ChannelForIT Review

АПРЕЛЬ 2015

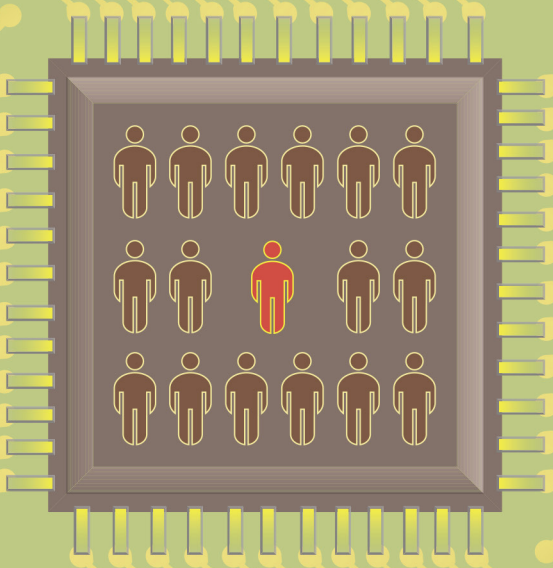
Украина. ЦОДы. Рыночные тренды

Современный ЦОД – ключ к успеху

Инновации ЦОД. Обещания vs реальность

Все будет флэш!

2015



ЦОД

Организация связности в распределенном ЦОДе с помощью оптических технологий

Мониторинг инфраструктуры ЦОДа

Виртуализация хранения данных

Channel for IT

http://channel4it.com

ChannelForIT Review

СТАТЬЯ НОМЕРА

5 УКРАИНА. ЦОДы. РЫНОЧНЫЕ ТРЕНДЫ

Олег Пилипенко

Как будет развиваться рынок ЦОДов в 2015 году? Можно ли ожидать дальнейшего строительства ЦОДов или основная активность будет направлена на модернизацию и поддержку уже существующих объектов? Будут ли и далее развиваться коммерческие ЦОДы? Какие основные технологические тенденции играют важную роль в развитии бизнеса ЦОДов в Украине и мире в ближайшие годы? Об этом мы решили спросить экспертов отечественного ИТ-рынка.

8 СОВРЕМЕННЫЙ ЦОД - КЛЮЧ К УСПЕХУ

По материалам Rittal

В настоящее время многие руководители предприятий задаются вопросом: какие ИТ-стратегии применить, чтобы планомерно поддерживать свою оперативную деятельность с помощью ИТ-решений и, в то же время, сдерживать затраты на ИТ-инфраструктуру?

11 ОРГАНИЗАЦИЯ СВЯЗНОСТИ В РАСПРЕДЕЛЕННОМ ЦОДе С ИСПОЛЬЗОВАНИЕМ ОПТИЧЕСКИХ ТЕХНОЛОГИЙ

Максим Калинкевич, Cisco

При создании распределенных ЦОДов одним из самых главных требований является обеспечение низкой задержки и высоких показателей надежности при передаче данных между площадками ЦОДа.

13 ВИРТУАЛИЗАЦИЯ ХРАНЕНИЯ ДАННЫХ

По материалам DataCore Software

Виртуализация хранения данных в настоящее время является одной из наиболее актуальных тем в сфере построения и модернизации ЦОДов. На рынке постоянно появляются решения, расширяющие привычный функционал СХД. Одним из поставщиков таких решений является компания DataCore, предлагающая решения класса SDS и ESV.

16 ИННОВАЦИИ ЦОД. ОБЕЩАНИЯ VS РЕАЛЬНОСТЬ

Олег Пилипенко

Новые технологии для построения и оптимизации ЦОДов появляются регулярно. Некоторые приживаются очень быстро, другие — медленно и сложно. Если отложить в сторону решения для инженерной инфраструктуры, то в последние годы четко доминируют две актуальные технологии: конвергентные инфраструктуры и программно-конфигурируемые системы. К последним относится целый спектр различных устройств и компонентов ЦОДа. Но насколько эти инновации актуальны для украинского ИТ-сектора? Об этом мы спросили экспертов.

18 ВСЕ БУДЕТ ФЛЭШ!

Ян Шмиголь

Флэш-технологии производят революцию в технологиях хранения и обеспечивают прирост производительности практически для любых приложений. Об основных тенденциях в области корпоративных систем хранения данных, важности своевременного внедрения инноваций и перспективах развития рынка издание ChannelForIT Review беседует с Владимиром Бондаренко.

22 АРХИТЕКТУРА METAFABRIC КОМПАНИИ JUNIPER NETWORKS

По материалам компании ITbiz Solutions

На сегодняшний день облачная среда, мобильность и большие объемы данных являются ос-

новными движущими силами преобразований в сфере ИТ. Предприятия и поставщики услуг во всех отраслях постоянно ищут способы получения конкурентных преимуществ, и роль ЦОДов и приложений в этом поиске сейчас велика, как никогда.

25 ЧТО ВАМ ДАСТ ВНЕДРЕНИЕ DLP?

Олег Пивовар, SVIT IT

В нашем предыдущем выпуске, посвященном ИТ-безопасности, мы уже писали о DLP-системах. Мы решили вернуться к этой теме, так как в последнее время на украинском ИТ-рынке, несмотря на спад активности в целом, значительно вырос спрос на DLP. Сегодня мы поговорим о том, какие реальные преимущества может дать такое внедрение компании, которой необходимо защищать свои информационные активы.

27 СИСТЕМЫ МОНИТОРИНГА ИНФРАСТРУКТУРЫ ЦОДа

Олег Иванин

ЦОД сегодняшнего дня – это сложный комплекс взаимосвязанных подсистем, каждая из которых должна не только гармонично взаимодействовать с остальными элементами инфраструктуры, но и быть надежной, отказоустойчивой и контролируемой. Для этого разработчики снабжают ЦОДы системами мониторинга технических параметров инфраструктуры.

35 БЕЗОПАСНОСТЬ ТРАДИЦИОННЫХ И ВИРТУАЛИЗИРОВАННЫХ ЦОДов С БРАНДМАУЭРАМИ НОВОГО ПОКОЛЕНИЯ

По материалам Группы компаний БАКОТЕК

Виртуализация помогает компаниям использовать аппаратную инфраструктуру ЦОДа более эффективно, что позволяет достигнуть снижения затрат и улучшения операционной эффективности. В большинстве случаев инициативы виртуализации берут свое начало изнутри, в собственной аппаратной и сетевой инфраструктуре, дополненной инструментами, такими как VMware или KVM и OpenStack для управления виртуализированной средой.

ChannelForIT Review

ОСНОВАТЕЛЬ И ИЗДАТЕЛЬ
ООО «ЭЙ ЭМ СИ УКРАИНА»

РЕДАКЦИЯ

Главный редактор
Олег Пилипенко

Редакторы
Иван Карповцев
Владимир Смирнов

Реклама и маркетинг
Олег Николаев
marketing@channel4it.com

Дизайн
Ольга Лукьянова
service@channel4it.com

Рукописи не рецензируются и не возвращаются.

Channel for IT

e-mail: publisher@channel4it.com
тел.: +38 (044) 384 09 96

О ChannelForIT:

Интернет-ресурс ChannelForIT предназначен для профессионалов в области корпоративных информационных технологий: ИТ-директоров, технических директоров, специалистов и экспертов в области информационных технологий, ИБ.

ChannelForIT публикует экспертные и аналитические материалы, интервью с экспертами отрасли, новости, информацию о вакансиях и мероприятиях в ИТ-отрасли.

Уважаемые дамы и господа, коллеги!

Предлагаем вашему вниманию новый выпуск электронного журнала ChannelForIT Review. Благодарим вас за внимание к нашему проекту.

Этот выпуск посвящен вопросам построения и модернизации Центров Обработки Данных. Тема актуальная, несмотря на непростую политическую и экономическую ситуацию. Многие компании успели обзавестись ЦОДами в минувшие годы и сталкиваются с задачами модернизации инфраструктуры, в частности, повышения энергоэффективности. Другие раздумывают о том, можно ли доверить свою информацию коммерческому ЦОДу. Третьи планируют реализовать гибридную модель эксплуатации своего ЦОДа в комбинации с коммерческим. И всем будет полезно узнать о новейших трендах в этой области, многие из которых обещают изменить и уже меняют знакомый всем специалистам облик ЦОДа — им посвящен целый ряд материалов выпуска. Также мы традиционно опросили экспертов, которые поделились с нами своим мнением о перспективах рынка и технологических трендах. Приятного и познавательного чтения!

До встречи в следующем выпуске ChannelForIT Review.

Ян Шмиголь

Издатель
ChannelForIT Review

УКРАИНА. ЦОДы. РЫНОЧНЫЕ ТРЕНДЫ

Олег Пилипенко

Согласно отчету DCD Intelligence, в 2014 году объем инвестиций в построение новых ЦОДов в Северной Америке возрос на 15%, а занимаемая ими площадь увеличилась на 3,5%. Кроме того, активный процесс построения новых ЦОДов сегодня отмечается в Азиатском регионе, вызванный, в первую очередь, бурным ростом числа интернет-пользователей.

Но в Украине ранее быстрый рост числа пользователей интернета замедлился. Так, на конец 2013 года украинская интернет-аудитория составила 17,5 млн человек (49,8% взрослого населения Украины), что на 1,5 млн больше, чем годом ранее. Согласно прогнозам, число пользователей интернета в 2014 году должно было достигнуть 20 млн, однако экономический кризис, война на Востоке и аннексия Крыма оказали негативное влияние на развитие рынка интернет-провайдеров, равно как и на развитие рынка ЦОДов.

Как будет развиваться рынок ЦОДов в 2015 году? Можно ли ожидать дальнейшего строительства ЦОДов, или основная активность будет направлена на модернизацию и поддержку уже существующих объектов? Будут ли и далее развиваться коммерческие ЦОДы? Какие основные технологические тенденции играют важную роль в развитии бизнеса ЦОДов в Украине и мире в ближайшие годы? Об этом мы решили спросить экспертов отечественного ИТ-рынка.

ВМЕСТО РАЗВИТИЯ — ЭКОНОМИЯ НА ВСЕМ

В нынешних экономических условиях особого прогресса на отечественном рынке центров обработки данных ждать не приходится — в этом были солидарны все опрошенные нами эксперты. Очевидно, что в 2015 году основной упор будет сделан на увеличение утилизации уже построенных корпоративных и коммерческих ЦОДов, а основная активность — направлена на модернизацию и поддержку уже существующих ЦОДов.

По мнению Юрия Ярощука, начальника отдела технологий ЦОД в «ЭС ЭНД ТИ УКРАИНА», объем рынка ЦОДов в Украине по-прежнему большой, однако не стоит ожидать каких-либо серьезных проектов на ближайший год. Крупные участники рынка направят свои усилия на оптимизацию существующих мощностей и не будут закладывать существенных вливаний в новые проекты.

С ним согласна и Ирина Бернацкая, системный консультант Dell: «На украинском рынке достаточно места для дальнейшего увеличения числа корпоративных и коммерческих ЦОДов. Украина — страна с развивающейся экономикой, один из европейских лидеров ИТ-аутсорсинга. Если бы не кризисная ситуация — в 2015 году нас бы ждал существенный рост».

Геннадий Карпов, директор по технологиям De Novo, более категоричен: «В нынешних условиях давать какие-либо прогнозы не то что на год, а даже на квартал – занятие в высшей степени неблагодарное. Тем не менее, с большой вероятностью можно утверждать, что 2015 г. для бизнеса можно будет охарактеризовать одним словом — «выживание». Понятно, что в таких условиях о сколь-либо заметной инвестиционной активности речь идти не может». С его точки зрения, потребности в ресурсах ЦОДов будут минимизированы и удовлетворены либо за счет уже существующих собственных ресурсов, либо, при отсутствии таковых, за счет ресурсов действующих операторов коммерческих ЦОДов. Заметного потенциала для роста количества корпоративных и коммерческих ЦОДов в 2015 г. нет.

КОРПОРАТИВНЫЕ ЦОДы БУДУТ ВЫТЕСНЯТЬСЯ КОММЕРЧЕСКИМИ

Еще около 10 лет назад в Украине не было полноценных коммерческих центров обра-

ботки данных, предназначенных для размещения корпоративных ресурсов предприятия. Но после 2009 года целый ряд операторов объявил об открытии новых коммерческих ЦОДов. Первоначально рынок отнесся к новой услуге настороженно, однако затем бизнес начал массово размещать свои вычислительные мощности в коммерческих ЦОДах. Как будут развиваться события далее: миграция в коммерческие ЦОДы продолжится или же корпоративные ЦОДы смогут удержать свои позиции?

По всей видимости, будущее — за гибридной моделью, полагает Геннадий Карпов из De Novo. Украина пройдет по пути более развитых стран. Дело в том, что коммерциализация ИТ сопровождается постепенным сокращением производства ИТ-сервисов в «домашних» условиях и появлением профессиональных операторов ЦОДов и облаков, способных предоставлять эти сервисы с более высоким качеством и за меньшие деньги. Содержание собственных ИТ-ресурсов останется уделом только крупных корпораций и компаний с «параноидальными» корпоративными политиками безопасности. Но даже в этих случаях высокое качество и умеренная стоимость услуг операторов ЦОДов и облачных услуг приведет, скорее всего, к формированию гибридных моделей в виде комбинации внешних и внутренних ИТ-ресурсов. Таким образом, в перспективе 3-5 лет гибридная модель станет доминирующим способом обеспечения ИТ-сервисов в корпоративном сегменте.

В Украине сегодня около 30 коммерческих ЦОД, заполняемость которых составляет 65-70%

Примечательно, что об этом же свидетельствуют и исследования компании Cisco: именно гибридный подход дает максимальную гибкость и низкую общую стоимость владения. Притом в Cisco отмечают рост перехода рабочих нагрузок в коммерческие ЦОДы как на уровне хостинга, так и миграции в облачные среды.

Борис Калачев, руководитель отдела сетевых решений компании Инком, указывает, что в Украине на сегодняшний день насчитывается около 30 коммерческих ЦОДов, заполняемость которых составляет 65-70%. Последние два-три года наиболее распространенными являются услуги IaaS и SaaS, ежегодно прибавляющие в росте на уровне 5-10% (в юнитах). Основным «потребителем» таких услуг выступает крупный корпоративный бизнес.

Учитывая мировую динамику, украинский рынок будет продолжать развиваться, особенно в направлении услуг «…As A Service». С другой стороны, украинский рынок пока отстает от европейского на 6-8 лет, а сегодняшняя сложная ситуация, скорее всего, еще более замедлит рост рынка. Но затем, очевидно, последует активная фаза роста.

Во всем мире государственный и промышленный секторы уже давно пользуются услугами коммерческих ЦОДов. Поэтому корпоративные ЦОДы со временем будут вытесняться коммерческими, а собственными ЦОДами будут владеть только очень крупные компании, и то — в гибридной модели. Однако быстрого изменения ситуации на рынке пока ожидать не приходится.

ЭНЕРГОЭФФЕКТИВНОСТЬ ЦОДа: АКТУАЛЬНО ЛИ ЭТО ДЛЯ УКРАИНЫ?

С 1 марта 2015 года НКРЭКУ ввела новые розничные тарифы для потребителей электрической энергии. Очевидно, это не последнее повышение, а значит владельцы ЦОДов должны позаботиться о повышении его энергоэффективности. Но как показал опрос, реализовать такую задачу очень непросто.

