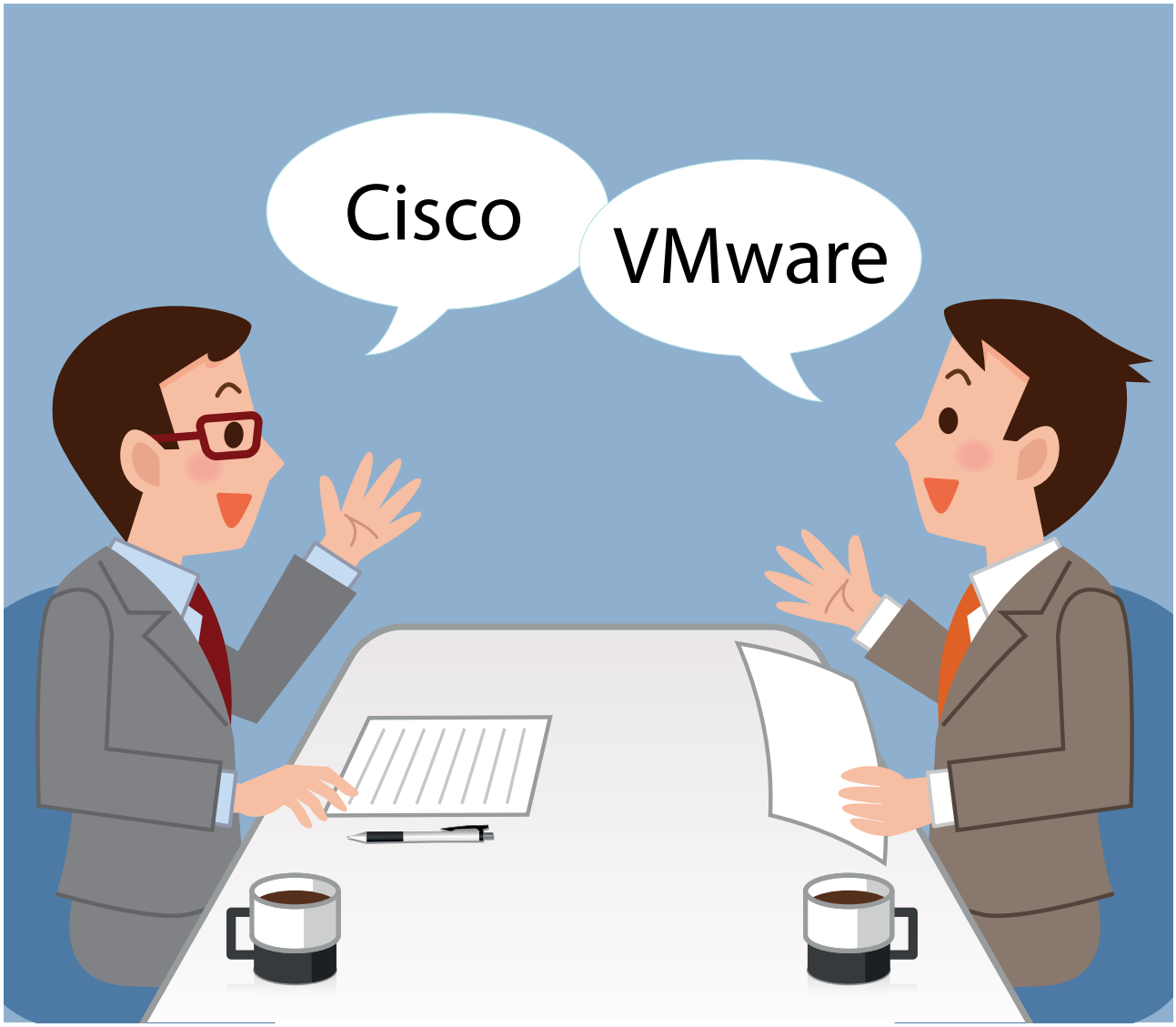
Что касается второго обстоятельства, появление на рынке большого количества фирменных SDN-подобных решений также требует наличия виртуализованных сетевых функций. Работать с виртуализованным оборудованием куда проще, чем с реальным: резервирование и масштабирование не вызывают в этом случае особых проблем.

Для конечного потребителя процесс виртуализации сетевых функций сулит сплошные выгоды: независимость от аппаратных платформ, плавное увеличение производительности и использование недорогих x86-серверов общего назначения. Однако применение лишь технологии NFV (Network Function Virtualization) не дает больших преимуществ в части администрирования сети. При замене физического оборудования на виртуальное никуда не исчезают проблемы с обеспечением отказоустойчивости, балансировкой нагрузки, настройкой маршрутизации, коммутации и т.д.

> Использование оверлейных сетей возможно далеко не во всех случаях. Ту же корпоративную сеть невозможно полностью построить, используя наложенные сети. Но в ЦОД или в распределенных сетях (WAN) использование технологии представляется весьма уместным

Хорошей идеей в данном случае является симбиоз 2 технологий – SDN и NFV. Используя возможности SDN по изоляции трафика, созданию сервисных цепочек и балансировке нагрузки и применяя в рамках создаваемой инфраструктуры виртуализованные сетевые функции, можно добиться поразительного результата. Становится возможным персонализировать набор сетевых услуг вплоть до конкретного подразделения или сотрудника в корпоративном секторе либо до конкретного абонента в случае оператора связи. А это прямой путь к предоставлению сетевых услуг по столь популярной в настоящее время сервисной модели, когда конечный потребитель платит только за то, что ему необходимо. JI

ДИАЛЕКТИКА ВИРТУАЛЬНЫХ СЕТЕЙ



ДМИТРИЙ БОРОДИН,
эксперт по системам передачи данных Центра сетевых решений компании «Инфосистемы Джет»

Виртуализация всего и вся идет уже довольно давно, и в последний год очередь дошла до виртуализации сетей. В образовавшуюся нишу отправилось множество свежих голов и стартапов, но главными претендентами на лидерство в этой области являются две компании – технологический лидер сетевых решений Cisco Systems и лидер рынка виртуализации серверов VMware. Их подходы, в соответствии с «родословной», противоположны, хотя решаемые задачи совпадают.

VMware – лидер магического квадранта Gartner разработчиков решений для виртуализации серверов архитектуры x86 за 2014 год.
Cisco Systems принадлежат 60% рынка сетевых технологий в 2014 году, по данным Infonetics Research.

Прежде всего стоит определиться с понятиями: что именно мы называем виртуальными сетями. В индустрии уже есть устоявшиеся термины, такие как виртуализация сетевых функций (Network Functions Virtualisation, NFV), то есть виртуализация устройств (маршрутизаторов, балансировщиков, межсетевых экранов), как правило, на серверах платформы x86.

Есть понятие «программно-определяемые сети» (Software Defined Network, SDN) – по факту, это централизованное управление потоками трафика, когда решение о выборе пути следования данных принимается на сервере и сообщается всем сетевым коммутаторам/маршрутизаторам. Понятие SDN сейчас во многом является маркетинговым, что размывает его смысл. Например, Cisco позиционирует ACI (Application Centric Infrastructure) как SDN, хотя это «программно-определяемое» решение не имеет программных компонент – даже контроллеры аппаратные.

В нашей статье мы будем называть виртуальными (по аналогии с виртуализацией серверов) сети, соответствующие следующим требованиям:

Общее множество ресурсов, единая точка управления. Это ключевая особенность SDN. Узел сети получает сервисы независимо от своего физического и логического размещения, а точка управления всей инфраструктурой одна и не меняется во время эксплуатации.

Быстрое выделение ресурсов. Когда компании нужно развернуть новый сервис или приложение, выделение ресурсов под него должно происходить быстро, при этом не влияя на остальные сервисы.

Узкая сегментация и изоляция приложений. Приложения должны быть изолированы друг от друга, даже если они работают на одном физическом CPU (на одном процессоре одного сервера). Разные компоненты приложения в соответствии с политикой безопасности должны иметь возможность взаимодействовать исключительно так, как задумано администратором.

Гибкость в адресации и топологии сети. Новые приложения могут располагаться в любом месте ЦОДа, компонентам на разных площадках, в том числе может потребоваться размещение в одной подсети. Сеть не должна ограничивать приложения в гибкости.

В итоге мы можем рассматривать виртуализацию сети аналогично виртуализации серверов. Отметим, что сама сеть с виртуализацией может быть дороже обычного варианта, но при этом снижать TCO за счет более эффективного использования ИТ-ресурсов. Отметим, что в статье будет идти речь о сетях в ЦОД.

2 ЛИДЕРА: НЕМНОГО ИСТОРИИ

Историю виртуализации сетей принято отсчитывать с 2006 года, когда Мартин Касадо, будучи аспирантом Стэнфордского университета, представил проект Ethane. Его основная идея: сетевые устройства должны осуществлять только передачу данных (data plane), а управление передачей данных (control plane) выполняет централизованный контроллер.

В 2007 году Мартин Касадо, Ник МакКьоун и Скотт Шенкер создали компанию Nicira и начали разработку платформы сетевой виртуализации (Network Virtualization Platform, NVP). Продукт работает на основе OVS (Open vSwitch) и стандарта OpenFlow, в настоящий момент носит название NSX MH (NSX Multi-Hypervisor).

В 2011 году была основана некоммерческая организация Open Network Foundation. Основателями проекта выступили гиганты ИТ-рынка – Google, Microsoft, Verizon, Yahoo!, Facebook, Deutsche Telecom. Цели организации – развитие программно-определяемых сетей. Фактически она развивает стандарт OpenFlow, ранние версии которого очень напоминали работы Мартина Касадо образца 2006–2007 годов, являясь по сути стандартом на основе концепций Ethane.

В 2012 году VMware приобрела Nicira за 1,26 млрд долларов.