По словам Геннадия Карпова из De Novo, на украинском рынке за словами «энергоэффективность ЦОДа» стоит гораздо больше спекуляций, чем реальных технических решений. Как это ни удивительно, но буквально единичные датацентры измеряют свой реальный коэффициент энергоэффективности (PUE).

Коммерческий ЦОД De Novo — один из немногих, где используется промышленная система управления производственным процессом (SCADA), которая позволяет не только контролировать PUE в реальном времени, но и дает всю необходимую информацию для анализа трендов и управления энергоэффективностью ЦОДа (например, выбор режимов free cooling, идентификация и устранение источников потерь). Такая забота об энергоэффективности не удивительна — при текущей нагрузке ЦОДа годовой платеж De Novo за электроэнергию составляет более 12 млн гривен.

Юрий Ярощук из «ЭС ЭНД ТИ УКРАИНА» также придерживается мнения, что, несмотря на растущие цены на энергоносители, немногие украинские компании уделяют должное внимание энергоэффективности. Зачастую затраты на электропитание и теплоотвод не относятся к ключевым факторам, влияющим на принятие решения по внедрению того или иного проекта.

В будущем, учитывая рост цен на энергоносители и тотальную экономию, отечественные предприятия начнут задумываться о такой проблеме и уже в следующем году можно будет увидеть иное положение дел.

ГОНКА «ЦИФР» ТРЕБУЕТ ОПТИМИЗАЦИИ РЕСУРСОВ ЦОДа

Информация, связанная с бизнесом, начиная с данных об объемах продаж до бухгалтерских записей, всегда играла решающую роль для компании. Теперь всеобъемлющий интернет охватывает даже более ценные данные. Миллиарды датчиков, интеллектуальные устройства, социальные сети и видеокамеры генерируют новые «большие данные» (BigData) с ошеломляющей скоростью.

В мире до сих пор идет гонка «цифр», отмечает Юрий Ярощук. Повышение качества аудио и видео влечет за собой увеличение объема передаваемых данных. Вместе с этим стоит отметить колоссальный рост объема хранимой информации. Данная тенденция сохранится в ближайшее время как в мире, так и на нашем рынке.

Росту объема передаваемых данных будет способствовать и внедрение долгожданной связи 3G в Украине. Компаниям необходимо будет переориентироваться на новые продукты. Пользователи в свою очередь будут чаще обращаться к онлайн-сервисам и сервисам потоковой передачи контента. В связи с этим операторы ЦОДов будут вынуждены наращивать каналы связи и оптимизировать стоимость хранения информации. C4IT

Oracle представил новые Ethernet-коммутаторы и сервисы виртуальных сетей для программно-конфигурируемых ЦОД

Корпорация Oracle представила новые высокопроизводительные и недорогие коммутаторы Ethernet 10Gb/40Gb и включила сервисы виртуальных сетей в Oracle SDN для удовлетворения двух основных сетевых потребностей современных облачных ЦОДов. Коммутаторы Oracle Ethernet Switch ES2-72 и Oracle Ethernet Switch ES2-64 созданы для максимально эффективного использования возможностей оптимизированных программно-аппаратных комплексов, серверов и систем хранения Oracle.

Новые недорогие компактные Ethernet-коммутаторы Oracle позволяют сократить существующие многоуровневые сетевые топологии, упрощая ИТ-инфраструктуру и уменьшая затраты за счет меньшего количества кабелей и упрощенного управления. При совместном развертывании с системами Oracle эти коммутаторы обеспечивают экономию благодаря возможности использования уже существующей кабельной инфраструктуры и единому управлению. Данные коммутаторы могут быть приобретены отдельно.

Oracle также добавила новые сервисы виртуальных сетей в Oracle SDN, практически исключив потребность в специализированных сетевых устройствах, которые не обеспечивают масштабируемость и гибкость. Oracle SDN динамически соединяет любую виртуальную машину с любым ресурсом и обеспечивает ускоренное развертывание мультиарендных сред с использованием частных виртуальных соединений, обеспечивая пропускную способность между серверами до 80 Гбит/с для радикального повышения производительности приложений. Одна сетевая инфраструктура соединяет до 1 000 серверов и до 16 000 частных виртуальных подключений.

Благодаря включению новых сервисов виртуальных сетей Oracle SDN теперь распространяется на весь ЦОД и предлагает уникальную возможность объединения сетевых архитектур InfiniBand и Ethernet, обеспечивая управление всей сетевой инфраструктурой с использованием единого интерфейса.

Oracle SDN поддерживает серверы SPARC и x86, Netra Modular System, а также оптимизированные программно-аппаратные комплексы, такие как Oracle Virtual Compute Appliance. C4IT

СОВРЕМЕННЫЙ ЦОД – КЛЮЧ К УСПЕХУ

По материалам Rittal

Высокоэффективные ИТ-системы рассматриваются сегодня как один из центральных факторов производства на предприятиях различных отраслей. Знание рынков, более быстрая реакция на запросы клиентов, превосходная послепродажная поддержка и гибко адаптируемые ИТ-решения — вот типичные примеры сегодняшних бизнес-потребностей. Поэтому становится очевидной необходимость привести свои центры обработки данных в соответствие современному уровню развития технологий, чтобы обеспечить себе уверенность в будущем. Однако насколько ЦОДы современны и энергоэффективны на самом деле? Часто эффективность энергопотребления в ЦОДах совсем не соответствует текущему уровню развития технологий. Предприятия из-за этого теряют деньги.

В настоящее время многие руководители предприятий задаются вопросом: какие ИТ-стратегии применить, чтобы планомерно поддерживать свою оперативную деятельность с помощью ИТ-решений и в то же время сдерживать затраты на ИТ-инфраструктуру?

За последние три-пять лет за счет виртуализации значительно усовершенствовались технологии в таких областях, как энергосберегающие процессоры и оптимальное использование ресурсов. Предприятия сталкиваются с проблемой: существующие ИТ-компоненты не так-то просто заменить новыми системами, поскольку инфраструктура центра обработки данных устарела и не поддерживает высокую энергетическую плотность новых серверов. Поэтому, если вы хотите внедрить в ЦОДе современные ИТ-системы, у вас должна быть возможность гибко адаптировать оборудование для энергоснабжения и контроля микроклимата. А на многих предприятиях установки уже не отвечают современному уровню развития технологий. Это закономерно порождает трудности: старые кабели передачи данных не справляются с сегодняшним объемом сетевого трафика, системы охлаждения устаревают, применяемые концепции резервирования часто тоже устарели и недостаточно надежны для того, чтобы обеспечивать высокую степень готовности, которой ожидают клиенты в современных условиях высокой рыночной конкуренции.

Предприятия охотно удовлетворили бы свои потребности за счет мощностей, предоставляемых общедоступными и гибридными облачными средами. Однако многих пугают риски технических сбоев и информационного шпионажа. Поэтому на первый план, так или иначе, выходят локальные ЦОДы, которыми предприятия управляют сами и в которых, например, можно развернуть частное облако. Но, поскольку ЦОДы нередко довольно стары, перед многими предприятиями встает необходимость основательно модернизировать их инфраструктуру в среднесрочной перспективе.

Проектирование и строительство ЦОДа с нуля может длиться несколько лет и поэтому представляет собой серьезную альтернативу неотложным модернизационным проектам лишь для малой части средних предприятий. И когда речь идет о том, чтобы в кратчайший срок развернуть новую ИТ-инфраструктуру, на помощь приходит экономичный и быстрый вариант модульных ЦОДов.

Что такое модульный ЦОД, мы попробуем объяснить на примере решения RiMatrix S от Rittal. Это стандартизированное модульное решение электропитания и охлаждения для построения ЦОДов, а проще говоря – это полнофункциональный мобильный ЦОД, который может быть установлен на любом свободном пространстве. Его можно использовать как самостоятельную внешнюю структуру в виде контейнера либо установить в существующем центре обработки данных или любом помещении.

С помощью данного решения удовлетворяется потребность предприятий в большей гибкости и адаптируемости. Например, он позволяет

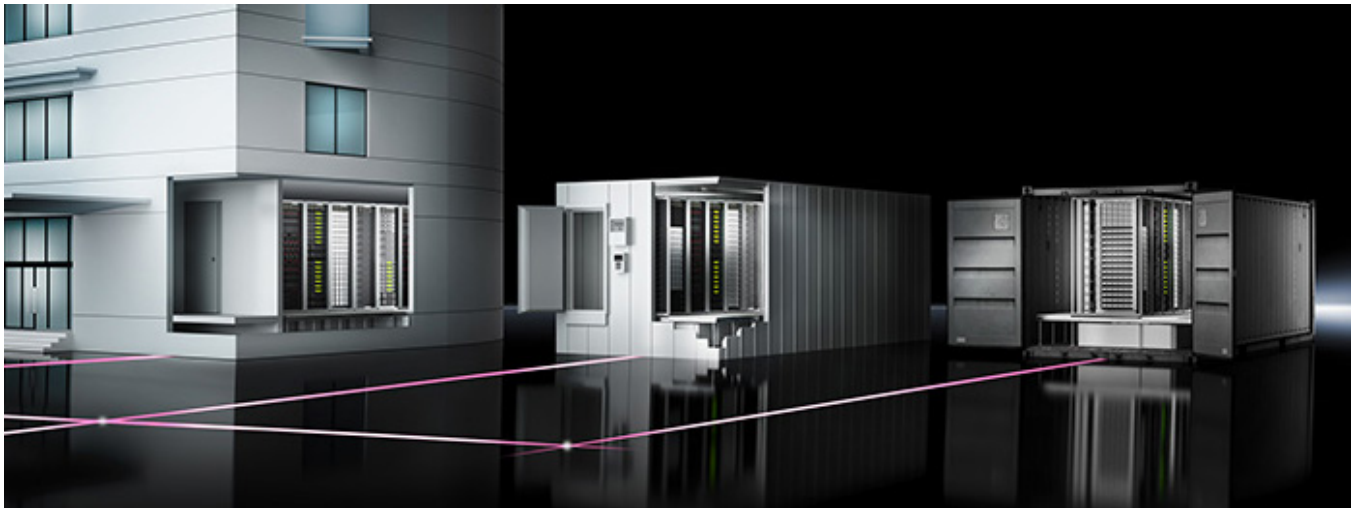


Рис. 1. Модульный центр обработки данных, Rittal RiMatrix S

быстро реализовать такие задачи, как сокращение цикла разработки продуктов, ввод в эксплуатацию новых систем или применение новых правил.

Базовая версия модульного ЦОДа RiMatrix S уже оснащена встроенной системой распределения энергии, кабельными переборками, системой доступа, а также эффективной системой контроля микроклимата. Последняя поставляется с мощностью охлаждения до 180 кВт и резервированием по схеме n+1 или n+2. Классы мощности на 7 и 10 кВт, что соответствует потребностям 90% ЦОДов. Его можно оснастить экономичным и экологически чистым прямым естественным охлаждением, при котором отфильтрованный внешний воздух используется для охлаждения ЦОДа. Агрегат работает в трех режимах: летний, зимний и смешанный, что позволяет значительно сэкономить на эксплуатационных расходах по сравнению с обычными решениями по контролю микроклимата.

Отличительной особенностью RiMatrix S от Rittal является нижнее расположение системы воздушно-водяного охлаждения. Теплообменник и системы трубопроводов размещаются непосредственно под серверными стойками TS IT, что обеспечивает экономию площадей. Для этого используется пространство под фальшполом высотой 50 см. В расположенных рядом со стойками плитах фальшпола монтируются мощные резервируемые вентиляторы с регулируемой скоростью вращения. В сочетании с закрытым горячим коридором они обеспечивают надежное охлаждение серверного и сетевого оборудования даже в верхней части стойки. Одна из стоек выделяется под системы электроснабжения, к которым подводятся два раздельных ввода электропитания. Всего в RiMatrix S насчитывается шесть или девять стоек, причем в шестистоечной версии стойка электропитания содержит и ИБП, который при отказе электросети поддерживает работу оборудования в течение 9 мин. Стойки не имеют дверей и боковых панелей, что способствует лучшему охлаждению. Вся система подключается к внешнему чиллеру.

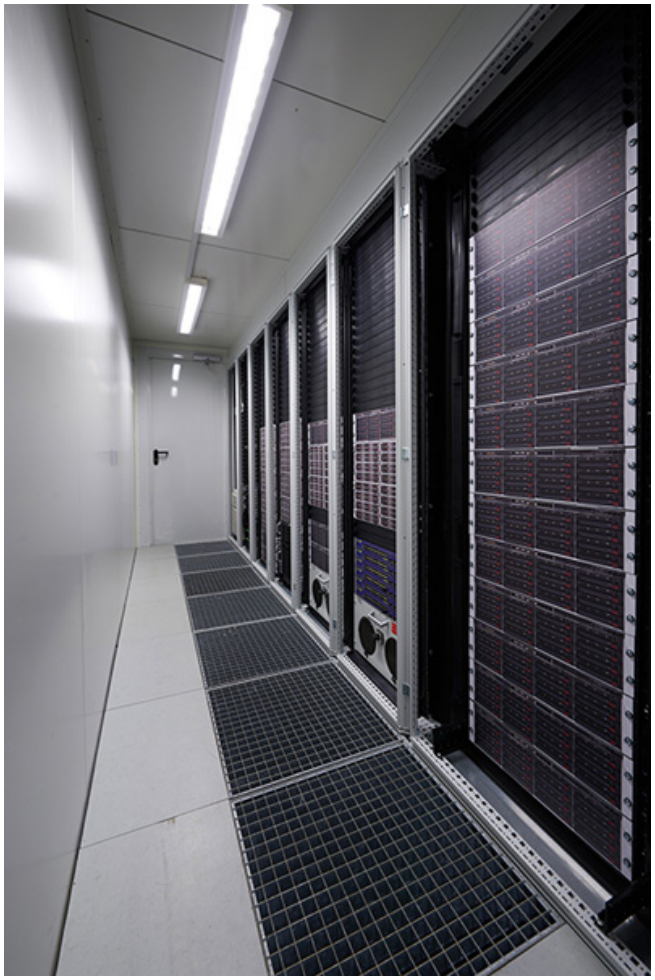
Благодаря акценту на стандартизацию модулей и согласование компонентов система RiMatrix S обеспечивает высокую эффективность энергопотребления. Кроме того, готовая система позволяет сэкономить на проектировании ЦОД. RiMatrix S можно наращивать модулями по 6 или 9 стоек при создании крупных ЦОД, размещать такие модули в контейнере или устанавливать в помещении, где требуется повышенная безопасность.

В состав RiMatrix S входит система контроля микроклимата с резервированием N+1. ИБП (при наличии встроенного источника бесперебойного питания) резервируется по схеме N+1. При установке модуля распределения питания Rittal PDU расход электроэнергии можно измерять вплоть до розетки. Для комплексного контроля применяется система мониторинга Rittal CMC III (Computer Multi Control), насчитывающая до 32 датчиков температуры, влажности и задымления. Данные измерения отражаются в программе RiZone с функциями управления. Дополнительно серверный модуль может быть оснащен системой пожаротушения.

RiMatrix S можно применять как при строительстве новых ЦОДов для создания конструкции с общими зонами горячего и холодного воздуха, так и для расширения существующих центров данных. Современные крупные ЦОДы также используют контейнерные модули, так как с их помощью при необходимости может

быть увеличена вычислительная мощность, что приводит к повышению загрузки системы.

Обладая шириной 3 метра, контейнер Rittal внутри очень просторен и предоставляет достаточно пространства в случае необходимости планового обслуживания и сервисных работ. Несмотря на это, его без всяких проблем можно перевозить на грузовике, корабле или самолете. Так как стандартные 20-футовые контейнеры, как правило, не обладают достаточной прочностью, необходимой для чувствительного ИТ-оборудования, ЦОД-контейнер Rittal оснащен усиленной наружной обшивкой с классом пожароустойчивости F30 и классом защиты от взлома 3. Система доступа может быть оснащена по выбору считывателем кодовых карт, электронным замком или кодовым кнопочным замком. С4IT



Процессоры AMD Zen дебютируют в серверах

Процессоры на микроархитектуре AMD Zen должны появиться на рынке в 2016 году и вначале будут предназначены для серверов. За ними последуют модели для рабочих станций и высокопроизводительных настольных ПК (HEDT). Этот подход, очевидно, продиктован желанием AMD поскорее укрепить позиции в сегменте высокопроизводительных решений.

По предварительным сведениям, процессоры Summit Ridge на микроархитектуре AMD Zen будут иметь до восьми x86-совместимых ядер. Их TDP, очевидно, не превысит 95 Вт. Современные процессоры AMD FX характеризуются, соответственно, показателями 95 и 125 Вт, а модели, рассчитанные на частоту до 5 ГГц, — даже 220 Вт. Возможен выпуск модификаций AMD Zen с пониженным энергопотреблением. Согласно неофициальным данным, в микроархитектуре Zen компания AMD планирует уйти от модульного дизайна и представить нечто похожее на Hyper-Threading.

По одним данным, процессоры будет выпускать TSMC по 16-нанометровой технологии FinFET, по другим данным, процессоры будут 14-нанометровыми. С4IT

Организация связности в распределенном ЦОДе с использованием оптических технологий

Максим Калинкевич,
системный инженер Cisco

При создании географически распределенных ЦОДов одним из самых главных требований является обеспечение низкой задержки и высоких показателей надежности при передаче данных между площадками ЦОДа.

По мере развития популярности облачных услуг хранения и обработки данных заказчики предъявляют все более высокие требования к качеству подобных сервисов. Ожидается, что доступ к ресурсам центров обработки данных (ЦОД) поставщиков облачных услуг можно получить в любое время из любой сети, и эти требования становятся особенно критичными в случае, если облачные услуги нацелены на сегмент корпоративных заказчиков.

При наличии большого количества корпоративных заказчиков, каждый из которых имеет географически распределенную инфраструктуру, поставщики облачных ресурсов вынуждены отходить от традиционной схемы построения ЦОДов (основная площадка — резервная площадка) и переходить к распределенной модели хранения и обработки данных, используя множество ЦОДов, распределенных географически. Ресурсы таких ЦОДов могут использоваться для индивидуальных заказчиков или приложений или же являться частью одной единой системы виртуализации.

В такой архитектуре одним из обязательных требований является обеспечение низкой задержки и высоких показателей надежности при передаче данных между площадками ЦОДа. Для этого площадки центра обработки данных связывают между собой прямыми высокоскоростными каналами, в результате чего получается многосвязная отказоустойчивая топология каналов связи распределенного ЦОДа. Такая система ЦОДа может предоставлять услуги хранения и обработки данных, а также сетевой связности для площадок конечного пользователя. При этом сами данные могут перемещаться внутри облачной инфраструктуры по сети от одного ЦОДа к другому в зависимости от текущих потребностей конечного заказчика.

По мере эволюции архитектуры ЦОДа к распределенной модели необходимо учитывать следующие ключевые аспекты:

• Снижение совокупной стоимости владения — уменьшение капитальных затрат, а также энергопотребления и арендуемого места в стойках.
• Максимизация утилизации каналов связи и минимальная стоимость на один бит передаваемой информации, конвергенция трафика SAN и LAN для передачи в одном канале связи.
• Комплексное управление всеми устройствами в сети для уменьшения времени, необходимого для наиболее частых операций, таких как ввод в эксплуатацию услуг и сервисов.

С точки зрения выбора технологии для построения сети, связывающей площадки распределенного ЦОДа между собой, требования следующие:

- Конвергенция в одной сети передачи технологий Ethernet, Fiber Channel, Infiniband
- Масштабируемость транспортных каналов от 10 до 100 Гбит/с и выше
- Гарантированное качество обслуживания для всего объема трафика
- Защита на уровне 50 мс
- Поддержка шифрования данных для наиболее критичного трафика

Технология плотного спектрального уплотнения (DWDM) является лидирующей с точки зрения обеспечения требований при передаче данных между площадками распределенной системы ЦОДа. Использование «темного волокна» при небольшом количестве каналов и небольшом расстоянии между площадками ЦОДа является обоснованным вариантом для топологии «основная площадка — резервная площадка», однако плохо подходит для случая, когда расстояния между географически

распределенными узлами превышают 80 км и когда необходимо организовать многосвязную топологию. Технология CWDM частично лишена этих недостатков за счет применения оптического спектрального уплотнения, но имеет ограничения с точки зрения поддерживаемых расстояний (до 120 км), количества доступных

Рис. 1. Cisco NCS 2006

каналов связи (до 16 в одной паре волокон) и их скорости (на рынке присутствуют модули 1,4 и 10 Гбит/с). Технология DWDM поддерживает передачу множественных каналов связи (40/80/96 в одной паре волокон) на скоростях до 200 Гбит и выше на расстояния в несколько тысяч километров, что делает ее лидером транспортных технологий для многосвязной топологии распределенного ЦОД.

Платформа Cisco NCS 2006 — один из лидеров на рынке DWDM-решений. Она способна эффективно решать задачи объединения ЦОДа, начиная от простых топологий «точка — точка» для схемы «активный — резервный ЦОД» и заканчивая сложными многосвязными оптическими топологиями. Поддерживается широкий набор клиентских интерфейсов, таких как традиционные Ethernet, SDH, интерфейсы SAN, а также интерфейсы различных стандартов передачи видео HD SDI, SD SDI. Отличительной особенностью этой платформы является возможность организации шифрования каналов передачи данных с аутентификацией данных как для интерфейсов на скоростях

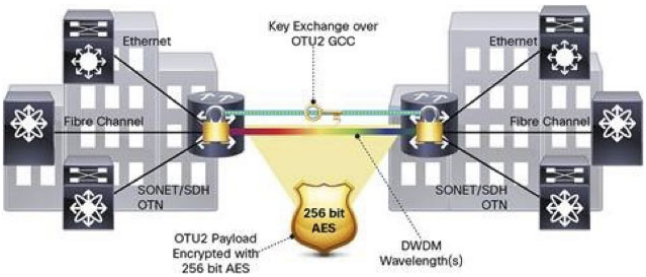


Рис. 2. Схема резервирования ЦОД

10 Гбит/с, так и для скоростей 100 Гбит/с. Сейчас максимальная скорость передачи на одну длину составляет 200 Гбит/с с возможностью увеличения в будущем до 250 Гбит/с. Система поддерживает возможность организации до 96 длин волн для передачи транспортных потоков между площадками ЦОД.

Подробную информацию о продукте можно получить по адресу или обратившись в локальное представительство Cisco. с4IT

Cisco UCS: революция на рынке серверов

Пять лет назад компания Cisco приняла решение расширить свое портфолио стоечными и блейд-серверами на базе процессоров Intel Xeon. Появление новых продуктов Cisco Unified Computing System (UCS) вызвало неоднозначные оценки на рынке. Скептики говорили, что это не тот бизнес, где Cisco может «выстрелить». Действительно, крайне сложно предложить что-то исключительное на рынке серверов, существующем уже не один десяток лет. Но оптимисты ожидали, что с появлением решений Cisco в мире традиционных серверов произойдет если не революция, то значительные изменения.

Результаты превзошли даже ожидания оптимистов. Компания сделала верный ход, предложив законченное решение, а не просто набор хороших по качеству отдельных «коробочек». В итоге оборот продаж Cisco UCS превышает $3 млрд в год. Почти 40 тыс. уникальных заказчиков выбрали эту платформу в качестве основы своих центров обработки данных.

Cisco заняла первое место по продажам блейд-систем в США и на обоих американских континентах с долей рынка более 40%. В мире компания вышла на второе место в сегменте серверов и на первое (с долей свыше 42%) — по продаже интегрированных комплексов «Cisco UCS + система хранения». Революция на рынке состоялась. с4IT

ВИРТУАЛИЗАЦИЯ ХРАНЕНИЯ ДАННЫХ

По материалам DataCore Software

Виртуализация хранения данных в настоящее время является одной из наиболее актуальных тем в сфере построения и модернизации ЦОДов. На рынке постоянно появляются решения, расширяющие привычный функционал СХД. Одним из поставщиков таких решений является компания DataCore, предлагающая решения класса SDS и ESV.

За последнее время состоялось несколько интересных программно-аппаратных альянсов и тестирований в области виртуализации хранения данных. Компания DataCore, поставщик Software Defined Storage (SDS) и Enterprise Storage Virtualization (ESV), создает свои решения на основе принципа аппаратной независимости и без привязки к определенным производителям аппаратных средств, что позволяет многим компаниям усовершенствовать свои решения. К примеру, SDS SANsymphony-V от компании DataCore позволяет одновременно снизить затраты за счет использования недорогих аппаратных ресурсов при создании СХД Hi-End класса, повысить производительность за счет оптимального использования серверных ресурсов (кэш размером до 1 ТБ, построенный на базе дешевой памяти сервера) и обеспечить безопасность хранения данных. Поэтому вполне закономерно, что производители аппаратного обеспечения дополняют свои решения программным функционалом SANsymphony-V для предложения высокотехнологичных решений в недорогом ценовом сегменте.

CISCO UCS

Успешно достигнута функциональная совместимость SANsymphony-V10 и Unified Computing System Cisco, а именно серверов UCS C-Series. Соответствующее тестирование проведено Cisco Interoperability Verification Testing (IVT) и решение сертифицировано. Как член партнерской программы Cisco Solution, DataCore Software может быстро создавать и развертывать решения для повышения производительности и расширения возможностей управления сетью.

Доскональное тестирование SANsymphony-V и Cisco UCS продемонстрировало легкость развертывания и внедрения решений для хранения данных, которые могут обслуживать виртуальные и физические хосты в конфигурациях с несколькими площадками. Теперь DataCore и Cisco могут обеспечить своим партнерам всесторонние аппаратные решения для ЦОД с возможностями корпоративных систем высочайшего уровня. На платформе Cisco решения охватывают сети, вычислительные ресурсы и хранение данных. Эти решения обеспечивают функции хранения данных корпоративного класса для гиперконвергентных систем, а также структур, которые обеспечивают независимое, масштабированное хранение данных и вычисления, и связаны между собой сетевой инфраструктурой Cisco. Дополнительные новые или имеющиеся СХД от третьих производителей могут быть легко интегрированы в эти решения в соответствии с требованиями бизнеса.

Партнерская программа Cisco Solution объединяет Cisco с независимыми производителями оборудования и ПО в области реализации комплексных решений для общих клиентов.

СЕРВЕРЫ FUJITSU PRIMERGY

Серверы Fujitsu PRIMERGY сертифицированы как DataCore Ready для виртуализации, объединения и безопасного хранения данных и абсолютно совместимы с Software-Defined Storage SANsymphony-V10, что позволяет создавать гарантированно рабочие, экономичные и высокодоступные решения при их совместном использовании. Кроме того, системы хранения DX-серии Fujitsu ETERNUS также получили статус DataCore Ready. Последние версии серверов Fujitsu и DataCore SANsymphony-V10 создают экономичные решения для хранения данных, обеспечивая максимальные потребности бизнеса благодаря вдвое большей производительности и масштабируемости по сравнению с предыдущими поколениями.

Общие решения от Fujitsu и DataCore, таким образом, отвечают самым высоким требованиям по производительности и надежности эксплуатации в крупных компаниях. Кроме того, серверы Fujitsu PRIMERGY позволяют быстро, экономически эффективно и легко развернуть решение Virtual-SAN для сред Microsoft Hyper-V или смешанных сред с VMware, для критически важных приложений, таких как Microsoft Dynamics ERP, базы данных SQL, SharePoint, Exchange, SAP, Oracle или VDI.

С помощью SDS SANsymphony-V серверы и системы хранения Fujitsu могут быть интегрированы в любую существующую инфраструктуру с оборудованием от EMC, Hitachi, HP, IBM, NetApp. Кэширование и технология автоматического многоуровневого хранения данных эффективно используют ресурсы серверов Fujitsu PRIMERGY и делают данный функционал доступным во всей инфраструктуре хранения данных компании. Также объединение всех ресурсов хранения данных с помощью SANsymphony-V делает доступным для всех систем в ИТ-структуре зеркалирование данных, резервное копирование на удаленные сайты, автоматическое многоуровневое хранение, хранение резервов и миграцию данных в новые или существующие СХД и флэш-среды. Достигается значительное увеличение производительности (до 30 раз), в частности, через функционал оптимизации случайной записи, особенно при высоких рабочих нагрузках, ориентированных на транзакции, такие как базы данных или ERP-системы.

Подобные совместные решения обозначают новое программно-определяемое поколение ресурсов хранения данных, объединяют ведущие ИТ-продукты, а тестирование решений и сертификации делает их легкими в освоении для заказчиков, которые стремятся купить качественные, оптимизированные и экономичные системы. Сертификация подчеркивает высокий уровень совместимости продуктов.

СЕРВЕРЫ DELL POWEREDGE

Новые совместные решения позволяют использовать и успешно эксплуатировать серверы Dell PowerEdge с SANsymphony-V и Virtual-SAN для того, чтобы обеспечить комплексное хранение данных в программно-определяемых системах хранения данных, способных объединить и обеспечить оптимизацию производительности существующих и будущих ресурсов хранения компании. Такие решения предлагают расширенные возможности корпоративного класса, обеспечивая производительность и масштабируемость в два раза выше по сравнению с предыдущим поколением. Программное обеспечение DataCore работает с серверами Dell PowerEdge и полным спектром СХД Dell MD-, SC- и PS-серий. Серверы DataCore на платформе Dell и дисковые массивы Dell могут быть легко интегрированы со всеми системами хранения и популярными версиями твердотельных накопителей, независимо от поставщика. Таким образом, пользователь получает ускорение производительности всей инфраструктуры хранения данных. Совместное решение предлагает расширенные функции СХД, такие как глобальное общее хранилище для кластеров, зеркалирование и отказоустойчивость, автоматическое многоуровневое хранение данных и миграцию ресурсов хранения между различными типами оборудования (диски и устройства флэш).

Статус DataCore Ready обозначает, что решение предварительно сертифицировано, гарантирует строгую совместимость, доказанную в процессе тестирования, и достижение заявленных параметров производительности. Кроме того, технологическое партнерство DataCore и Dell и взаимная независимая сертификация позволяют убедительно обосновать выбор платформы Dell-DataCore для ИТ-инфраструктуры.