Обычно сделки такого масштаба осуществляются за счет передачи ценных бумаг/обязательств, но в данном случае VMware оплатила покупку живыми долларами. Было объявлено, что платформа сетевой виртуализации Nicira отныне будет называться VMware NSX.

Компания Cisco, наблюдая за трендами виртуализации и программируемости сетей, решила их возглавить. Сони Джандани перешла из Cisco в стартап Insieme Networks. Его основателями выступили три бывших сотрудника Cisco Марио Маццола, Прем Джейн и Лука Кафьеро, одним из основных инвесторов стала сама Cisco Systems. Cisco окончательно приобрела Insieme в ноябре 2013 года. Результатом работы стартапа стала ACI (Application Centric Infrastructure) – инфраструктура, ориентированная на приложения. Название очень точно описывает суть решения, но об этом позже. Аналогичным образом в свое время появились Fibre Channel коммутаторы MDS, серверные решения Cisco UCS, коммутаторы Cisco Nexus.

ЕСТЬ ЕЩЕ ВАРИАНТЫ?

Стоит отметить и другие решения по виртуализации сетей.

Arista одной из первых начала продвигать SDN-решения, сейчас их продукт позволяет хорошо автоматизировать сеть, интегрируется с различными гипервизорами и оркестраторами. Автоматизацию сети функционально дополняет интеграция с VMware NSX.

HP предлагает OpenFlow SDN-контроллер. Главное узкое место OpenFlow контроллеров – крайне скудный функционал «из коробки», функции наращиваются путем установки приложений.

В HP создали магазин приложений по аналогии с Android Market и Apple App Store. Другой вопрос – малый размер таблиц под Flow-записи на стандартных микросхемах коммутации – сняли с помощью подхода «SDN только до распределения». Пока приложений не так много, поэтому магазин не пользуется большой популярностью.

Juniper Networks, когда речь заходит о виртуальных сетях, предлагает аппаратные шлюзы для VMware NSX.

Есть еще множество небольших компаний, стремящихся на новый рынок, но либо они сейчас занимают незначительные ниши, либо их решения еще не совсем соответствуют требованиям современных ЦОДов.

> Cisco рассматривает приложения с точки зрения бизнеса – в качестве сервисов, которые оказываются пользователю. Например, это почта, ERP, CRM и т.д.

Стоит отметить Cumulus, которая предлагает операционную систему для установки на White/Brite Box коммутаторы (без поддержки/с поддержкой производителя). Она может быть интересна тем компаниям, у которых вся инфраструктура на Linux, много специалистов по этой ОС и довольно большая сеть.

Также внимания заслуживает Pluribus Networks, которая делает коммутаторы путем подключения специализированных микросхем к серверам. В итоге аппаратный коммутатор может сохранять/обрабатывать сетевой трафик приложений и имеет очень большой задел по программируемости и мониторингу приложений на сетевых устройствах.

VMWARE NSX

VMware делает виртуализацию сетей так, как привыкла работать, – с помощью ПО на серверах.
По сути, NSX – это лицензии, виртуальные машины и модули для гипервизора, которые устанавливаются автоматически с виртуальной машины.

Со стороны сетевого оборудования виртуальная сеть выглядит как множество VXLAN-туннелей между серверами. То есть от сетевого оборудования требуется только обеспечить хорошую пропускную способность, не нужны даже большие CAM-таблицы и поддержка multicast.

Опустим описания концепции и подхода – их много в пресс-релизах вендора. Остановимся на предоставляемом функционале. NSX позволяет объединять виртуальные машины в одну виртуальную подсеть, даже если серверы, на которых эти машины расположены, находятся в разных подсетях. Это обеспечивается штатным функционалом VXLAN.

В том числе можно объединить несколько площадок в единую сеть, если они находятся на небольшом расстоянии (до 50–100 км), в ином случае могут потребоваться другие технологии.

NSX дает возможность маршрутизировать трафик между виртуальными машинами в виртуальной сети. Для этого не нужно перенаправлять его куда-либо, маршрутизация осуществляется локально на отправляющем сервере. Таким образом, решается проблема неоптимального пути, а также сайзинга.

В решении есть компонент безопасности – межсетевой экран.

Его правила применяются не только между сетями, но и внутри одной сети, даже если виртуальные машины находятся на одном сервере, при этом нет необходимости перенаправлять весь трафик на другую виртуальную машину (это уменьшает расходы). За (меж-)сетевое экранирование, как и за маршрутизацию, отвечает модуль в гипервизоре. NSX интегрируется со сторонними средствами безопасности и может загружать правила безопасности из них. Также можно задавать их через API или вручную. Поскольку правила гибкие и наглядные, зачастую NSX рассматривают исключительно как средство безопасности.

Для подключения виртуальной сети к остальной физической сети можно использовать аппаратные (от классических производителей) или виртуальные шлюзы. Штатный виртуальный шлюз, помимо подключения к внешним сетям, обеспечивает следующий функционал: NAT, DHCP, VPN, маршрутизацию с поддержкой OSPF. Также он выполняет функции межсетевого экрана, балансировщика нагрузки, обладает отказоустойчивостью.

> Сейчас Cisco разрабатывает виртуальный контроллер APIC-EM, предназначенный для корпоративной части сети. Это принципиально иной продукт, который будет управлять существующим оборудованием. Его настройка будет существенно отличаться от ACI.

Управляется NSX либо автоматизированно через оркестратор, либо администратором через графический интерфейс vSphere (так же, как и остальная виртуальная инфраструктура VMware). Управление NSX осуществляется из отдельного раздела, доступ к которому можно дать как сетевым, так и инфраструктурным администраторам.

Поскольку сетевые сервисы выполняются на серверах распределенно, возникает вопрос, насколько «железо» загружается от этой дополнительной задачи. VMware заявляет, что дополнительная нагрузка на гипервизор не превышает 6%.

Кратко перечислим возможности и роли NSX:

- возможность полностью менять топологию сети и сервисы, в том числе подключать новые сегменты без влияния на уже существующие из одной точки и быстро;
- распределенный маршрутизатор/коммутатор на всех серверах с виртуальными машинами;
- распределенный (меж-)сетевой экран;
- шлюз NSX с сетевыми сервисами;
- VXLAN Overlay: топология виртуальной сети не зависит от топологии сети физической.

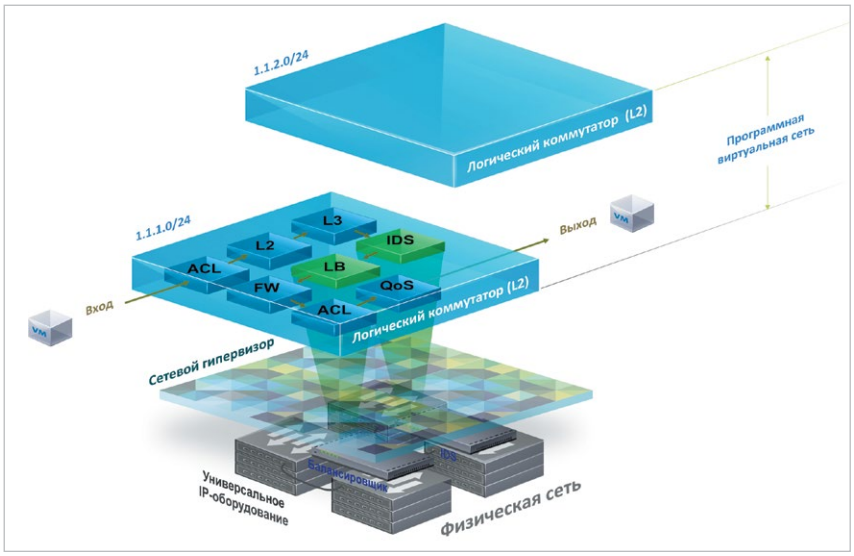


Рис. 1. Логический путь трафика внутри NSX

ACI от Cisco

Сегодня, по данным мировых аналитических агентств, около 80% вычислительной нагрузки виртуализовано, в то же время 80% компаний по-прежнему имеют серверы без виртуализации (обычно в дополнение к виртуализованным). 42% компаний используют более одного гипервизора – не только VMware ESXi, но и другие. NSX же решает задачи только для фермы серверов VMware.

Cisco стремится занять свободную нишу с помощью ACI. Решение состоит из коммутаторов серии Nexus 9000 и аппаратных контроллеров на базе серверов Cisco UCS. Коммутаторы могут работать либо в стационарном режиме NX-OS так же, как и остальные коммутаторы Nexus, либо в режиме ACI – под управлением контроллера. Nexus 9000 обладают большой плотностью портов, хорошей производительностью, но в режиме NX-OS функционал у них не так обширен. В режиме фабрики (ACI) контрол-