Таким образом, различные типы ресурсов хранения и автономные системы объединяются в виртуальные сети хранения, доступные всей ИТ-инфраструктуре и больше не будут существовать как отдельные острова хранения данных, используемые определенными приложениями. DataCore позволяет интегрировать их в полноценную инфраструктуру хранения данных. Системные администраторы могут легко выделить емкость, оптимизировать использование и установить общие правила, позволяющие динамически выбирать уровень и ресурсы для хранения и наиболее подходящие способы получения желаемой производительности и доступности.

СЕРВЕРЫ И СХД HUAWEI

Huawei Storage Solution фокусируется на разработке решений, их тестировании и сертификации под корпоративные приложения, в том числе сочетаний СХД Huawei и платформ виртуализации, VDI-решений VMware и Citrix, СУБД Oracle и Microsoft SQL Server, систем Microsoft Exchange Mail Server и т.д. Компанией Huawei Storage Solution проведено тестирование решения хранения в сочетании

флэш-массива Huawei OceanStor Dorado2100 G2 и DataCore SANsymphony-V, а также Oracle 11g OLTP на платформе виртуализации VMware VSphere 5.5. Тестирование проводилось для того, чтобы проверить совместимость и обосновать выгоды, а также параметры:

- повышения производительности;
- облегчения управления и мониторинга;
- масштабируемости и высокой доступности.

Это решение демонстрирует, как DataCore SANsymphony-V, в сочетании с Huawei SAN, могут быть использованы приложением Oracle OLTP.

Архитектура решения

На рисунке ниже изображена архитектура физической среды.

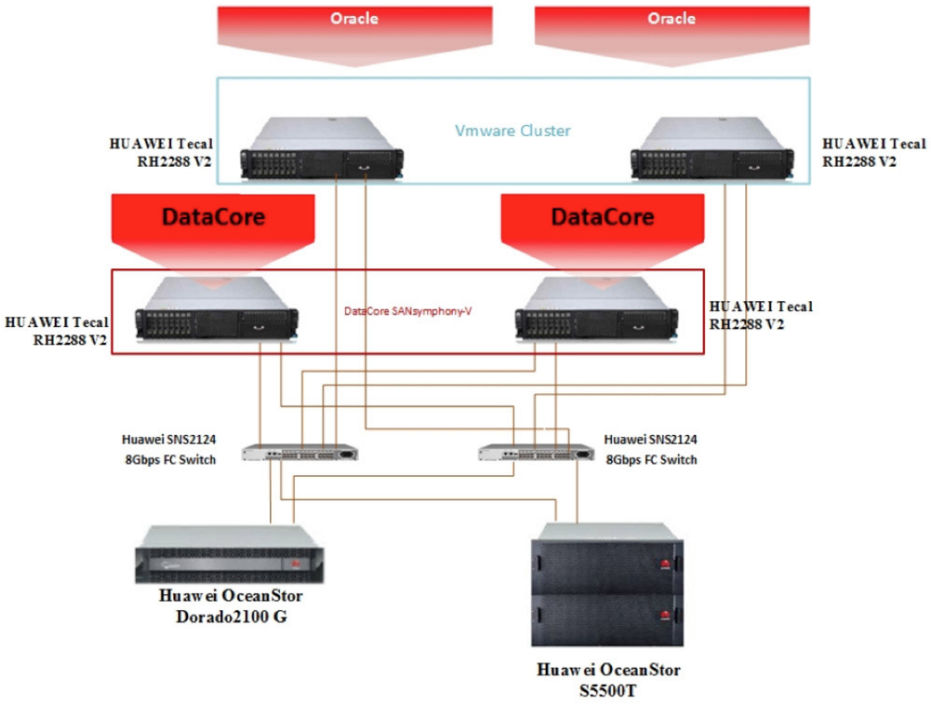


Рис. 1. Архитектура физической среды при тестировании решения в сочетании флэш-массива Huawei OceanStor Dorado2100 G2 и DataCore SANsymphony-V, а также Oracle 11g OLTP

Два физических сервера с Microsoft Windows Server 2012 R2 были использованы для развертывания серверов DataCore SANsymphony-V, еще два физических сервера были использованы для развертывания хостов VMware Vsphere ESXi и двух автономных экземпляров сервера Oracle. Один массив Huawei OceanStor S5500T – традиционная SAS-система хранения – и один Flash-массив Dorado2100 G2 были развернуты как системы хранения.

Полученные результаты

Повышение производительности:
- увеличение количества транзакций в минуту (TPM) на 400% и IOPS более чем на 300% в конфигурации без зеркалирования виртуального диска;
- снижение среднего времени отклика (database response time) в конфигурации без зеркала виртуального диска;
- устранение узких мест в подсистемах на SAS-дисках в конфигурации зеркального виртуального диска, улучшение TPM в 9 раз и уменьшение среднего времени отклика более чем в 7 раз.

Улучшения без прерывания деятельности:
- Auto-tiering от DataCore SANsymphony-V может легко и без прерывания работы повысить производительность приложений;
- SSD LUN могут быть быстро и без перерыва работы добавлены к существующей среде и обеспечить поэтапный подход к внедрению флэш-технологий.

Простота настройки и мониторинга:
- С помощью DataCore SANsymphony-V можно быстро настроить и легко изменить виртуальные SAN. Диски и LUN могут быть легко добавлены, изменены или удалены с помощью одного клика, без прерывания запущенного приложения.

Примеры, которые приведены выше, иллюстрируют технологическое партнерство брендов. В настоящее время готовится и проводится тестирование системы SANsymphony-V с многими локальными производителями аппаратных систем в нескольких странах, в том числе и с украинскими производителями. Это позволит компаниям выбирать решения практически из любого ценового сегмента, опираясь на данные по совместимости и производительности, полученные в результате тестов, а также строить решения на оборудовании тех производителей, которым доверяют и поддержкой которых пользуются. c4it

ИННОВАЦИИ ЦОД. ОБЕЩАНИЯ VS РЕАЛЬНОСТЬ

Олег Пилипенко

Новые технологии для построения и оптимизации ЦОДов появляются регулярно. Некоторые приживаются очень быстро, другие — медленно и сложно. Если отложить в сторону решения для инженерной инфраструктуры, то в последние годы четко доминируют две актуальные технологии: конвергентная инфраструктура и программно-конфигурируемые системы. К последним относится целый спектр различных устройств и компонентов ЦОДа. Но насколько эти инновации актуальны для украинского ИТ-сектора? Об этом мы спросили экспертов.

ЕСТЬ ЛИ СПРОС НА КОНВЕРГЕНТНОСТЬ?

Популярность конвергентной и гиперконвергентной инфраструктуры в последние годы уверенно растет. Но интересуется ли украинский рынок ЦОДов подобными технологиями и есть ли уже завершенные внедрения? Мнения отечественных экспертов по этому поводу разделились. Одни уверены, что интерес рынка к подобным инновациям и внедрения уже присутствуют. Другие полагают, что конвергентность это, скорее, маркетинговый лозунг.

«Под конвергентной инфраструктурой подразумевается инфраструктура, которая имеет общие ресурсы для максимально широкого класса задач, отличается минимальными операционными затратами и позволяет сосредоточиться на инновациях, – говорит Вадим Запарованый, ведущий инженер-консультант департамента телекоммуникаций компании Инком. – В Украине заказчики положительно относятся к конвергенции серверных ресурсов и ресурсов хранения. Активно используется виртуализация и все меньше процессов по принципу: одно приложение – один сервер.

Но если говорить о конвергенции сетевой части и особенно каналов связи, то здесь ситуация немного хуже. Возможно, это связано с тем, что сетевая инфраструктура традиционно менее чувствительна к изменениям бизнеса, чем вычислительная. Внедрения по конвергенции сетевой инфраструктуры наиболее востребованы операторами связи, крупными банками и операторами ЦОДов».

Ирина Бернацкая, системный консультант Dell, отмечает, что конвергентность — уже не новое понятие, и в сегменте ИТ интерес к таким инфраструктурам постоянно растет. Это обусловлено тем, что подобные решения представляют множество преимуществ для заказчиков: будучи компактными, энергоэффективными и практически бесшумными, они обеспечивают высокий уровень производительности.

В Cisco также уверены, что конвергентная инфраструктура набирает популярность в нашей стране. Продукт Unified Computing Systems (UCS) – полностью конвергентная инфраструктура — в настоящее время насчитывает более 100 инсталляций в Украине (банки, ритейл, промышленность, малый и средний бизнес). В то же время Геннадий Карпов, директор по технологиям De Novo, считает, что на данный момент эти термины, скорее, играют роль маркетинговых лозунгов. Технологии, которые за ними стоят, стали пригодны к промышленному использованию буквально в последние пару лет. Поэтому их практически невозможно встретить в корпоративных инфраструктурах – такая архитектура достаточно инертна и не особо склонна к инновациям. Другое дело операторы облачных сервисов – для них инновации являются основным драйвером эффективности и рыночной дифференциации. Кстати, в облаке De Novo два ресурсных кластера из трех подходят под определение «гиперконвергентный» — каждый узел располагает не только вычислительными ресурсами, но и сетевыми и ресурсами хранения данных (технология VMware vSAN).

Юрий Ярощук, начальник отдела технологий центров обработки данных, «ЭС ЭНД ТИ УКРАИНА», также довольно сдержанно относится к тематике конвергентности: «Хотя на ИТ-рынке всегда есть интерес к инновационным

технологиям и новинкам, однако некоторые решения так и остаются нереализованными. Несмотря на то, что по отчетам вендоров конвергентная и гиперконвергентная инфраструктуры набирают популярность, реальных внедрений, в сравнении с традиционным построением ЦОД, остается мало». Рынок Украины – не исключение. Виной тому является высокая стоимость внедрения таких технологий, которая у западных компаний нивелируется за счет операционных затрат. В Украине же операционные затраты значительно ниже.

ПРОГРАММНО-ОПРЕДЕЛЯЕМЫЕ РЕШЕНИЯ КАК СПОСОБ ДОСТИЖЕНИЯ ЦЕЛЕЙ БИЗНЕСА

Сегодня много говорят о решениях класса «software-defined», то есть программно-определяемых решениях. Насколько это актуально для украинского ИТ-бизнеса и какие именно направления из общей группы решений такого типа пользуются наибольшим успехом? Термин «software-defined» появился и развивается как часть виртуализированной инфраструктуры. Данный термин обещает пользователю независимость от аппаратных средств и политики вендоров, что в реалиях современного состояния ИТ весьма важно, комментируют специалисты Бакотек. Уже известны программно-определяемые сети, ПК и серверы, СХД и даже радио. Все эти решения подразумевают независимость от аппаратных средств и виртуализацию. С развитием виртуализации и «облачных» решений в Украине, вендоры и дистрибьюторы все активнее предлагают соответствующие решения. Однако Геннадий Карпов из De Novo смотрит на программно-определяемые решения скептически: «Пока об этих технологиях говорить рано, они практически отсутствуют. Разве что отдельные виртуальные инфраструктуры можно, с некоторой натяжкой, отнести к классу software-defined datacenter (SDDC). Если же говорить о software-defined network (SDN) и software-defined storage (SDS), то их время еще не пришло – эти «юные» технологии еще ждут своих первопроходцев, которыми, скорее всего, станут облачные операторы».

«Тем не менее, многие компании все же начали, не без лоббирования вендорами, присматриваться к данным технологиям. Некоторые «software-defined» уже идут практически «из коробки» с поставляемыми решениями, — говорит Юрий Ярощук из «ЭС ЭНД ТИ УКРАИНА». — В качестве примера можно назвать виртуальные коммутаторы Cisco Nexus 1000v. Многие вендоры рекомендуют вместо приобретения выделенных бандлов установку их решений на виртуальные машины: это и серверы IP-телефонии, и маршрутизаторы, и сетевые экраны. Данные решения успели себя хорошо зарекомендовать, а учитывая, что существующих мощностей с избытком хватает для большинства задач, логично предположить, что данная тенденция сохранится и в будущем».

Ирина Бернацкая, Dell, отмечает интерес во всем мире (равно как и в Украине) к программно-определяемым хранилищам. С увеличением актуальности Big Data решения SDS становятся более востребованными. Кроме того, SDS платформы — это фундаментальная технология для программно-определяемых ЦОД (Software-Defined Data Center, SDDC). Впрочем, несмотря на то, что интерес к SDS уверенно растет, мы все еще находимся на ранней стадии. Но, по данным аналитиков IDC, рынок SDS будет развиваться быстрее, чем любой другой сегмент на рынке файловых и объектных систем хранения. Борис Калачев, руководитель отдела сетевых решений компании Инком, называет следующие преимущества SDN: централизация; разделение области данных и управления (контроллер); программируемость и application awareness; открытость и платформонезависимость.

Рост числа сервисов, подкрепленный усилиями компании VMware, привел к появлению в свое время термина «виртуализация», что глобально поменяло ИТ-мир. Виртуализация и большое количество пользователей с разными задачами способствовали появлению технологии «multitenancy» (множественная аренда), что, в свою очередь, потребовало возникновения термина «оркестрация» для возможности управления всем этим массивом. Первоначально в виртуальную среду начали перемещать вычислительные мощности, теперь очередь дошла до сетевой инфраструктуры и других сервисов — Network Function Virtualization (NFV). Таким образом, SDN в своем роде начался с ЦОДа (Amazon Web Services). Вендоры уже больше года несут в массы свои реализации SDN-контроллеров, участвуют в рабочих группах по созданию и стандартизации северного и южного интерфейсов. Но, скорее всего, они сделают все, чтобы затянуть процесс и не потерять свой бизнес или даже его часть, — сетует Борис Калачев.

В нашей стране нет компаний, подобных Amazon, Google или Facebook, которые могут навязать правила игры даже вендорам. Следовательно, массовая востребованность решений будет пока отложена. Тем не менее, Борис Калачев уверен в перспективах SDN. При этом очень не хотелось бы, чтобы гениальная идея осталась лишь «трендом года» или была надолго отложена. C4IT

ВСЕ БУДЕТ ФЛЭШ!

Ян Шмиголь

Флэш-технологии производят революцию в технологиях хранения и обеспечивают прирост производительности практически для любых приложений. Об основных тенденциях в области корпоративных систем хранения данных, важности своевременного внедрения инноваций и перспективах развития рынка издание ChannelForIT Review беседует с Владимиром Бондаренко.

ChannelForIT Review: Что происходит сейчас в мире СХД? Какие тренды Вы можете отметить?

Владимир Бондаренко: Более всего меняют отрасль систем хранения флэш-технологии, причем старт этому был дан еще 7-8 лет назад. За последние годы произошла буквально революция, появились системы хранения данных, которые изначально разработаны под флэш-технологии, так называемые all-flash arrays.

Владимир Бондаренко

В чем нюанс прежних систем? В том, что все они имеют устаревшую архитектуру, которая не приспособлена к работе с большим количеством флэша. Конструктивно их разрабатывали для работы с известными нам традиционными механическими дисками. Разница между обычным диском и флэш-диском в намного большей производительности последнего, отсутствии механических частей, меньшем энергопотреблении и тепловыделении. Современный флэш-диск корпоративного класса (производятся 100, 200, 400, 800-гигабайтные и ожидаются 1.6 Тб модели) обеспечивает до 20 тысяч операций ввода-вывода в секунду, в то время как традиционный NL-SAS/SAS диск — только 75-120 операций. Это очень большая разница! Как результат – устаревшая архитектура накладывает ряд определенных ограничений по производительности. Например, если вы превысите определенное число флэш-дисков в системе, она не сможет активно эти диски «раскачать», т.е. получить от них максимум производительности. Так, флэш-диск будет выдавать, например, 1700 операций ввода-вывода в секунду вместо возможных 5-10 тысяч, а это значит, что деньги на флэш-диски потрачены не совсем эффективно. Совершенно очевидно, что с точки зрения соотношения «цена за операцию ввода-вывода» флэш-диск имеет значительное преимущество, в то время как традиционный механический диск имеет наилучшее соотношение «цена за гигабайт» хранимой информации.