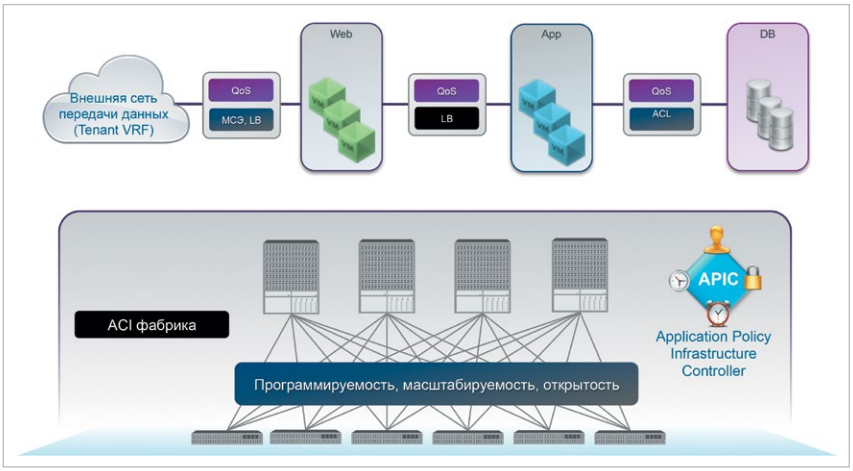


Рис. 2.Схема работы ACI

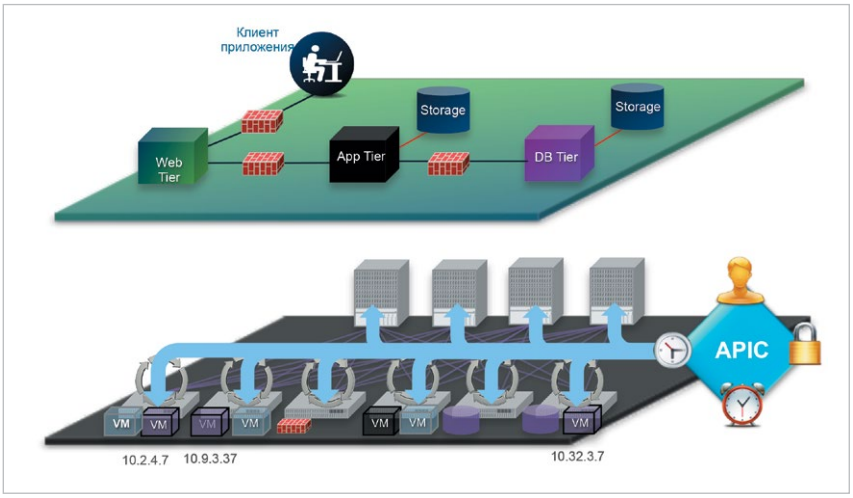


Рис. 3. Одна инфраструктура – много логических сервисов

лер оперирует понятиями приложения. На рис. 2 изображено типичное 3-уровневое приложение.

Администратор указывает, какие серверы или виртуальные машины относятся к той или иной группе серверов и как эти группы должны взаимодействовать. Остальное – забота контроллера, который динамически перенастраивает все оборудование. Таким образом, трафик динамически перенаправляется на межсетевые экраны и балансировщики нагрузки. Сетевые сервисы можно реализовать на оборудовании стороннего производителя, если он выпустил профайл, согласно которому APIC понимает возможности этого «железа». Многие крупные производители (например, Check Point, F5) уже выпустили такие профайлы. Контроллер перенастраивает сеть при миграции виртуальных машин, удаляя правила там, где они больше не нужны.

На рис. 3 изображены физическая и логическая сети для одного приложения. Логических сетей может быть очень много, они могут иметь совершенно разную топологию, но это никак не влияет на физическое расположение узлов в сети. Поведение сети зависит от правил и политик, заданных для взаимодействия компонент каждого приложения. Трафик, который не подходит ни под одно явно заданное правило взаимодействия групп, будет дропаться.

Физически всегда используется 2-уровневая архитектура (Spine-Leaf), причем Spine- и Leaf-коммутаторы отличаются на аппаратном уровне. Аппаратные особенности позволяют контроллеру получать такую информацию, как количество переданных пакетов между двумя группами серверов, задержек на передачу и потерь по каждому из путей внутри фабрики и между группами серверов в целом. Также они гарантируют решение проблем out of order delivery и пр. В том числе на основе этой информации строится система оценок в диапазоне от 0 до 100. Оценка выдается как приложению в целом, так и отдельным группам соединений, коммутаторам и т.д. Другой вопрос, насколько она полезна, если на нее в том числе влияет количество свободных портов на уровне доступа.

Стоит отметить, что Cisco кардинально меняет подход к управлению сетью. Классически сеть настраивалась из командной строки, теперь же вся настройка происходит с помощью кликов мышкой по множеству «мастеров». Пример такого «мастера» изображен на рис. 4. Более того, в интерфейсе контроллера настраивается логика работы приложений, а не коммутаторов. В интерфейсе коммутаторов в режиме ACI возможности по внесению изменений в конфигурацию крайне ограничены.

СРАВНЕНИЕ И ВЫВОДЫ

Если говорить о технических возможностях, NSX хорош там, где все или абсолютное большинство серверов виртуализованы с помощью VMware. ACI в принципе работает только там, где сеть в ЦОД построена на коммутаторах Nexus 9k, зато к ACI напрямую подклю-

чаются как виртуальные машины (VMware ESXi), так и физические серверы.

NSX – это виртуальная сеть до виртуальной машины. А машины должны быть обязательно виртуализованы с помощью технологий VMware. Cisco в общем случае предоставляет сеть до подключаемых серверов, но политики фабрики можно «растянуть» до виртуальных машин с помощью установки виртуального коммутатора AVS, аналога Nexus1000 для ACI. AVS официально поддерживается только под VMware ESXi (на март 2015), но ходят слухи, что существуют AVS для Hyper-V. Отметим, что AVS под VMware не поддерживается самой VMware, поэтому есть риск «застрять» между поддержками двух вендоров в случае инцидента.

> Если вы планировали строить Cisco FabricPath, имеет смысл посмотреть в сторону ACI, скорее всего, получится и дешевле, и функциональнее (правда, будьте готовы описать все сетевые взаимодействия в ЦОДе).

NSX – «размазанная» сеть, проблема сайзинга во многом решается автоматически: вынос части виртуальных машин на новые серверы означает и вынос нагрузки на обработку трафика, поскольку внутри NSX трафик обрабатывается локально. ACI компенсирует локальную обработку на большие и «толстые» каналы, внутри фабрики множество 40 Gb/s каналов, чтобы заворачивать трафик на нужные сервисы. Зато у заказчика всегда

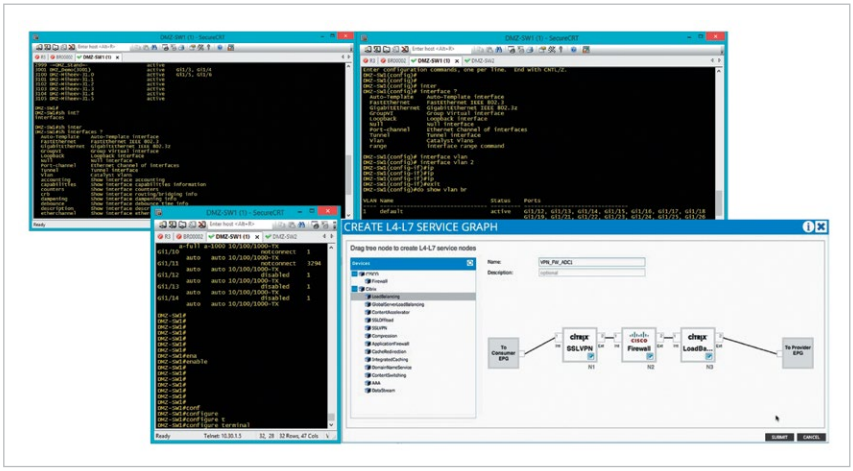


Рис. 4. Интерфейс настройки ACI

есть выбор. Например, функционала встроенного в NSX балансировщика нагрузки многим будет недостаточно. Использовать сторонние решения VMware позволяет, но так же, как это происходит в классических сетях. NSX такую балансировку автоматизировать и упрощать не будет.

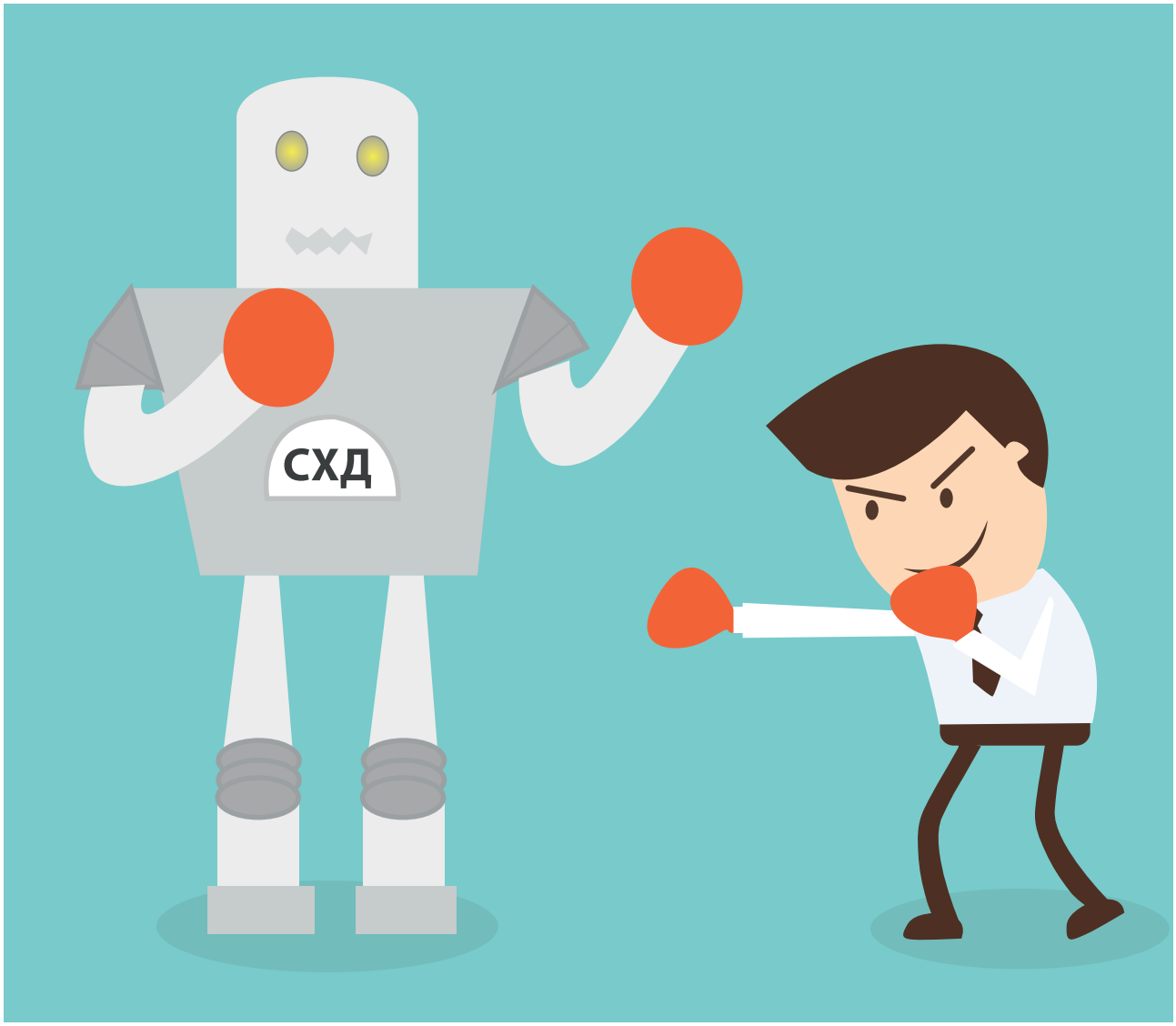
Что касается автоматизации за счет оркестратора, Cisco ACI «из коробки» интегрируется с Cisco UCS Director, VMware NSX – с VMware vCAC (vCloud Automation Center). Обе компании активно участвуют в проектах свободных оркестраторов и заявляют интеграцию с OpenStack.