Кроме широкой функциональности (дедупликация, компрессия, репликация, многоуровневое хранение и т.п.), у систем хранения имеются две наиболее распространенные метрики: это стоимость операции ввода-вывода (так называемый IOPS) и стоимость гигабайта объема. Эти две характеристики в какой-то мере противоречивы: чем больше производительности (операций ввода-вывода) вы хотите получить, тем больше традиционных дисков вам необходимо приобрести. Поэтому у заказчиков ранее всегда была дилемма: либо приобретать

больше емкости, но жертвовать производительностью, либо выбирать высокую производительность в ущерб объему. С началом применения технологий многоуровневого хранения, в которых сочетаются как традиционные, так и флэш-диски, заказчики получили возможность приобрести оптимальные и более сбалансированные системы хранения по соотношению «цена-емкость-производительность».

Подобные системы хранения, называемые «гибридными», т.е. использующие как флэш, так и традиционные диски, в настоящее время наиболее распространены и популярны на рынке. Так, для получения «скорости» в них устанавливают флэш-диски, а для «емкости» – традиционные NL-SAS. Таким образом достигается оптимальное соотношение «цена-емкость-производительность». Накопленный опыт и знания в области применения флэш-дисков позволили разработать принципиально новые системы хранения данных, которые архитектурно спроектированы исключительно для работы с флэш-дисками, обеспечивая им максимальную отдачу не только с точки зрения производительности, но и функциональности (дедупликация, компрессия, репликация и т.д.). Именно эти системы сейчас имеют на рынке наибольшую динамику роста продаж, поскольку обеспечивают взрывной рост производительности практически для всех типов приложений, особенно для высоконагруженных сред баз данных, виртуальных инфраструктур. Реализации подобных решений были в Украине в прошлом году.

Это совсем не значит, что в ближайшие годы all flash-array заменят хорошо нам известные гибридные системы, но процесс замещения в ряде областей уже происходит.

Флэш-технологии не ограничиваются лишь дисками для систем хранения, также активно развивается сегмент карт-ускорителей, которые устанавливаются непосредственно в серверы и комплектуются специализированным программным обеспечением. Вот такой современный треугольник использования технологий твердотельной памяти: серверный flash в виде карт-ускорителей, полностью оптимизированные для работы с флэш-дисками системы all flash-array и флэш-диски (флэш-модули) в традиционных (гибридных) системах хранения данных.

ChannelForIT Review: Насколько решены вопросы с надежностью продуктов на базе флэш-технологий?

В.Б.: Насколько я знаю, вопрос надежности решен, поскольку на системы хранения all-flash-array производители предоставляют расширенные гарантии (например, 7 лет на диски вместо обычной 3-летней гарантии). Дело в том, что корпоративные флэш-технологии и те, которые используются в потребительском сегменте, отличаются. Чтобы немного углубиться в технические детали, следует поинтересоваться терминами SLC, MLC, eMLC. Не все флэш-диски одинаковы с точки зрения надежности и производительности. Так, разница может составлять разы. Следует обращать на это внимание, поскольку их стоимость также существенно разнится.

«Для программно-определяемых СХД экономическим двигателем служит недорогая и широко распространенная платформа x86»

ChannelForIT Review: С Вашей точки зрения, какие технологии будут далее определять развитие СХД?

В.Б.: Последние несколько лет в индустрии начали активно говорить о программно-определяемых ЦОДах. При этом в рамках программно-определяемых ЦОДов появились технологии программно-определяемых систем хранения. Почему индустрия стала двигаться в таком направлении? С одной стороны, это обеспечивает огромную технологическую гибкость, высокую скорость выделения ресурсов и независимость от производителей аппаратных платформ. С другой стороны, x86-платформа за последние 5 лет очень сильно прибавила в производительности, что позволило реализовать на ней широкую программную функциональность систем хранения, например, такую как дедупликация, компрессия, многоуровневое хранение, обеспечение качества сервисов (QoS).

Поэтому для программно-определяемого ЦОДа и программно-определяемых СХД экономическим двигателем служит недорогая и широко распространенная платформа x86, и многие современные системы хранения данных на сегодняшний день базируются именно на ней. Упрощенно говоря, СХД — это Intel-серверы, которые работают под управлением специализированных операционных сред (систем). А это значит, что вся функциональность такой системы хранения в какой-то момент может быть реализована в виде виртуальной машины, работающей в среде программно-определяемого ЦОДа. Физически роль хранилища данных могут выполнять обычные, более дешевые системы хранения, или внутренние диски серверов, объединенные в общий пул хранения с различными характеристиками производительности.

Таким образом, флэш-технологии и программно-определяемые СХД будут определять развитие рынка корпоративных систем хранения данных в ближайшие годы.

ChannelForIT Review: Как происходит развитие технологий: вендоры подталкивают рынок к использованию новых изобретений или же рынок выдвигает свои требования и производители откликаются на них?

В.Б.: Я бы сказал, что движение происходит с обеих сторон. С одной стороны, у всех вендоров имеются центры разработок, где изобретают новые технологии, подходы, продукты. С другой стороны, тесная работа с партнерами и заказчиками позволяет производить продукты и технологии, которые максимально отвечают их потребностям. В результате происходит обоюдно направленное движение. Как показывает практика, крупные вендоры, несмотря на большие финансовые возможности и широкую базу клиентов, не всегда могут быстро и правильно определить наиболее «горячую» и востребованную технологию. В итоге, чтобы не упустить рынок, они прибегают к покупке другой компании и восполняют свой технологический пробел.

Приведу пример двустороннего движения. До 2008 года в системах хранения данных не использовались флэш-диски, и компания EMC в январе анонсировала флэш-диски в системах старшего класса, а к концу года они стали доступны и для систем среднего класса. Почему это было сделано?

Во-первых, потому что за последние 5 лет процессоры x86 и технологии виртуализации очень сильно прибавили в производительности – в несколько раз. Это позволило на одном физическом сервере размещать большее число виртуальных машин, что значительно увеличило нагрузку на хранилища данных. В то же время производительность жесткого диска за тот же период не изменилась. Выросла емкость дисков, но скорость их вращения не изменилась и сегодня максимально составляет 15 000 оборотов, поскольку существуют физические ограничения. В итоге образовался значительный разрыв в скорости работы вычислительных мощностей и подсистем хранения данных. Именно флэш-диски, с их высокой производительностью, смогли заполнить возникший технологический разрыв.

Во-вторых, с экономической точки зрения флэш-диски имеют существенно более низкую стоимость на единицу производительности, потребляют меньше электроэнергии и выделяют меньше тепла. Это несет прямые финансовые выгоды для заказчика.

Можно ли считать это инновацией? Однозначно. Это продукт «впереди поезда» – и все же, это удачный маркетинговый ход или ответ на вызовы рынка? Заказчики нуждались в такой технологии, поскольку, по данным аналитических компаний, уже в 2009 году количество реализованных виртуализированных серверов превысило число физических. Это был признак того, что рынок меняется и нужны технологические перемены. В течение следующих двух лет флэш-диски в том или ином качестве появились практически у всех производителей корпоративных систем хранения.

Первое время флэш-диски действительно стоили очень дорого, потому что технология была совершенно новая. Но сегодня уже рынок массово использует флэш-диски, поскольку они на практике доказали свою эффективность. Наша страна в этом плане не является исключением.

ChannelForIT Review: На какие линейки оборудования сегодня делают акцент заказчики?

В.Б.: Сегодня заказчики делают акцент не на определенных линейках оборудования, а фокусируются на решениях, которые позволят им более экономно использовать то, что у них уже есть, или же минимально инвестировать в новое. Суть задачи заключается в том,

чтобы как можно более эффективно хранить имеющуюся информацию, используя одни и те же ресурсы. В решении этой задачи поможет исследование инфраструктуры заказчика специалистами, которые проверят, какие данные активны, а какие – нет, и посоветуют, что можно сделать с неактивными данными. При этом не всегда обязательно приобретать новую систему или апгрейд, иногда достаточно просто переконфигурировать систему, выгрузить неактивные данные на более дешевый и медленный носитель.

Существуют инструменты, которые позволяют выполнить анализ, а затем произвести оптимизацию хранения информации на различных системах хранения данных. Кроме этого, возможно одновременно проанализировать работу как СХД, так и приложений баз данных Oracle или виртуальной среды, детально рассмотреть, что происходит на уровне приложений. По результатам обследования можно сформировать рекомендации для конкретного заказчика и его инфраструктуры хранения. Это затратно с точки зрения времени и ресурсов, но, как показывает практика, только такой подход дает гарантированный результат для заказчика.

Если все же говорить о продажах новых систем, то, как я ранее уже сказал, наиболее востребованы гибридные системы хранения среднего класса.

ChannelForIT Review: Традиционно ИТ-технологии наиболее востребованы в банковском сегменте и в телеком-индустрии. Кризис ничего не изменил в этом раскладе?

В.Б.: Наверное, нет. Наиболее крупные проекты в области корпоративных систем хранения в нашей стране в последние несколько лет были реализованы в банках и телекомах. Динамика прироста объемов данных в этих сегментах выше, чем у других.

Конечно, существуют возможности использовать ресурсы, которые находятся в публичном облаке, но практика показывает, что крупные заказчики предпочитают модель «гибридного облака», когда бизнес-критичные системы находятся в частном облаке, а другие, менее важные, могут быть размещены в публичном.

С ростом спроса на облачные технологии увеличивается спрос на системы хранения со стороны провайдеров таких услуг, этот сегмент имеет большие перспективы, и многие вендоры активно развивают такое сотрудничество. Также не следует забывать и о технологиях видеонаблюдения, в частности, такие проекты, как «безопасный город», могут генерировать значительный спрос на СХД с высоким потенциалом роста в будущем. Большие данные тоже внесут свою лепту в этот процесс.

«Наиболее крупные проекты в области корпоративных систем хранения в нашей стране в последние несколько лет были реализованы в банках и телекомах»

ChannelForIT Review: Каковы Ваши прогнозы по развитию локального рынка на 2015 год?

В.Б.: По итогам 2014 года аналитики IDC сообщают о значительном снижении практически всех сегментов ИТ-рынка: печати, серверов, систем хранения данных, причем спад составляет от 40% до 60%. И это на фоне того, что в 2013 году темпы роста были отрицательные. Рынок сужается, увеличивается конкуренция. Ограничение бюджетов и девальвация локальной валюты заставляют заказчиков еще более тщательно подходить к выбору поставщиков как с точки зрения технологий, так и с точки зрения финансов. Но как бы все ни было сложно, заказчики бюджетировали проекты на 2015 год даже в условиях нынешней неопределенности, а значит новые проекты будут реализованы. Год будет сложным, я бы сказал, очень сложным. Вообще, я оптимист и верю в доброе светлое будущее. У нас в стране огромный потенциал, и именно он дает мне основания для позитива. Мы сильная нация, способная преодолеть все эти трудности. А рынок, – конечно же, он восстановится и снова станет расти. Все будет флэш! c4it

АРХИТЕКТУРА METAFABRIC КОМПАНИИ JUNIPER NETWORKS

По материалам компании ITbiz Solutions

На сегодняшний день облачная среда, мобильность и большие объемы данных являются основными движущими силами преобразований в сфере ИТ. Предприятия и поставщики услуг во всех отраслях постоянно ищут способы получения конкурентных преимуществ, и роль ЦОДов и приложений в этом поиске сейчас велика, как никогда.

С появлением ЦОДов, основанных на технологиях виртуализации, ИТ-руководители начинают рассматривать сеть как очередной рубеж в достижении большей гибкости и эффективности с одновременным снижением расходов.

Но сеть имеет сложную физическую структуру, ею непросто управлять, и она не подходит для динамических сред приложений, превалирующих в современных ЦОДах. Кроме того, ЦОДы большинства организаций распределены по нескольким сайтам и облачным средам, что вызывает дополнительные затруднения. И наконец, высокая динамичность ЦОДа предъявляет все больше требований к сети, включая повышение ее производительности, поддержку новых приложений и сохранение совместимости с существующими приложениями, что приводит к необходимости еще более частых обновлений.

Растущая популярность и широкое распространение коммутационных фабрик, новых протоколов, автоматизации, оркестровки, технологий безопасности и программно-конфигурируемых сетей настоятельно требуют более гибких сетей. Компания Juniper Networks применила весь свой опыт в области сетевых технологий для решения проблем современных ЦОДов и создала архитектуру MetaFabric — комбинацию средств коммутации, маршрутизации, безопасности, ПО, оркестровки и программно-конфигурируемых сетей, работающих совместно с открытой технологической экосистемой и ускоряющих развертывание и поставку приложений как для предприятий, так и для поставщиков услуг. Архитектура MetaFabric позволяет создавать простые, открытые и интеллектуальные ЦОДы, которые ускоряют развертывание и поставку приложений внутри множества сайтов и облачных сред, а также за их пределами. Эта архитектура устраняет сложности и уязвимости, связанные с географически распределенной структурой ЦОДа, их вычислительными узлами и системами хранения данных, независимо от того, являются ли эти ЦОДы собственностью организации или используются на условиях аренды в общедоступном облаке.

Когда развитие сети и приложений выходит на уровень, где все работает одновременно и согласованно, производительность существенно возрастает, расходы на обслуживание сети падают, сотрудники получают возможность работать с лучшими приложениями и, кроме того, повышается общая доступность ЦОДов. Архитектура MetaFabric позволяет достичь двух целей: она сокращает срок окупаемости инвестиций для ЦОДа и максимально увеличивает ценность сети и системы безопасности ЦОДа с течением времени.

РЕАЛИЗАЦИЯ АРХИТЕКТУРЫ METAFABRIC

Применительно к современным ЦОДам архитектура MetaFabric предоставляет преимущества:

• Упрощенное управление. Компания Juniper имеет большой опыт реализации упрощенных средств управления в ряде ЦОДов с семейством продуктов Juniper Networks QFabric, технологией виртуального шасси и архитектурой коммутации фабрики виртуальных шасси. Благодаря архитектуре MetaFabric упрощается управление системами, развернутыми в разных местоположениях. Клиенты могут самостоятельно выбирать приложения, такие как Juniper Networks Junos Space Network Director, контроллеры программно-конфигурируемых сетей (в том числе Juniper Networks Contrail и VMware NSX) и облачные платформы орке-

стровки, такие как OpenStack.
• Согласованный уровень управления. Все компоненты архитектуры MetaFabric могут совместно использовать данные и распространять сведения о своем состоянии как в рамках одного местоположения, так и на другие местоположения, обеспечивая комплексный подход к аналитике. Juniper использует стандартизированные сетевые протоколы и распространяет эти функции на уровень управления, поддерживающий наложенные виртуальные сети и протоколы программно-конфигурируемых сетей. Интеграция обеспечивает комфортное сосуществование физических и виртуальных шлюзов, таких как универсальные граничные маршрутизаторы Juniper Networks MX 3D, выполняющие преобразования «в любых направлениях» с использованием различных протоколов и технологий.
• Оптимизированный уровень данных. Архитектура MetaFabric максимально повышает производительность за счет оптимизации маршрутов трафика. В сети ЦОДа этот результат достигается с помощью универсальных коммутационных фабрик с низкой прогнозируемой задержкой. Независимо от местоположения, такие протоколы, как Ethernet VPN (EVPN), автоматически и динамически меняют маршруты трафика, обеспечивая наилучшую производительность и наиболее эффективное использование ресурсов в любой период времени.
• Существующая сеть и безопасность. Независимо от поставленных задач: обновление ПО на устройствах, установка дополнительной стойки, добавление переходного устройства или даже создание нового ЦОДа — эта архитектура обеспечивает беспроблемное внедрение на любом уровне, одновременно сохраняя открытые стандартизированные технологии. Сеть ЦОДа должна быть способна пережить все, что угодно, а изменения всегда были ее основным «противником». Архитектура MetaFabric устраняет и эту проблему.

Эти принципы и технические преимущества делают архитектуру MetaFabric идеальной сетевой платформой и платформой безопасности для ЦОДа, которая готова прийти на помощь ИТ-руководителям, пытающимся сократить сроки окупаемости инвестиций и одновременно максимально увеличить ценность с течением времени.

В ЧЕМ ОСОБЕННОСТИ АРХИТЕКТУРЫ METAFABRIC?

Архитектура MetaFabric не является отдельным продуктом или технологией.

Это готовое решение для ЦОДа, созданное на основе комбинации высокоэффективных платформ коммутации, маршрутизации и безопасности, использующих многофункциональные микропроцессоры, программируемые системы, адаптируемое программное обеспечение, оркестровку, программно-конфигурируемые сети и открытые API-интерфейсы для интеграции с существующей технологической экосистемой.

Центры обработки данных очень отличаются друг от друга. Одни ЦОДы отличаются высокой степенью виртуализации; другие ЦОДы создаются для работы с частным облаком в условиях полной автоматизации; третьи предназначены для обеспечения высокой производительности и малой задержки; четвертые — для удобства масштабирования; некоторые даже успешно развиваются в программно-конфигурируемых сетях.

Архитектура MetaFabric подходит для каждого из этих сценариев, предоставляя простые и открытые составные компоненты, которые позволяют клиентам самостоятельно выбирать точку отсчета для создания новой сети.

Архитектура MetaFabric включает в себя следующее:

• Коммутаторы, оптимизированные для ЦОДов и обеспечивающие оптимальное соотношение производительности, функциональности и гибкости, необходимое для поддержки любой коммутационной фабрики для любых приложений.
• Маршрутизаторы, в роли которых выступают простые высокопроизводительные шлюзы, позволяющие объединить несколько сайтов ЦОДа в единую сеть, взаимодействующую с облачными средами, виртуальными/физическими сетями и программно-конфигурируемыми сетями с помощью стандартных протоколов и открытых интерфейсов.
• Простая, гибкая и полностью открытая программно-конфигурируемая сеть, которая позволяет выполнять автоматизацию и оркестровку процесса создания виртуальных сетей для новых сервисов и способствует достижению большей гибкости и увеличению дохода.
• Адаптивные системы безопасности для ЦОДа, более эффективные, чем современные межсетевые экраны, и использующие технологии защиты, обнаружения и реагирования на определенные угрозы.
• Средства управления, предназначенные для интеллектуальной автоматизации и оркестровки, виртуализации сети, анализа и контроля, обеспечивают быструю доставку

приложений и высокий уровень доступности.
• Экосистема, в которой успешно взаимодействуют различные технологии, предлагает партнерам Juniper, чья деятельность связана с разработкой ЦОДов, полный комплекс вычислительных ресурсов, систем хранения данных, средств виртуализации, функций безопасности, программно-конфигурируемые сети и оркестровки.

ДЛЯ КОГО НАИБОЛЕЕ ВЫГОДНА АРХИТЕКТУРА METAFABRIC?

Архитектура MetaFabric выгодна для всех, даже для организаций с одним-единственным местоположением ЦОДа, которым требуется сеть для обеспечения гибкости приложений и одновременно — простой и открытый подход. Распространение этих преимуществ на другие местоположения и облачные среды делает выгоду еще более существенной.

Организациям, планирующим развиваться за счет внедрения облачных сред, мобильных технологий и больших данных, архитектура MetaFabric поможет сократить срок окупаемости инвестиций и достичь более высокой долговременной ценности. Это относится к любой организации в любой вертикальной отрасли и/или сегменте поставщиков услуг, включая (но не ограничиваясь этим):

- ЦОД для ИТ-предприятий, планирующих дальнейшую виртуализацию.
- ЦОД для финансовых организаций, которым требуется более высокая степень надежности и более высокая производительность.
- ЦОД для государственных учреждений, где требуется соблюдение определенных правил безопасности.
- Крупные предприятия, которым требуется программно-конфигурируемая сеть для оркестровки частного облака.
- Поставщики облачных услуг, которые хотят максимально увеличить доход от каждого пользователя (RPU), предлагая новые услуги.

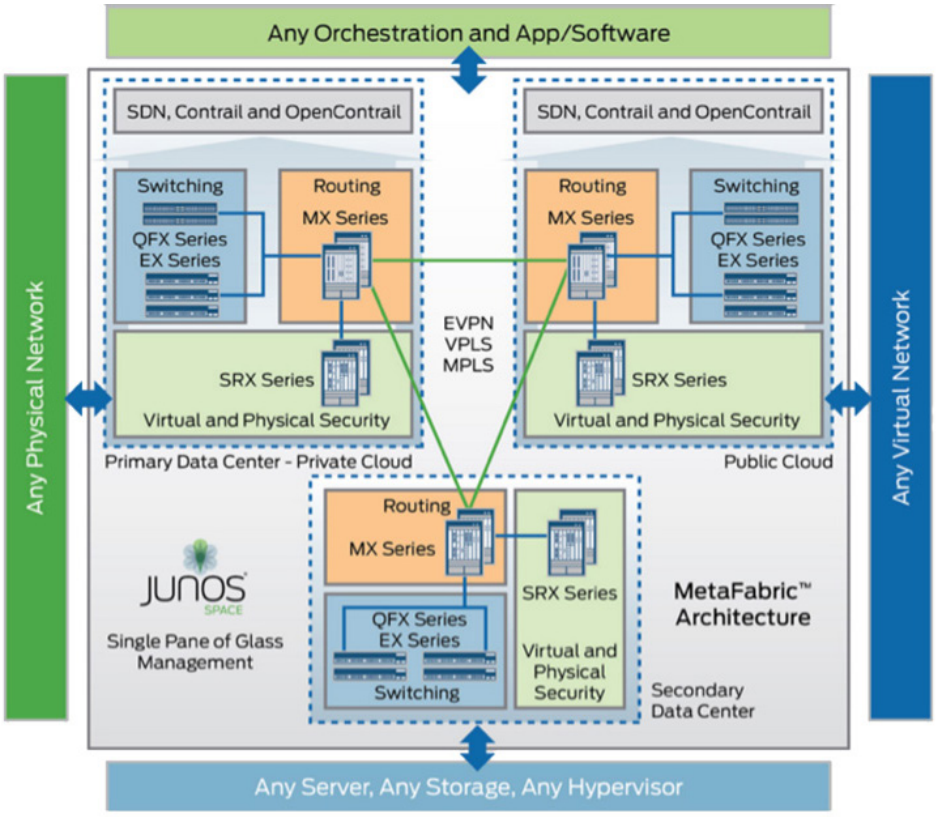


Рис. 1. Составные компоненты архитектуры MetaFabric

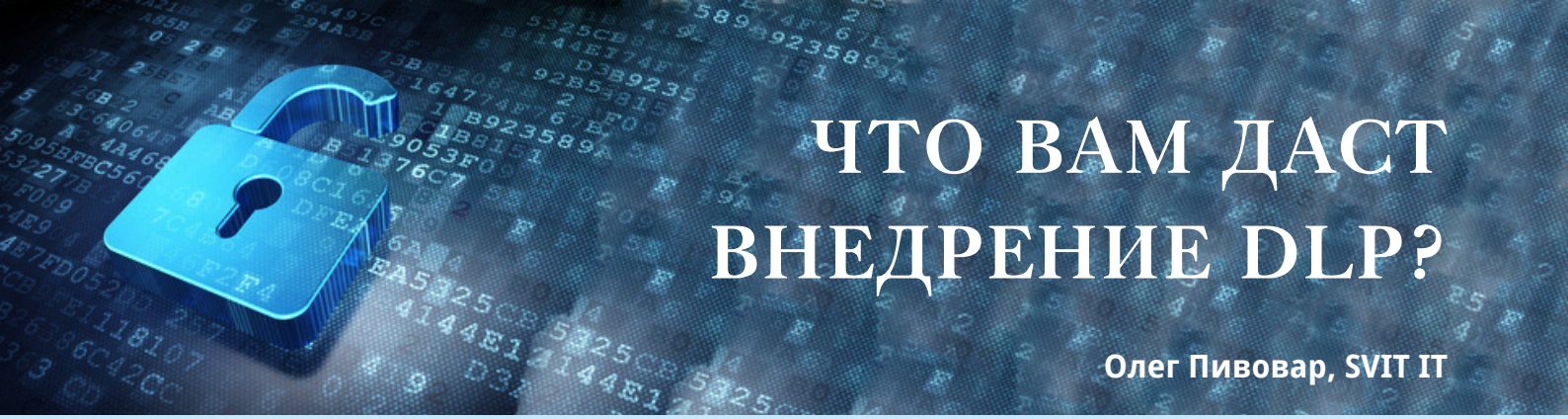
ЗАКЛЮЧЕНИЕ

В заключение можно сказать, что возможности архитектуры MetaFabric от компании Juniper можно считать практически безграничными и адаптируемыми для любых типов ЦОДа.

По мере внедрения коммутационных фабрик, технологий автоматизации, оркестровки и безопасности и программно-конфигурируемых сетей приложения ЦОДов будут требовать все большей гибкости и быстродействия.

Какие бы цели не преследовали современные организации, будь то совершенствование мобильных возможностей для пользователей, или решение проблемы больших данных посредством аналитики, или разработка гибких адаптивных облачных услуг, — архитектура MetaFabric станет надежной и эффективной инвестицией в будущее.

Компания ITbiz Solutions — официальный реселлер продуктов компании Juniper Networks — предлагает услуги внедрения и технического сопровождения проектов по построению ЦОДов на основе архитектуры Metafabric от Juniper. c4it



ЧТО ВАМ ДАСТ ВНЕДРЕНИЕ DLP?

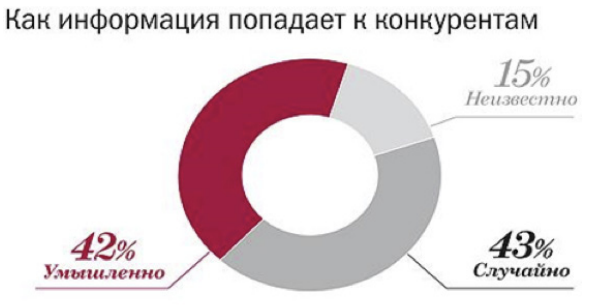
Олег Пивовар, SVIT IT

В нашем предыдущем выпуске, посвященном ИТ-безопасности, мы уже писали о DLP-системах. Мы решили вернуться к этой теме, так как в последнее время на украинском ИТ-рынке, несмотря на спад активности в целом, значительно вырос спрос на DLP. Сегодня мы поговорим о том, какие реальные преимущества может дать такое внедрение компании, которой необходимо защищать свои информационные активы.

Если мы проанализируем текущую экономико-политическую ситуацию в стране, то напрашивается довольно простой вывод: в условиях информационной войны понимание ценности конфиденциальной информации уже ни у кого не вызывает вопросов – и не только у ИТ-служб. У топ-менеджмента однозначно (по крайней мере, очень хочется в это верить) появилось понимание того, к чему может привести утечка данных. И несмотря на это, владельцы, инвесторы, руководители зачастую даже не представляют, как важная/секретная/суперсекретная бизнес-информация покидает их инфраструктуру и в каких объемах!

Давайте вспомним знаменитое высказывание братьев Натана и Якоба Ротшильдов: «Кто владеет информацией – тот владеет миром». И теперь представим обычный день «менеджера среднего звена» вашей компании. С каким объемом информации он работает каждый день? Почта: 10, 20, 100 писем? Общение в социальных сетях, форумах, профессиональных сообществах, финансовая документация, отчетность, поиск новой/лучшей работы и еще масса других действий.

А теперь самое интересное. Как вы думаете, исходя из модели рабочего дня «менеджера среднего звена», какое количество утечек конфиденциальной информации из вашей организации происходит по злому умыслу, а какое – по чистой случайности или же халатности?



Данную статистику предоставила компания Symantec – многолетний признанный лидер рынка решений DLP в мире. Начиная с 2006 года, Symantec, по оценке Gartner, уже 7 раз подряд является абсолютным лидером и продолжает удерживать свои позиции в области защиты от утечек и потери данных.

Какие две основные задачи должна ставить перед собой современная DLP-система?

Первая – выявление и предотвращение утечек конфиденциальной информации.

Вторая – ликбез для сотрудников компании.

Приоритетность данных задач вы можете определить сами!

Что же касается экономических выгод от внедрения DLP-системы в вашей организации, то на первый взгляд они не совсем очевидны. Внедряя DLP, компания инвестирует в человеческий, организационный и финансовый ресурс, соответственно, получая потенциальные финансовые выгоды за счет минимизации финансовых рисков, связанных с возможными утечками конфиденциальной информации. Кроме того, снижается нагрузка на подразделения ИТ и ИБ, что, в свою очередь, увеличивает эффективность работы сотрудников этих подразделений.

Наконец, при правильном построении процесса вокруг DLP происходит прозрачная и понятная интеграция подразделений, которые зарабатывают деньги, и подразделений, которые эти деньги защищают. Что, в свою очередь, влечет за собой повышение уровня безопасности на организационном и прикладном уровнях.

Это основные, но далеко не все выгоды, которые бизнес получает при внедрении DLP. А теперь о наболевшем: «безопасники» меня

обязательно поймут! Прямого возврата вложенных инвестиций при внедрении DLP нет, как, впрочем, и для большинства (а скорее, всех) продуктов в сфере информационной безопасности. Но все же неоспоримым остается тот факт, что лучше получать косвенные выгоды, чем покрывать финансовые и репутационные потери.

В заключение хочется сказать следующее: если вы (топ-менеджер, старший офицер безопасности, собственник бизнеса) видите и понимаете то, что есть необходимость в построении процессов ИБ на основе DLP, то данное решение нужно внедрять уже сейчас. Так как эта задача ложится не только на отдел информационной безопасности, а и на все отделы в компании, которые имеют доступ к конфиденциальной информации. Независимо от того, продукт какого вендора вы выберете, процесс внедрения DLP займет у вас в среднем от 8 до 12 месяцев. С4IT

Треть всех серверов, СХД и коммутаторов сейчас покупают для облачных ЦОДов

По подсчетам экспертов из IDC, в настоящее время для комплектации облачных ЦОДов приобретают «почти треть» всех реализуемых серверов, систем хранения и Ethernet-коммутаторов. По их оценке общий квартальный оборот мирового рынка аппаратного обеспечения для облачных серверных ферм по итогам июля-сентября 2014 года составил $ 6.5 млрд, что означает рост показателя на 16 процентов в годовом исчислении.