Что касается DCI, NSX позволяет объединять в единую виртуальную сеть несколько площадок в рамках города или соседних городов, на больших расстояниях нужны специализированные технологии уменьшения задержек для приложений. Отметим, что связь удаленных площадок через NSX предпочтительнее, чем без него, даже если VXLAN не требуется. NSX имеет встроенные механизмы уменьшения BUM трафика, ARP запросов и т.д.

ACI-фабрику же можно разнести на несколько помещений в рамках одного здания, между которыми будет множество 40 Гб каналов. У Cisco есть очень хорошая технология обеспечения связности удаленных площадок – OTV. Но устройства, которые поддерживают ACI, не поддерживают OTV, и наоборот. В настоящее время есть рекомендованный дизайн связи нескольких фабрик ACI с помощью OTV (он не будет частью ACI), в дальнейшем планируется управление OTV-каналом с помощью ACI контроллера APIC.

В заключение стоит сказать, что финансовые аналитики из Goldman Sachs в отчете для инвесторов провели наглядную аналогию между подходами ACI и NSX – iPhone vs Android. ACI, как и iPhone, имеет вертикальную интеграцию, собственные микросхемы, аппаратную и программную часть. Как и Apple, Cisco сохраняет полный контроль над своей экосистемой. VMware NSX, как Android, работает на различных аппаратных платформах, может использоваться разными способами, например, в качестве межсетевого экрана или для DCI. Производитель не заставляет пользователя следовать жестко заданной архитектуре. Аналитики считают, что в этом противостоянии победителя не будет – обе компании, решающие одну задачу разными способами, займут свою часть рынка. JI

КОНКУРЕНТЫ ЖЕЛЕЗНЫХ СХД



АРТЕМ ДЕМАРИН,
эксперт отдела систем хранения данных
компании «Инфосистемы Джет»

Когда за окном плохая погода, многие предпочитают пользоваться услугами VoD (Video on Demand), а не идти в кинотеатр, или заказать еду с доставкой на дом, а не посещать кафе. Потребление различных ресурсов в качестве услуг год от года набирает популярность и сегодня для большинства людей является чем-то обыденным и само собой разумеющимся.

Постепенно требования к предоставлению ресурсов как услуг стали применяться и к ИТ-инфраструктуре/ИТ-сервисам. Активное использование систем серверной виртуализации дало возможность абстрагироваться от фиксированных конфигураций и обеспечить создание ресурсов по запросу. Это позволило на первичном этапе рассматривать ИТ-инфраструктуру и ИТ-сервисы в качестве услуг, но всё еще не давало требуемой гибкости и динамичности для удовлетворения всех текущих запросов пользователей. Для обеспечения этих характеристик и управления динамической инфраструктурой была разработана концепция программно-определяемого центра обработки данных (Software Defined Datacenter, SDDC), которая предусматривает абстрагирование от аппаратной части абсолютно всех компонентов ЦОД.

Этот подход существует уже довольно продолжительное время, но его реализация затрудняется из-за нескольких стопоров. Основной – инфраструктура хранения данных. В отличие от приложений, серверов и сети, ресурсы хранения, а вместе с ними данные продуктивных систем, зачастую оказываются привязаны к уникальному оборудованию различных производителей.

Исторически каждый производитель старался сделать свое

> Концепция SDDC предполагает упрощение инфраструктуры ЦОД за счет использования более однородных вычислительных компонентов и назначение им ролей на уровне ПО. При этом допускается как выделение компонентов под роль, так и совмещение нескольких ролей на одном наборе оборудования

решение на базе доступных ему аппаратных платформ и операционных систем или разрабатывал полностью новый комплекс с собственными программными интерфейсами (API) и уникальным набором функций. В итоге платформы и продукты настолько разнообразны, что массивы даже одного производителя могут быть не совместимы между собой (отсутствуют возможности полного или частичного взаимодействия, такие как, например, репликация).

Развитие стандартных вычислительных компонентов, в частности значительное повышение вычислительной мощности серверов платформы x86, и активное применение облачных технологий дали стимул для развития программно-ориентированных СХД (Software-Defined Storage, SDS).

Это решения, в которых за все функции хранения и управления данными отвечает ПО на базе набора стандартных компонентов вычислительных сред (серверов, дисковых полок расширения, коммутаторов, контроллеров и т.д.). Их главная особенность – отсутствие специализированных аппаратных средств, полностью или частично обеспечивающих реализацию отдельных функций. В данный момент можно выделить **несколько классов программно-ориентированных СХД:**

- программно-аппаратные решения, которые архитектурно повторяют классические массивы (EMC XtremIO, IBM FlashSystems и т.д.);
- независимое программное обеспечение для построения решения на базе x86 серверов (EMC ScaleIO, pNFS, RAIDIX, EuroNAS, Open-E и т.д.);
- объектные хранилища данных (Gluster, OpenStack Swift, Ceph, EMC Atmos, HDS HCP, Quantum Lattus, EMC ViPR и т.д.);
- Hadoop-совместимые хранилища (Apache Hadoop HDFS-совместимые решения);
- системы виртуализации дисковых ресурсов (EMC ViPR, IBM SVC, Huawei VIS и т.д.).

Отметим, что эта классификация является условной и зачастую продукты реализуют функции, относящиеся к нескольким классам.

ОБЪЕКТИВНЫЙ ПОДХОД

Производители классических массивов, предугадывая возможные тенденции развития ИТ-инфраструктур и пытаясь оптимизировать расходы на разработку новых продуктов, в последние 7–10 лет начали добавлять SDS-решения в свои портфели. Они в большинстве повторяют классические системы хранения: обеспечивают доступ к данным по стандартным протоколам (FC, iSCSI, IB, FCoE,

CIFS, NFS) и схожий функционал (динамическое управление ресурсами, репликация, мгновенные снимки, клоны и т.д.).

Соответственно, SDS-системы, архитектурно повторяющие классические массивы, имеют аналогичные технические ограничения: фиксированное количество контроллеров (нод), интерфейсных портов взаимодействия и накопителей (жестких дисков, SSD). Но переход на программно-определяемую реализацию функционала сделал возможным использование технологий, которые ранее были доступны только в сложных Hi-End (например, виртуализация внешних дисковых ресурсов). Включение продуктов на основе SDS в наборы решений базового и среднего уровня позволило производителям значительно увеличить функционал в этих сегментах.

Наибольшие популярность и распространение на данный момент имеют SDS-решения с объектным принципом хранения данных. Их основные потребители – средние и крупные сервисные провайдеры услуг по облачному хранению: Dropbox, Amazon, Google, Apple и др. В случае частных облаков применение объектного подхода гарантирует унификацию вычислительных компонентов и динамическое расширение инфраструктуры за счет добавления универсальных новых нод (серверов), которые могут обеспечивать сервис хранения одновременно с другими ролями.

В отличие от классических решений, которые отвечают за гарантированное хранение всего массива данных (в рамках одного ресурса), объектный принцип предусматривает хранение множества копий частей массива данных – так называемых объектов. Сохранность данных обеспечивается при доступности хотя бы одного экземпляра из множества.

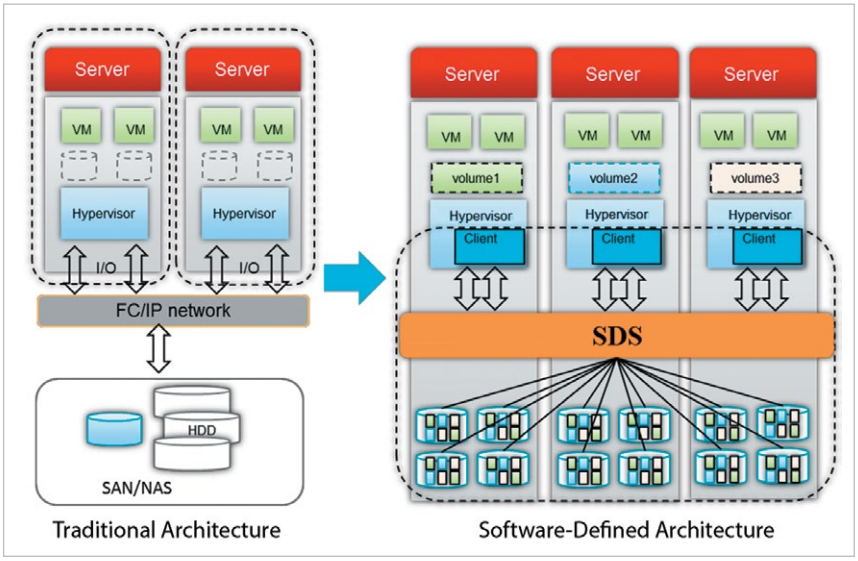


Рис. 1. Верхнеуровневое сравнение традиционной и программно-ориентированной архитектур хранения

За счет применения объектного хранения стала возможна организация резервирования данных в зависимости от места расположения компонентов SDS. Например, можно дублировать объекты на ресурсах разных узлов (серверов – участников SDS), размещенных в разных стойках ЦОД. Исходя из этого допускается потеря части компонентов при условии сохранения одной или более копий каждого объекта.

Объектный принцип обеспечивает значительно бóльшие масштабируемость и гибкость управления ресурсами. Повышение масштабируемости достигается за счет применения множества равноправных нод. В результате эта характеристика меньше зависит от ограничений аппаратных компонентов, чего нельзя сказать о классических массивах. Гибкость управления ресурсами обеспечивается за счет использования динамических алгоритмов распределения и хранения объектов, что позволяет оперативно подстраивать и изменять принципы хранения в зависимости от внешних факторов (бизнес-требований).

Основным недостатком объектных хранилищ является необходимость иметь N-кратный объем ресурсов (N – количество хранимых копий объектов, соответственно, уровень защиты данных) и осуществлять доступ к данным по объектным протоколам (S3, Rest API). Затраты на избыточный объем возмещаются за счет использования компонентов массового производства (серверы, жесткие диски, коммутационное оборудование), которые значительно дешевле специализированного аппаратного обеспечения, выпускаемого небольшими партиями. Проблема с протоколами доступа к данным стоит более остро. Большинство бизнес-приложений и прикладного ПО на данный момент не имеют какой-либо поддержки объектных протоколов. Доработка или замена используемого ПО за приемлемое время и вменяемые деньги очень часто невозможна. В связи с этим основные SDS-продукты на данный момент имеют отдельный компонент (роль) для предоставления ресурсов по классическим протоколам (iSCSI, NFS, CIFS).

Применение объектных или основанных на них систем хранения по сравнению с классическими или подобными им массивами требуют иной, в большинстве случаев более детальной проработки и оценки возможностей решения. Это связано с совершенно другим подходом к организации инфраструктуры, резервированию данных (РК) и комплекса в целом (Disaster Recovery, DR). Допущенные в этом месте ошибки могут дорого обойтись. Одно из возможных последствий – отсутствие постоянной производительности. В зависимости от используемых алгоритмов распределения и кэширования данных может наступить ситуация, когда будет производиться обращение не к локальным ресурсам, а к другим узлам (членам группы хранения единого набора данных) по внутренней сети – Ethernet, InfiniBand, WAN. На рис. 2 показан пример подобного колебания производительности.

Красная линия отображает время отклика при выполнении операций ввода/вывода. Пиковые значения приходятся на выполнение операций на удаленном узле. Увеличение времени отклика напрямую влияет на производительность операций (чем больше время выполнения, там меньше операций можно выполнить за определённый период). Как видно из примера, задержка на выполнение удаленных операций не постоянна и может быть причиной значительной деградации общей производительности. Чем продолжительнее выполнение операций на удаленном узле, тем больше будет влияние на суммарную производительность.

Для минимизации влияния этой особенности многоузловых SDS на продуктивные среды необходимо проводить предварительную глубокую проработку конфигурации и оценку принципиальной возможности ее применения.

Основные области и решения, в которых началось активное применение технологий SDS:

- тестовые среды и среды разработки;
- системы публичного/корпоративного облачного хранения (Dropbox и др.);
- системы машинной обработки неструктурированных данных (социальные сети, статистическая обработка данных и др.);
- публичный/корпоративный web-хостинг данных;
- хранение резервных и архивных данных;
- общецелевые файловые хранилища (общие файловые ресурсы);
- BLOB-хранилища вторичных данных информационных систем;
- хранилища виртуальных машин.

Программно-определяемые СХД – наиболее гибкие и динамично развивающиеся технологии в группе решений по хранению данных. В них применяются

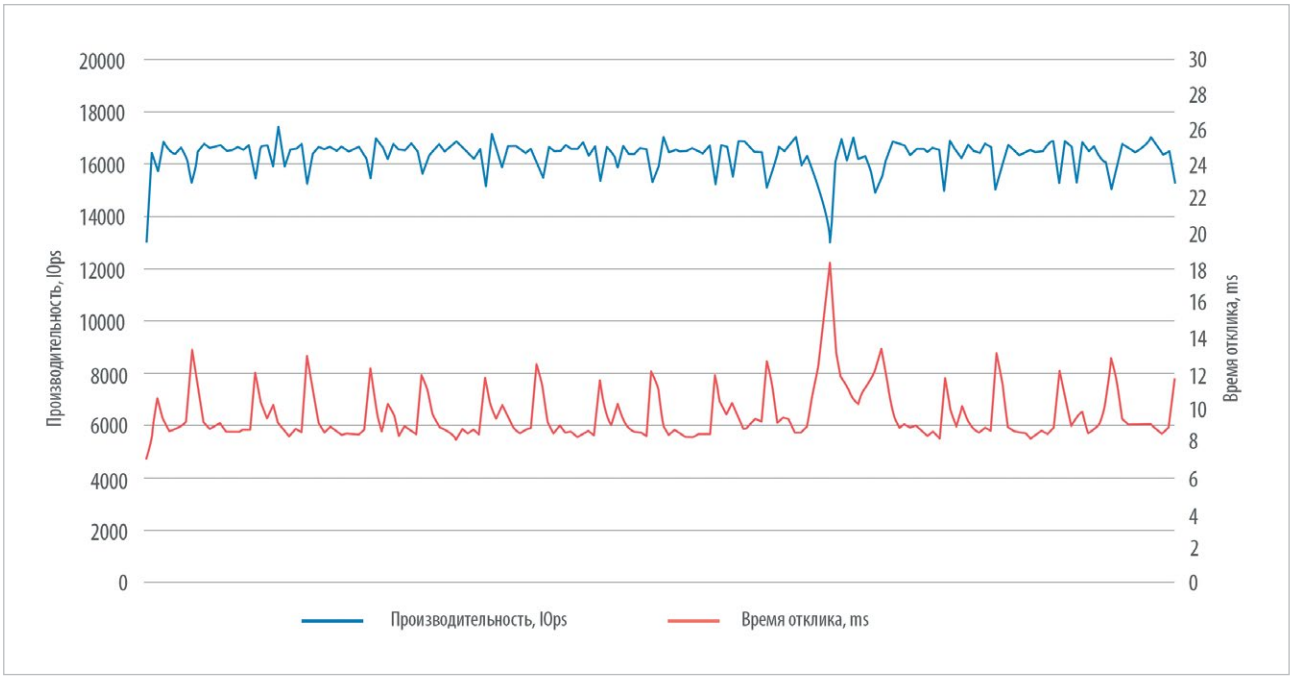


Рис. 2. График возможной многонодовой производительности SDS-решения

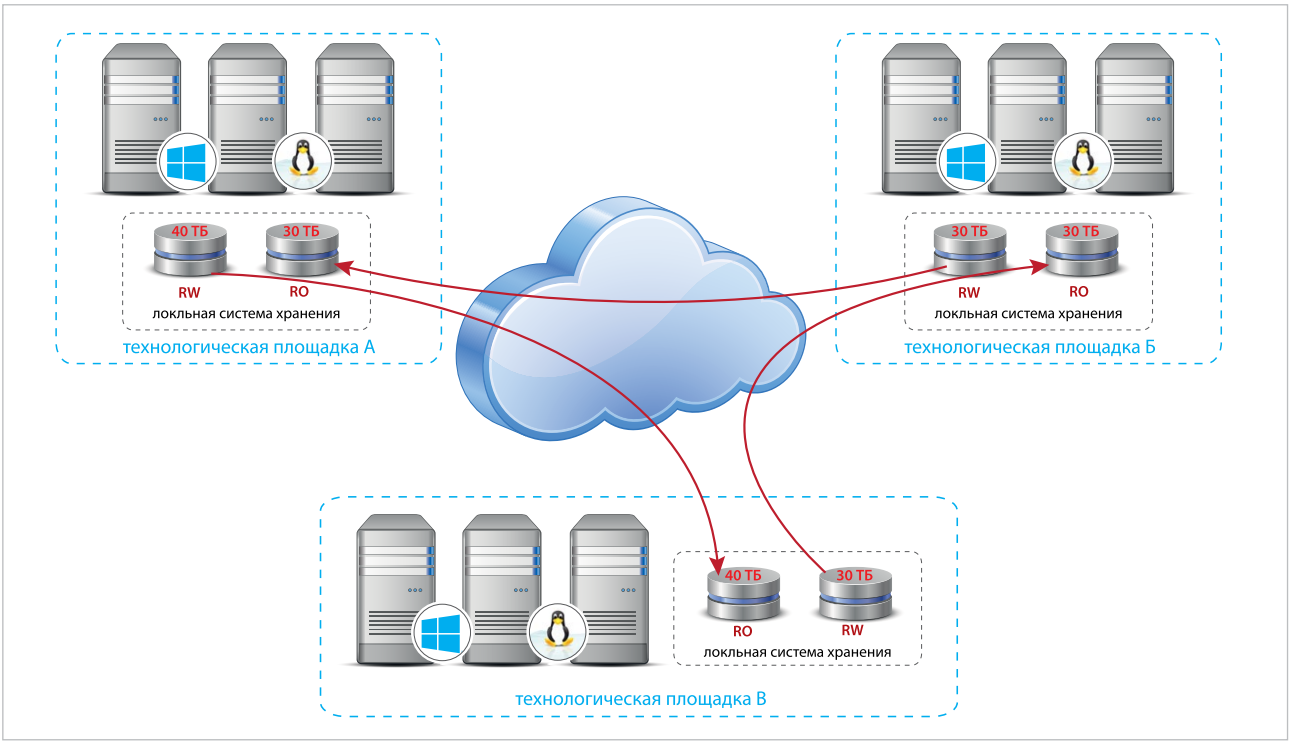


Рис. 3. Обобщенная схема решения с применением классических массивов

уникальные алгоритмы, за счет которых возможно уменьшение количества используемых компонентов и суммарной стоимости решений. В качестве примера рассмотрим задачу по построению ресурса хранения. Компания имеет 3 ЦОДа в пределах одного города, которые соединены IP-каналами связи достаточной пропускной способности. Есть следующие требования к ресурсам хранения:

- ✓ общий объем данных – 100 ТБ;
- ✓ обеспечение одновременного доступа на чтение/запись из 3 ЦОДов;
- ✓ обеспечение отказоустойчивости до уровня потери одного из ЦОДов.