На ЦОДы, используемые для развертывания публичных облачных платформ, приходится около половины этой суммы. Остальные расходы пошли на модернизацию и расширение гибридных облачных платформ. Совокупный оборот мирового рынка аппаратного обеспечения для публичных облачных платформ в 2014 году составил около $13 млрд. Сейчас такие платформы обслуживают порядка 5% всех рабочих нагрузок. С4IT

EMC не хочет продавать VMware

EMC не собирается продавать свою долю в VMware, несмотря на сильное давление акционеров. Об этом заявил генеральный директор EMC Джо Туччи. По его словам: «Мы считаем, что наши возможности будут шире, а бизнес-модель эффективнее, если мы останемся единым целым. Мы нацелены на борьбу с крупнейшими компаниями рынка, такими как IBM. Я уверен, что мы получим больше преимуществ, находясь вместе».

Напомним, что EMC купила 80% акций VMware в 2003 году, заплатив за них около 635 млн долларов наличными. С тех пор неоднократно возникали слухи о приобретении оставшейся 20-процентной доли VMware основным акционером, подкрепляемые взаимными перестановками в высшем руководстве компаний. В 2014 году хедж-фонд Elliott Management, миноритарный акционер с примерно 2% акций EMC, заявил, что VMware нужно продать, так как после этого акции EMC могут заметно подорожать. Доподлинно неизвестно, до чего Туччи договорился с фондом. В октябре того же года возникли новые слухи о том, что обсуждается слияние EMC и Hewlett-Packard, однако оно якобы не произошло из-за финансовых разногласий. Туччи отказался комментировать и эту информацию.

В настоящее время EMC основывает бизнес на шести основных стратегических инициативах, прежде всего на облачных технологиях, Big Data и массивах хранения данных на основе флэш-памяти. С4IT

HP Cloudline: серверы для облачных сред

HP расширила портфолио серверных систем для облаков в сотрудничестве с Foxconn. Новая линейка HP Cloudline нацелена на гипермасштабируемые среды. Все новинки двухпроцессорные, выполнены в стоечных форматах и основаны на Intel Xeon E5 v3 Series. Модели CL7300 и CL7100 – для требовательных к дисковой подсистеме приложений, CL2200 (типоразмер 2U) – низшего ценового сегмента для приложений Big Data, CL2100 (1U) – сервер общего назначения; CL1100 – недорогой сервер для высокопроизводительных Front-End веб-приложений. С4IT

СИСТЕМЫ МОНИТОРИНГА ИНФРАСТРУКТУРЫ ЦОДа

Олег Иванин

ЦОД сегодняшнего дня – это сложный комплекс взаимосвязанных подсистем, каждая из которых должна не только гармонично взаимодействовать с остальными элементами инфраструктуры, но и быть надежной, отказоустойчивой и контролируемой. Для этого разработчики снабжают ЦОДы системами мониторинга технических параметров инфраструктуры.

Сегодня на рынке действуют разнообразные производители аппаратных и программных средств для построения систем мониторинга инженерной инфраструктуры ЦОДа, и в настоящей статье мы обзорно остановимся на практике построения такой системы, ориентируясь на следующие критерии:

1. Оптимальное решение с минимальными материальными затратами.
2. Простота систем визуализации.

В начале статьи назовем наиболее популярных на сегодня производителей систем мониторинга ЦОДа, чья продукция доступна в нашей стране.

APC (Schneider Electric)

Schneider Electric обладает развитым набором решений в сфере мониторинга, многие из которых попали в продуктовый набор после приобретения различных компаний. В частности, APC в свое время привнесла в портфолио Schneider Electric решения NetBotz и ISX Central, которые продолжили успешно развиваться.

В 2012 году все решения для мониторинга и автоматизации было решено объединить в рамках общего семейства StruxureWare, куда вошли решения всех бизнес-подразделений компании. Общее семейство подразделяется на отдельные направления, в частности, за мониторинг ЦОДа отвечает ПО StruxureWare for Data Centers, куда входят модули Data Center Expert и Data Center Operation.

StruxureWare DC Expert (ранее StruxureWare Central) — физическая основа системы мониторинга. Фактически, это стоечный 1-2-процессорный x86-сервер с предустановленной операционной системой и всем необходимым ПО, собирающий, обрабатывающий и хранящий всю информацию от внешних устройств, который вместе с тем предоставляет ее в удобном графическом виде администратору ЦОДа. DC Expert предлагается в трех основных модификациях — Basic, Standard и Enterprise, которые отличаются своими возможностями.

Благодаря поддержке протоколов SNMP и ModBus DC Expert может осуществлять мониторинг решений очень многих производителей (не только APC by SE). К DC Expert можно подключить ИБП, кондиционеры, щиты распределения питания, АВР, ДГУ, чиллеры и другие устройства, в том числе серверы и СХД. Также к серверу подключаются блоки системы мониторинга NetBotz, которую мы рассматриваем далее. Здесь отметим только, что она агрегирует данные от нескольких десятков внешних датчиков и видеокамер и может выступать в качестве самостоятельной системы мониторинга для небольших ЦОДов. В случае крупного объекта требуемое количество NetBotz управляется одним сервером DC Expert.

Не вдаваясь в подробности, кратко перечислим основные возможности этого программного комплекса. Например, StruxureWare Operation позволяет отображать данные на схеме физической компоновки устройств. Таким образом, сразу становится понятно, где установлено то или иное оборудование — в каком зале, шкафу, юните. В окне оператора отображается подробная информация обо всех подключенных устройствах. Также контролируются все операции с оборудованием ЦОДа. Обеспечивается графическое отображение отказов устройств на схеме компоновки стоек, а также фронтальный вид любой стойки. Система содержит калькулятор эффективности

использования электроэнергии (PUE), который предоставляет информацию по ежедневному потреблению.

Emerson и Avocent

Компания Emerson Network Power обладает широким набором различных решений для построения инженерной инфраструктуры ЦОДа. Здесь и кондиционеры, и холодильные машины, и системы распределения электропитания, и ИБП, и серверные шкафы, и многое другое. Но, чтобы подход был действительно комплексным, нужна развитая система мониторинга, которая бы позволяла контролировать все разнородное оборудование в ЦОДе, как производства Emerson, так и сторонних производителей.

На разных этапах развития программно-аппаратных средств вопрос решался по-разному. Например, создавались инструменты мониторинга для отдельных подсистем. В случае с кондиционерами, скажем, это решение iCOM — специальная плата, устанавливаемая в контролируемое устройство. До 32 таких внутренних карт могут объединяться с помощью концентратора и управляться из одной точки. Похожие решения есть и для ИБП. Однако Emerson в последние годы купила целую серию крупных компаний (Liebert, Knuerr, Chloride), чьи решения надо было интегрировать в общую концепцию с единым управлением. Логичным шагом в этом направлении стало приобретение в 2008 году компании Aperture — независимого разработчика ПО для систем мониторинга ЦОД, а в 2009-м — Avocent, признанного лидера в сфере комплексных аппаратных и программных систем мониторинга для ЦОДов. В результате портфолио Emerson пополнилось целой серией многофункциональных разработок для контроля и управления всеми подсистемами ЦОДа. Недавно все основные продукты в этом направлении были объединены в комплексную платформу под названием Trellis.

Основная проблема построения систем мониторинга инфраструктуры ЦОДа – это наличие в руках разработчика (системного интегратора) комплекта программно-аппаратных средств, полностью удовлетворяющего разнообразным требованиям к контролю набором своих функций и обязательно доступного по цене. Не всякий собственник может позволить себе строить ЦОД с нуля, при этом используя оборудование одного производителя. Практика построения систем мониторинга ЦОДа говорит, что в большинстве ЦОДов имеется набор разнородных решений, которые, хотя и объединены концептуально, все же обладают целой серией «идеологических» отличий, вызванных различными подходами производителей.

Важность удаленного наблюдения и управления отдельными устройствами понятна всем и реализуется всеми разработчиками ЦОДов. Для большинства активных компонентов ЦОДы в том или ином виде снабжаются средствами мониторинга. Однако в условиях крупного или даже среднего комплекса, где есть хотя бы несколько ИБП, кондиционеров, БРП, отслеживать работу каждого отдельного устройства неудобно, а совсем отказаться от мониторинга означает гарантированно получить проблемы с эксплуатацией инженерной инфраструктуры в ближайшем будущем.

ОПРЕДЕЛЯЕМ ОБЪЕКТ АВТОМАТИЗАЦИИ И МОНИТОРИНГА В ЦОД

Кратко перечислим основные составляющие инженерной инфраструктуры, что позволит нам систематизировать требования к системам мониторинга:

- Системы отопления и вентиляции.
- Системы кондиционирования.
- Системы электроснабжения (постоянного, резервного и бесперебойного).
- Дизель-генераторные электрические установки (ДГУ).
- Отдельно осуществляется мониторинг параметров окружающей среды в помещениях ЦОДа.

Какие же типовые требования к системам мониторинга инженерной инфраструктуры ЦОДа сегодня нужно учитывать разработчику систем мониторинга?

Разработчику необходимо предусмотреть в проекте систему мониторинга всех систем ЦОДа и основного оборудования ЦОДа. Также необходимо предоставить полное описание всех инженерных систем ЦОДа, значения аварийных сигналов и процедуры реагирования на них. Разработчику нужно предусмотреть систему контроля параметров окружающей среды в помещении ЦОДа. Система должна предупреждать эксплуатационный персонал при аварийном состоянии любого контролируемого параметра, выполнять дополнительное световое и звуковое оповещение охраны в случае поступления к мониторингу аварийного сигнала от любой из инженерных систем ЦОДа.

Конструктивно система должна включать три уровня: датчики для получения информации о контролируемых параметрах; контроллеры

для сбора, первичной обработки и регистрации собранной информации; средства передачи и отображения информации в виде, удобном для восприятия человеком.

Система должна обеспечивать передачу информации в цифровом виде, а также управляющих команд в пределах системы и на выходе из нее. Это должно быть реализовано с помощью сетевого стандарта Ethernet хотя бы по одному из следующих протоколов обмена данными – TCP\IP; SNMP; FTP; SMTP.

Верхний уровень системы – средства передачи и отображения информации – должен интегрироваться в локальную сеть ЦОДа. Для этого контроллеры системы должны аппаратно подключаться к структурированной кабельной системе (далее – СКС) ЦОДа. Доступ к информации о всех контролируемых и управляемых параметрах системы, а также управление элементами инфраструктуры ЦОДа должны выполняться с рабочего места системного администратора, а также быть доступными компьютерам в локальной сети ЦОДа через web-браузер с мобильных устройств.

Контроллеры системы, которые подключаются к локальной сети ЦОД, должны иметь web-интерфейс для возможности наладки режимов их работы. Необходимо предусмотреть рассылку сообщений в электронную почту и SMS-сообщений ответственным лицам заказчика согласно списка – ориентировочно это могут быть 20 человек. При этом необходимо учесть задержку в поступлении SMS-сообщения не более чем 2 минуты.

Система обязательно должна иметь средства разграничения прав доступа к информации о контролируемых и управляемых параметрах для любого пользователя локальной сети ЦОДа. Заказчику должен быть предоставлен список и расшифровки аварий оборудования, процедуры реагирования при возникновении аварийных ситуаций и при поступлении информации о состоянии оборудования. Сигнализацию при этом надо разделить на три группы с соответствующими процедурами реагирования:

- аварийные
- некритические сообщения
- информационные

ФУНКЦИИ СИСТЕМЫ МОНИТОРИНГА

Формирование тревог и обработка событий

Системе необходимо обеспечить гибкое управление событиями, включая фильтрацию событий, агрегацию, маскирование, корреляцию, подтверждение событий и анализ первопричин.

Должны быть предусмотрены настраиваемые тревоги, поддерживающие различные типы уведомлений (звук, всплывающие сообщения, электронная почта, SMS и т.д.).

При эскалации тревог должна предлагаться помощь. Правила настройки эскалации тревог должны быть гибкими, и необходимо обеспечить выполнение определенных действий с использованием привязок при возникновении тревог. Корректирующие действия могут управляться оператором или в неинтерактивном режиме, согласно ранее введенным пользователем настройкам.

Построение диаграмм и трендов

Диаграммы должны поддерживать различные типы, такие как непрерывные, столбцевые, круговые, а также динамическое обновление. Необходима поддержка автоматических трендов.

Генерация отчетов

Разумеется, система должна обладать эффективным средством генерации отчетов, поддерживающим любой редактор данных.

ПОСТРОЕНИЕ СИСТЕМ МОНИТОРИНГА

Проведя краткую систематизацию объекта автоматизации и мониторинга инженерной инфраструктуры ЦОДа, опишем подобную систему, с нашей точки зрения, являющуюся типовой.

Состав системы

Система мониторинга и диспетчеризации обеспечивает централизованный сбор информации о состоянии, параметрах и работе:

- ИБП.
- Кондиционеров.
- Шкафных блоков распределения питания.
- Системы мониторинга факторов окружающей среды в помещении ЦОД.
- Также система обеспечивает диспетчеризацию ДГУ и контроль состояния АВР и секционных переключателей.

Необходимо помнить, что состав, расположение и характеристики составляющих системы

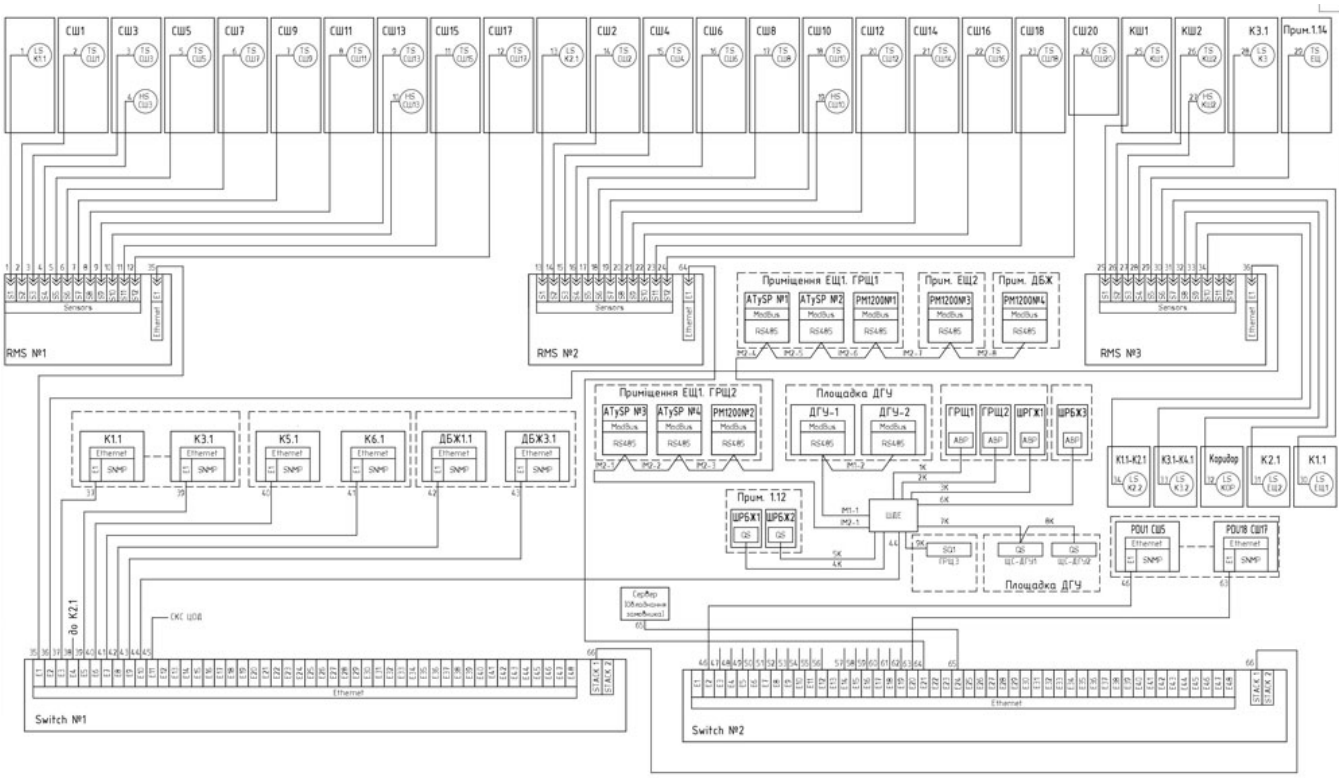


Рис. 1. Структурная схема типовой системы мониторинга ЦОД

всегда определяются в соответствии с требованиями заказчика и возможностью расширения системы в будущем.