Решение этой задачи с применением классических дисковых массивов в полной мере невозможно. На текущий момент существуют системы, обеспечивающие одновременный доступ (на чтение/запись) только с 2 технологических площадок (например, HDS G1000 GAD) или из всех ЦОДов к единому хранилищу, расположенному в одном из дата-центров и резервируемому в других. Условным решением можно считать организацию ресурсов хранения с делением на сегменты по площадкам и резервированием этих сегментов между ЦОДами. Пример такой реализации представлен на рис. 3.

Подобный подход требует не менее 200 ТБ суммарной полезной емкости для обеспечения хранения и резервирования и ограничивает локальный полный (чтение/запись) доступ объемом локального сегмента. Доступ на запись в удаленные сегменты должен будет производиться через каналы связи между площадками. Эта реализация требует обеспечения работы прикладного ПО с тремя независимыми сегментами данных.

Теперь рассмотрим вариант с использованием SDS-систем с объектным доступом. Возможно построение единого хранилища данных с расположением компонентов (узлов) на 3 площадках. Применение динамических алгоритмов хранения позволяет обеспечить хранение не менее 1 копии на каждой площадке, что гарантирует сохранность данных при потере до 2 из 3 ЦОДов. Этот подход, как и в случае с классическим массивом, требует хранения 3-кратного объема, но использование недорогих компонентов снижает ТСО аппаратной части решения.

В ряде случаев размещение в каждом ЦОДе полного объема требуемого оборудования невозможно (из-за отсутствия места, ресурсов электропитания, охлаждения и т.д.). Выход – применение решения на базе SDS с уникальными (более сложными) алгоритмами распределения данных, например Quantum Lattus. Благодаря ему хранение данных

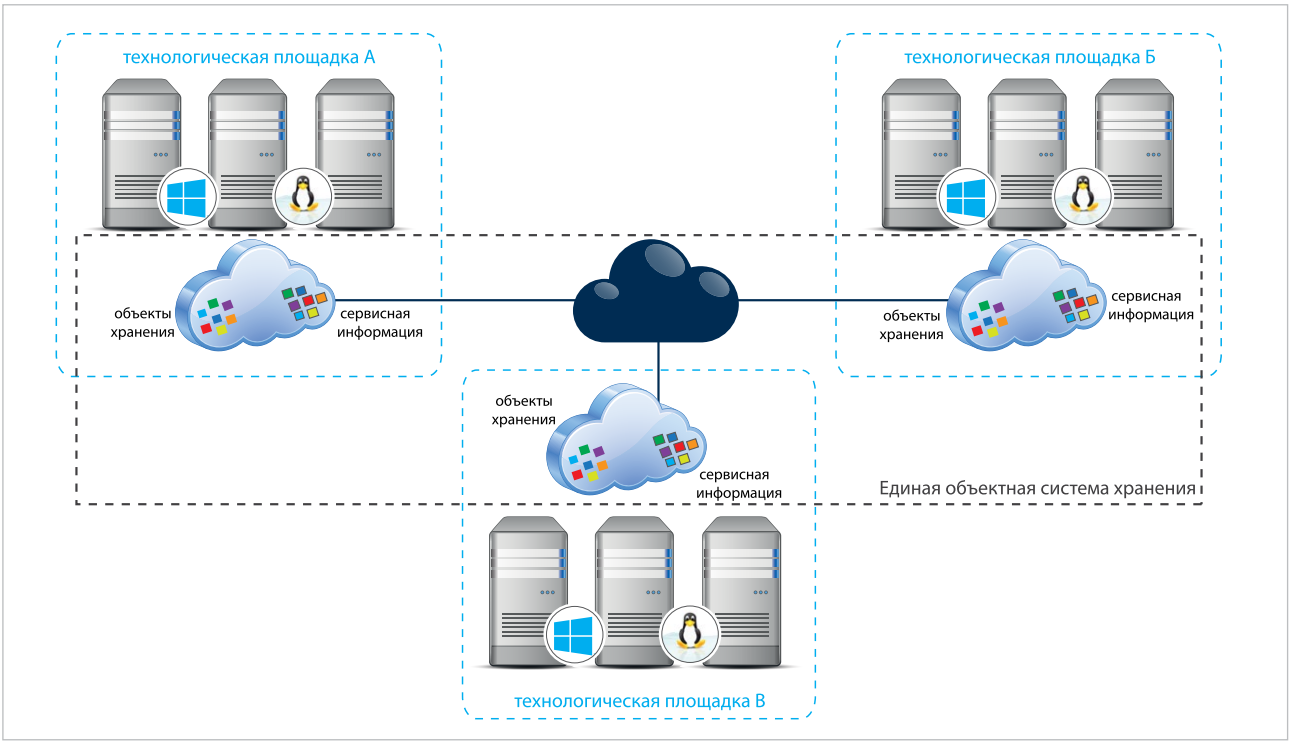


Рис. 3. Обобщенная схема решения с применением классических массивов

производится совместно с хранением дополнительной сервисной информации для их восстановления. Наиболее похожее решение – RAID 5 или 6 с использованием данных четности для восстановления массива. Главным отличием Quantum Lattus от классического RAID является возможность регулирования уровня сервисной информации. Это позволяет задавать требуемый уровень сохранности данных при выходе из строя определенного количества компонентов. К примеру, можно задать потерю всех компонентов одной из технологических площадок, в данном случае требуемый объем хранения для обеспечения 100 ТБ полезной емкости составляет ~164 ТБ.

Решение минимизирует используемую емкость для обеспечения хранения данных, но при этом накладывает более жесткие требования к доступности, пропускной способности межплощадочных каналов связи и набору используемого ПО систем резервного копирования и архивирования данных (требуется наличие возможности работы с объектными системами хранения).

***

Развитие и использование SDS-систем стоит рассматривать как наиболее перспективное направление в индустрии хранения. На данный момент реальное применение SDS ограничено несколькими факторами, но наращивание их функционала и постепенное увеличение стабильности и прогнозируемости работы компонентов со временем позволят рассматривать программно-ориентированные СХД в качестве основных систем хранения для большинства областей.

Остается надеяться, что столкновения в лоб новых программных и классических продуктов не будет, смена решений произойдет плавно или же будет найдена точка равновесия, при котором оба вида займут свои ниши и не будут сильно конкурировать. Мы же сегодня можем занять место в круге защитников той или иной технологии либо наблюдать со стороны, используя для своих задач всё самое «вкусное» от них обеих. JI

> Основным ограничением в использовании объектных SDS-решений является неготовность ПО. Реализация новых функций в крупных программных продуктах в большинстве случаев запаздывает, а зачастую это невозможно архитектурно

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ – ЭТО ПРЕДМЕТ «ТОРГА»

Если обеспечить 100%-ную техническую защищенность бизнеса, он просто не сможет приносить прибыль. Если же не ставить никаких защитных ограничителей при проведении операций или реализации банковских продуктов, мошенники, скорее всего, камня на камне не оставят». В таком ключе проходила наша беседа с **Василием Окулесским, к. т. н., начальником управления информационной безопасности Департамента по обеспечению безопасности Банка Москвы.**

J.I.: Василий Андреевич, какова Ваша оценка текущей ситуации с мошенничеством в банковской сфере?

В.О.: Сейчас мы наблюдаем рост от 30 до 50% по разным видам мошенничества по сравнению с прошлым годом. Изменилась и его видовая структура: в первую очередь идет резкий возврат к мошенничеству с банкоматами. За последний год совокупная банкоматная сеть российских банков выросла на 40%, этот чисто технический фактор стал подспудной причиной роста преступлений. Изменились и сами методы атаки на банкоматы. Появились так называемые «взрывники», причем их отличает высокая скорость «работы» – вся операция по хищению занимает меньше минуты. Вернулись программные средства атаки, находившиеся на пике популярности в 2009 году. Причем наблюдаются принципиально

новые методы: банкоматы атакуют дистанционно, провоцируют перезагрузку, или атака идет непосредственно на исполнительные устройства – на тот же депозитор. Объем ущерба от таких действий существенно превышает потери от других видов мошенничества с банкоматами.

В российской банковской сфере наблюдается устойчивый тренд на развитие функциональности web-банкинга для физических и юридических лиц. Мошенникам новый функционал тоже нравится, прежде всего в плане потенциально открывающихся возможностей для хищения денег. Соответственно, банки просто не могут не вкладываться в повышение безопасности своих интернет-сервисов. Отмечу, что из всех российских банков «просто так» инвестирует в свою ИБ только Тинькофф Банк – для него это единственное средство обеспечить безопасность бизнеса.

Тенденция последних нескольких месяцев – атаки на информационные системы банков. Атакуют непосредственно средство управления корреспондентскими счетами – это позволяет мошенникам одномоментно выводить огромные деньги. Подобные операции требуют от злоумышленников высокой квалификации и серьезной подготовки.

J.I.: То есть объектом атак зачастую является уже не клиент, а сам банк?

B.O.: Да, это связано с несколькими факторами. Во-первых, банки тратят много усилий на защиту своих клиентов, и это действительно работает. Во-вторых, клиенты стали более продвинутыми в ИБ-вопросах. Сейчас формулировка «купил антивирус, поставил на компьютер, но он почему-то не работает» встречается гораздо реже. Клиенты уже знают, что и как нужно ставить, обновлять, каковы юридические последствия от применения лицензионного и нелицензионного ПО и т.д. Люди более подготовлены, их стало труднее атаковать, все это вынуждает мошенников «переходить» на банки.

Отмечу, что сама структура и средства подобных атак принципиально другие. Поэтому необходимо пересмотреть парадигму формирования банковских информационных систем. Безопасники должны подключаться к работе еще на первых этапах жизненного цикла системы, а не на стадии ее сдачи в промышленную эксплуатацию. То есть нужно учитывать все ИБ-вопросы еще при разработке.

Более того, должно измениться само понимание информационной безопасности. Защита информации – это не дискретный процесс «поставили решение, все работает, расслабились», а непрерывная деятельность, своеобразный способ мышления людей, которые разрабатывают системы, работают с конфиденциальными документами и др.

J.I.: Каким именно должно быть это мышление?

B.O.: Приведу простейший пример, касающийся 3 основных составляющих ИБ – конфиденциальности, целостности и доступности данных. В отношении этой триады наблюдается интересный логический парадокс: если понятие, на первый взгляд, кажется простым и ясным, его реализация на практике практически невозможна. Что такое целостность? Простой вопрос. Но вот вы подписываете документ электронной подписью, основное требование при этом – вы должны быть уверены в том, что именно подписываете. То есть должна быть обеспечена целостность изначального объекта подписи и того, что вы видите на экране. Насколько вообще электронный документ в базе данных соответствует бумажному оригиналу? Насколько легитимна воспроизведенная на бумаге подписанная электронная версия? Кто имеет представление о том, что такое Windows, понимает, что озвученное выше требование в принципе не реализуемо. Или нужно отказываться от столь популярной операционной системы и технологии работы в многозадачных режимах, причем изобрести такой способ визуализации электронных документов, который бы

обеспечивал целостность на всех стадиях их преобразования.

Вопрос не так уж и прост, он упирается в технические средства, технологию работы. Если мы не будем решать его на уровне изначальной постановки задачи, то попросту не сможем понять, что именно должны защищать, что для нас является объектом обеспечения ИБ. Не факт, что документ, который мы реально защищаем, соответствует тому, что был на входе и действительно подлежал защите.

J.I.: Какой тип мошенничества наиболее опасен в настоящий момент?

B.O.: Пальма первенства сейчас, как и последние несколько лет, – у внутренних мошенничеств. Их невозможно блокировать системами противодействия. Если сотрудники сговорятся между собой, вам, грубо говоря, ничего не поможет. Выявить внутренних злоумышленников очень трудно, а последствия таких сговоров существенно масштабнее, чем ущерб от какого-либо другого вида мошенничества.

ОТДАТЬ % МОШЕННИКАМ?

J.I.: В чем заключаются основные подходы к обеспечению ИБ в Вашем банке?

B.O.: Мы планомерно усиливаем безопасность наших сервисов. Но фокус внимания в части обеспечения ИБ сместился. Если раньше мы защищали клиента от периодически возникающих угроз – фишинга, возможности подмены его реквизитов, обеспечивали защиту средств аутентификации, то сейчас мы априори считаем, что клиент всегда поражен. 80% клиентов изначально пользуются банковскими сервисами под контролем мошенников. Поэтому парадигма защиты должна быть изменена. Мы предполагаем, что периметр уже достаточно защищен, поэтому переключаем внимание на транзакции. Собственно, одно из наиболее эффективных современных направлений – это анализ транзакций.

J.I.: Возможно, через определенное время банки будут вынуждены признать, что их инфраструктура также является априори уязвимой и управляемой мошенниками на 80%. И значит, единственным выходом будет контроль уже внутрибанковских транзакций с помощью систем, аналогичных решениям для контроля клиентских транзакций.

B.O.: В этом есть доля истины. Я не открою Америку, если скажу, что обеспечение информационной безопасности развивается по спирали, и каждый виток происходит на принципиально другом уровне. 10 лет назад мы говорили практически о том же – нужно защищать внешний периметр банка. За эти годы мы прошли несколько витков защиты клиента и снова вернулись к начальной точке – банку. Только теперь речь идет об изменении самой идеологии построения информационной инфраструктуры для изначального учета ИБ-вопросов.

J.I.: Как известно, бизнес зачастую негативно относится к развитию и ужесточению ИБ. Как Вам удается приводить банк в соответствие современным практикам обеспечения информационной безопасности?

В.О.: Самый эффективный стимул для повышения уровня ИБ в компании – обязательное участие бизнеса в процессе возмещения финансового ущерба от мошенничества. Например, у нас идет разработка нового банковского продукта. Мы посмотрели свою ИБ-триаду, выдали замечания, закрыли видимые нам дыры. Именно видимые нам, поскольку в каждой разработке есть несколько связанных пластов. Уязвимости в пластах мы устраняем, а вот особенности связей между ними гораздо лучше знает команда разработчиков. В документах по продукту, с которыми мы работаем, они не прописываются. В то же время эти связи зачастую и являются объектами атаки. Если разработчики совершенно не заинтересованы в том, чтобы выстроить их правильно с точки зрения ИБ, по выходу продукта мы рискуем ощутить на себе повышенное внимание мошенников. Если же финансовые потери будут коррелировать с конкретными премиями разработчиков и тех бизнес-подразделений, которые инициировали появление продукта, они сами будут стремиться по максимуму «вычистить» его.

Механизм обеспечения ИБ, действующий уже на этапе предложения продукта на рынке, – всем известные stop loss. Как только по нему фиксируются несколько мошеннических операций или сумма ущерба от действий злоумышленников превышает допустимое значение, банк останавливает предложение. Мы анализируем продукт, устраняем узкие места и только потом снова запускаем его в работу. Естественно, для любого бизнеса первостепенна прибыль от оказываемых услуг, поэтому он, скорее, заинтересован в увеличении допустимого числа мошеннических операций или суммы ущерба. По факту это предмет торга между ИБ- и бизнес-подразделениями, наша общая задача – находить компромисс. Мы постепенно выстроили у себя этот подход. «Мы уже знаем – будут stop loss и лимиты, так что давайте совместно работать» – такова позиция бизнеса при внедрении нового продукта. Наш мобильный банкинг – пример того, как ответственно бизнес подходит к вопросам ИБ: изначально он озвучил более жесткие условия аутентификации клиентов на мобильных устройствах, чем предлагали мы.

J.I.: Допустим, нужно максимально быстро вывести на рынок новую услугу, чтобы опередить конкурентов и не потерять потенциальную прибыль. Можете ли вы в этом случае несколько снизить критичность вопроса обеспечения ИБ?

В.О.: «Закрыть глаза» мы в любом случае не можем, просто работаем в таком же напряженном темпе, что и разработчики. Явную шелуху отбиваем сразу, уязвимости, которые мы не успеваем проработать глубоко и детально до выхода продукта, устраняются на этапе stop loss.

Вообще если бизнес выпускает на рынок сырую с точки зрения ИБ услугу, он должен быть готов к тому, чтобы отдать мошенникам определенный процент с каждого заработанного на ней миллиона. Официальный ущерб здесь может составлять и 5, и 50%. Ответственность за риски мошенничества

> Если правильно выстроить систему баланса финансовой ответственности между подразделениями, бизнес-процессы, имеющие высокую фродулентность, автоматически становятся более безопасными

в данном случае целиком будет лежать на бизнес-подразделении, и это должно быть отражено в соответствующем бизнес-соглашении.

Как я уже говорил выше, распределение ответственности действует отрезвляюще. Допустим, вы устанавливаете банкомат в потенциально опасном месте, невзирая на рекомендации ИБ-шников по поводу сигнализации, видеонаблюдения и т.д. Стоимость современного банкомата – около 30 тыс. долларов. Если мошенник ломает его, ремонт может быть отнесен на общебанковский счет, на счет процессинга или же вашего розничного подразделения. В аналогичной ситуации в будущем к ИБ-специалистам прислушаются. Мы говорим с бизнесом на его языке – о потере прибыли, рисках, финансовой ответственности и т.д.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ

J.I.: Не так давно Банк Москвы внедрил систему защиты от мошенничества в каналах ДБО для юридических лиц. Расскажите, какие цели стояли перед проектом? Достигнуты ли они?

В.О.: Наш проект в некотором роде уникален – мы ставили своей целью не повышение уровня безопасности, а снижение стоимости самой процедуры выявления мошенничества. До этого 400 операционисток банка звонками подтверждали каждый новый платеж – их было около 10 тысяч в день. В результате мы уменьшили число контрольных звонков во фронтальных подразделениях при проведении платежей – по отдельным направлениям более чем в 10 раз. Нагрузка на операционисток снизилась, они переключились на продажу банковских продуктов – деятельность, напрямую приносящую прибыль.

Правильная формулировка цели проекта с нашей стороны – «давайте сделаем безопасность дешевле» – привела к тому, что бизнес-подразделение согласилось внедрить антифрод-систему и задействовало для этого свой бюджет.

J.I.: Внедренный аналитический инструмент, по сути, сам принимает решения. Где проходит грань между достаточностью и избыточностью автоматизации? Какие решения нельзя доверить программному мозгу?