Типовая система архитектурно включает в себя три уровня:

• Верхний уровень – центральный сервер (оборудование заказчика) для получения, обработки, архивирования, передачи и отображения информации в виде, удобном для восприятия человеком.
• Средний уровень – коммутаторы RMS Compact II (5 ед.) и шкаф диспетчеризации ШДЕ для сбора, первичной обработки и регистрации собранной информации.
• Нижний уровень – датчики температуры, влажности и затопления для получения информации о контролируемых параметрах, а также о подключенных к сети SNMP-устройствах со встроенными датчиками и контроллерах ДГУ.

В качестве основного оборудования для построения системы мониторинга используется продукция Emerson, которая выполнит функции сбора данных от систем кондиционирования, локального электроснабжения в зале ЦОД и микроклимата. ПО верхнего уровня выполнит функцию интегрирующей интерактивной оболочки для операторов.

С целью экономии средств в качестве систем сбора, рассылки сообщений и текущей визуализации используется оборудование компании ОВЕН, которое собирает и обрабатывает данные о состоянии системы электроснабжения ЦОД, расходах электроэнергии и тревожные сообщения о состоянии этих систем. Web-интерфейс этой системы интегрируется оболочкой программного обеспечения Emerson.

ТИПОВОЕ ТЕХНИЧЕСКОЕ РЕШЕНИЕ

Что мы используем из оборудования Emerson:

Рис. 2. Блок сопряжения датчика влажности воздуха Emerson

Рис. 3. Блок сбора и отображения данных RMS-2

Рис. 4. Тыльная панель подключения блоков RMS-2

Рис. 5. Лицевая панель блока RMS-2 для установки в шкаф

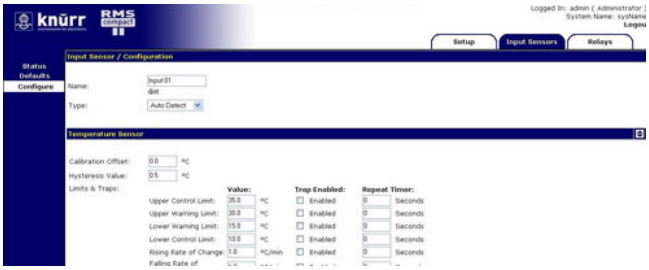


Рис. 6. Фрагмент экрана web-интерфейса конфигурации RMS-2 (англоязычный)

Рис. 7. Способ монтажа датчиков контроля открытия двери

Рис. 8. Пример монтажа датчика температуры воздуха

Рис. 9. Датчик затопления (наличия воды). Устанавливается в подполе, под кондиционерами

Система мониторинга и диспетчеризации серверного оборудования строится на базе программно-аппаратного комплекса Nform производства компании Emerson, что предусматривает возможность ее резервирования, в том числе на удаленных объектах, и аппаратного комплекса производства компании ОВЕН.

Также типовым проектом предусмотрено подключение к системе датчиков и блоков распределения питания (PDU), устанавливаемых в серверных шкафах. Система имеет средства разграничения прав доступа к информации о контролируемых параметрах для любого пользователя локальной сети объекта. В каждом серверном и коммутационном шкафу установлено по одному датчику температуры на передней стенке шкафа на высоте 1,5 м от фальшпола. В коммутационных и серверных шкафах устанавливаются датчики влажности на передней стенке шкафа на высоте 1,2 м от фальшпола. Датчики затопления располагаются на полу помещения машинного зала под каждым блоком кондиционеров PX051DA и HPS10 в помещении ЦОД, под конденсатосборниками и дренажными приямками.

Датчики температуры, влажности и затопления подключаются к коммутаторам RMS Compact II, расположенным в коммутационном шкафу и серверных шкафах. В сеть Ethernet-объекта с помощью сетевых коммутаторов подключаются коммутаторы RMS Compact II, ИБП, кондиционеры и шкафные блоки шкафов распределения питания (PDU). Кондиционеры, ИБП и PDU подключаются к сети Ethernet посредством SNMP-карт мониторинга. В серверном шкафу устанавливается центральный сервер системы диспетчеризации с установленным ПО Nform 4.0 Standard Edition. Сервер соответствует требованиям ПО NForm 4.0 Standard Edition и соединен с подключенными к сети SNMP-устройствами и внешней сетью Ethernet через коммутатор. Решение предусматривает диспетчеризацию с использованием контроллера ПЛК323 про-

изводства компании ОВЕН, который устанавливается в шкафу диспетчеризации системы электроснабжения. Подключение контроллеров ДГУ к ПЛК323 происходит по протоколу Modbus RTU (интерфейс RS-485).

Рис. 10. Анализаторы параметров электрической сети Schneider Electric PM 1000 (Modbus)

Проектом предусмотрен мониторинг состояния АВР и секционных переключателей, устанавливаемых в ГРЩ, ШРГЖ и ЩК-ДГУ с использованием контроллера ПЛК323 и модулей дискретных входов МВ110-16д производства компании ОВЕН, устанавливаемых в шкафу диспетчеризации системы электроснабжения. Подключение модулей МВ110-16д на карте к ПЛК323 происходит по протоколу Modbus RTU (интерфейс RS-485). Для передачи аварийных сигналов по сети GSM используется контроллер ПЛК323 со встроенным GSM-модемом.

Рис. 11. АВР управления электрическими вводами, контроль по сети Modbus

Рис. 12. Контроллер сбора и обработки информации о состоянии системы электроснабжения. ПЛК-323 ОВЕН

Рис. 13. Устройство удаленного ввода дискретных сигналов ОВЕН МВ110-16Д (Modbus)

ОПИСАНИЕ ФУНКЦИОНИРОВАНИЯ

Система работает в непрерывном режиме, обеспечивая возможность сбора и представления эксплуатационному персоналу информации о состоянии параметров и исправности элементов инженерной инфраструктуры серверного помещения, включая подсистемы энергоснабжения, бесперебойного питания, подсистему кондиционирования и состояние окружающей среды.

Система обеспечивает передачу сигналов мониторинга и управляющих команд в пределах системы (между сервером системы, коммутаторами, кондиционерами, UPS и PDU) и их передачу конечному пользователю с помощью сетевого стандарта Ethernet по протоколам обмена данными – SNMP, SMTP.

Средства передачи и отображения информации верхнего уровня системы диспетчеризации подключаются к локальной сети объекта. Система мониторинга и диспетчеризации предусматривает предупреждение эксплуатационного персонала при аварийном состоянии любого из контролируемых параметров. Проектом предусмотрена светозвуковая сигнализация на мониторе АРМ при аварийном состоянии любого из контролируемых параметров.

Доступ к информации о всех контролируемых параметрах системы и к управлению элементами инфраструктуры ЦОД выполняется с рабочего места системного администратора, а также из доступных компьютеров в локальной сети ЦОД, через web-браузер с мобильных устройств.

Контроллеры системы имеют web-интерфейс для возможности наладки режимов их работы. Проектом предусмотрена возможность рассылки сообщений на электронную почту и SMS-сообщений ответственным сотрудникам. Проектом предусмотрена рассылка SMS-со-

общений на 20 номеров. Данные об отправке сообщений архивируются в базе данных контроллера с возможностью последующего просмотра архива.

пользователя определяется заказчиком на этапе внедрения системы.

ОСОБЕННОСТИ ЭЛЕКТРОПИТАНИЯ И КАБЕЛЬНАЯ СЕТЬ

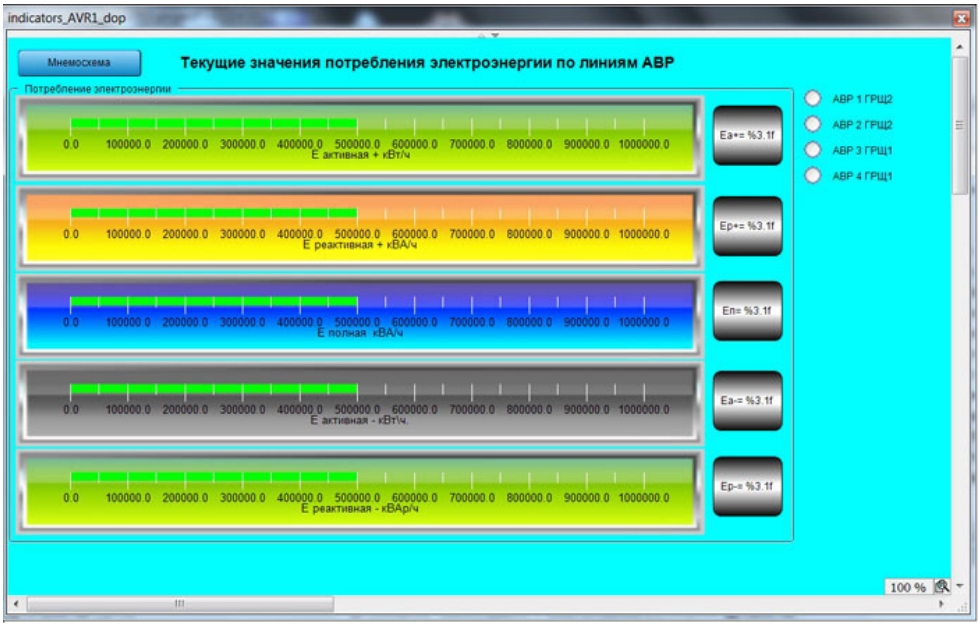


Рис. 14. Система визуализации web ПЛК 323 ОВЕН

Электропитание системы мониторинга и диспетчеризации обеспечиваются бесперебойным электропитанием. Кабельную сеть системы желательно строить по «шинной» топологии, в рамках кабельной информационной сети.

Передача информации по кабельной сети системы происходит на основе открытых стандартных протоколов типа Ethernet, SNMP. Все кабельные трассы прокладываются по металлическим лоткам.

Система обеспечивает диспетчеризацию дизель-генераторных установок и контроль наличия напряжения после АВР, установленных в ГРЩ, ЩРГЖ и ЩС-ДГУ.

Доступ к информации контролируемых параметров системы и управления элементами инфраструктуры выполняется с рабочего места системного администратора или с помощью web-интерфейса с компьютеров, подключенных к сети Ethernet предприятия.

Система имеет средства разграничения прав доступа к информации и параметров для любого пользователя локальной сети с использованием индивидуальных паролей и логинов. Уровень доступа к информации для каждого

Рис. 15. Скриншот экранов построения гистограмм электрической нагрузки секций ЦОД

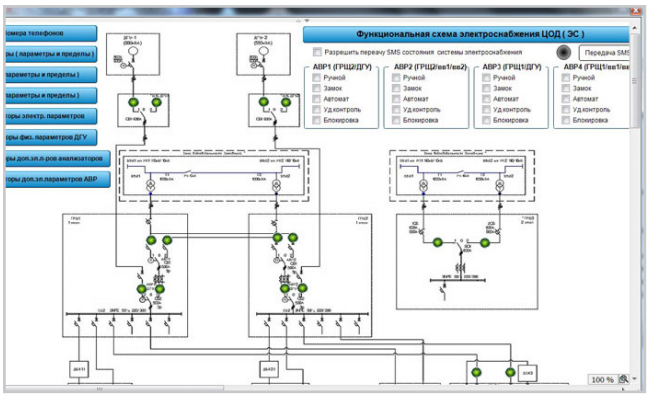


Рис. 16. Скриншот web-интерфейса системы контроля системы электроснабжения

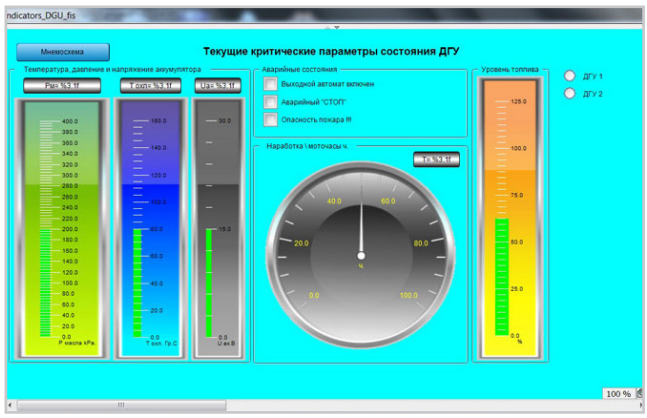


Рис. 17. Экранная форма системы контроля состояния ДГУ

Рис. 18. Экранная форма системы контроля электроснабжения с помощью анализаторов электрической сети

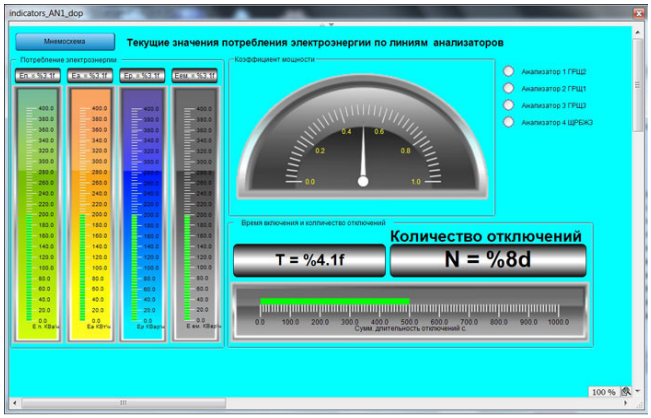


Рис. 19. Экранная форма контроля параметров ДГУ

Использованное оборудование:

1. Устройство контроля параметров среды RSM Compact II (Emerson)
2. Датчик температуры RMS Temperature Sensor (Emerson)
3. Датчик влажности RMS Humidity Sensor (Emerson)
4. Датчик воды RMS Water Sensor (Emerson)
5. Модуль Volition RJ