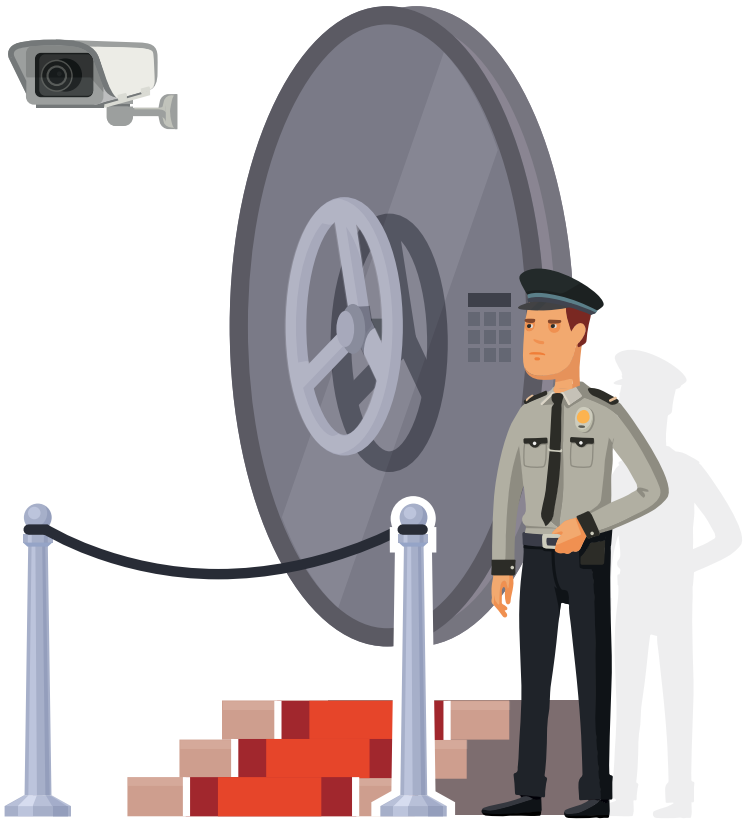
В.О.: Граница все время находится в движении, она располагается между автоматическим проведением и автоматической блокировкой платежа. Если уровень мошенничества, по которому выставлен уровень риска в системе, снизился/повысился, мы корректируем в ней критерии принятия решений. При этом нельзя полностью автоматизировать оценку операций и отдавать весь процесс на откуп аналитическому инструменту. То есть доверие к антифрод-системе есть, но его уровень должен контролироваться. Иногда решение по платежу может принять только человек, у нас это неоднократно подтверждалось. Как сказано в одной пословице, машина – «дура»: она не может предусмотреть все нюансы. Например, технический сбой привел к увеличению времени отклика между системами, в итоге решение не определилось с ответом. У нас в штате есть обученные специалисты, которые порой могут сработать быстрее, чем антифрод-решение. Поэтому в нашем случае мы говорим об автоматизированной системе, а не об автоматической. Так что мы доверяем, но проверяем.

> Наш бизнес пришел к пониманию, что, с одной стороны, безопасность стоит денег, а с другой – без нее денег будет гораздо меньше

«Штучный товар»

J.I.: Внедрение и эксплуатация сложной системы контроля рисков – это большой труд банковской команды. Какими компетенциями должны обладать сотрудники, призванные обеспечивать эксплуатацию подобных решений? Существует ли дефицит таких кадров?

В.О.: Отвечу вопросом на вопрос: сколько оттенков красного может увидеть среднестатистический человек? Сложно сказать. А в нашей работе это как



раз самое важное – уметь различать максимальное количество «оттенков» рисковых операций в системе. Специалист должен уметь выявлять признаки возможного мошенничества, в том числе с помощью профессиональной интуиции. Это приходит исключительно с опытом. В нашей области работают люди с разным изначальным багажом знаний.
У одних – ИТ-шников – хороший бэкграунд по системному анализу больших объемов данных, но они никогда не работали с мошенническими операциями. Другие – «опера» – собаку съели на оценке операций, они мыслят в терминах IP-адресов, логов, но при этом не представляют себе принципы организации баз данных, не знают, как проводить системный анализ. Обмен опытом, совместная командная работа таких экспертов дают синергетический эффект. Крайне важно иметь грамотного руководителя подразделения по борьбе с фродом, который выстроит весь процесс, правильно расставит акценты. Резюмируя все вышесказанное: подготовленные, обученные специалисты в нашей области – «штучный товар».

J.I.: Вы уже частично затронули вопрос взаимодействия ИБ-службы с бизнес-подразделениями. Какой Вы себе представляете оптимальную структуру функции противодействия мошенничеству?

В.О.: Самое главное – взаимодействие ИБ и бизнеса должно быть описано в формате бизнес-процесса. Причем все его участники должны четко понимать, что нужно делать в случае инцидента, – детально представлять себе порядок реагирования. Для этого в Банке Москвы существует положение о порядке взаимодействия. При описании бизнес-процесса нужно разделить зоны и меру (не исключено, что и материальную) ответственности каждой группы участников. Вспоминается «Про Федота-стрельца, удалого молодца» Леонида Филатова: «Сознаю свою вину. Меру. Степень. Глубину».

> Подчеркну, что сегодня должно измениться само понимание информационной безопасности. Защита информации – это не дискретный процесс «поставили решение, все работает, расслабились», а непрерывная деятельность, своеобразный способ мышления людей, которые разрабатывают системы, работают с конфиденциальными документами и др.

В нашем Департаменте по обеспечению безопасности есть внутренние документы, описывающие, что, куда, в какой форме и как быстро ИБ-специалисты должны передавать при инциденте. Счет зачастую идет на минуты, поэтому сидеть и размышлять о том, что нужно сделать и кто виноват, недопустимо. У сотрудника должен срабатывать четкий алгоритм действий «раз-два-три». При этом у него под рукой все шаблоны документов, которые нужно отправить, актуальные списки электронных адресов. То есть нужно наладить процесс и тренировать людей.

J.I.: Как можно оценить экономическую эффективность работы подразделений, чьи функции связаны с борьбой с мошенничеством?

В.О.: Никак. Нашу экономическую эффективность невозможно измерить. Например, в этом месяце мы выявили больше случаев мошенничества, чем в прошлом. О чем это говорит? Мы стали лучше работать? Или мошенники взяли ударные темпы «производства»? ИБ-подразделение может оценивать свою деятельность только с точки зрения процентного соотношения отработанных и выявленных инцидентов. Грубо говоря, если у нас отработаны все выявленные факты мошенничества, мы эффективны.
Но в любом случае остается слепое пятно – невозможно узнать, всё мы вычислили или нет.

Как ни парадоксально, бизнес может оценить эффективность нашей работы исключительно по потерям. Ущерб от мошенничества есть? Есть – прогнозируемый, попадающий в рамки планируемых потерь. Значит, баланс, о котором мы говорили выше, соблюден, безопасность работает хорошо. Если уровень ущерба выше допустимого, значит, где-то «дыра». Причем не факт, что это недоработка в ландшафте информационной безопасности. Возможно, один из бизнес-процессов требует детального пересмотра для повышения уровня ИБ. И над этим мы будем работать совместно с командой экспертов из других подразделений банка.

J.I.: Большое спасибо, что нашли время для беседы!

ПРОГРАММНО-ОПРЕДЕЛЯЕМЫЕ ЦОД – БОРЬБА ЗА БУДУЩЕЕ

Что из себя представляют технологии, которые, возможно, вскоре нам всем придется внедрять? Можно ли полноценно использовать программно-определяемый ЦОД, не изменяя работающих в нем прикладных систем? Эксперты компании «Инфосистемы Джет» отвечают на эти и многие другие вопросы.

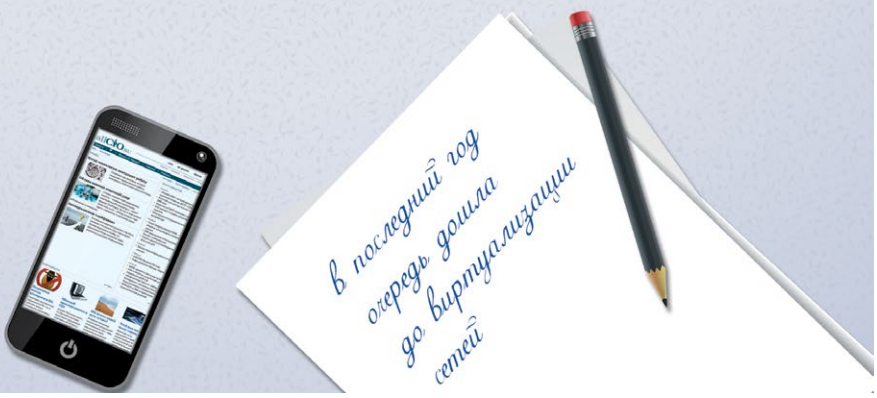
Источник: Jet Info № 11, 2014, www.jetinfo.ru

ГДЕ И КАК ХРАНИТЬ ДАННЫЕ?

АВТОР: РОМАН ВОЛОДИН

Как повысить эффективность хранения корпоративных данных, сэкономив бюджет на ИТ? Какие перспективы у облачного хранения? Современные Full-flash массивы и привычные жесткие диски – как найти баланс? На эти другие актуальные вопросы ответил **начальник отдела СХД компании «Инфосистемы Джет» Роман Володин.**

Источник: AllCIO.ru, октябрь 2014 г.



Jet Info
ИЗДАЕТСЯ КОМПАНИЕЙ «ИНФОСИСТЕМЫ ДЖЕТ»

Главный редактор Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1,
тел. (495) 411 76 01, факс (495) 411 76 02, e-mail: Jetinfo@jet.msk.su, www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем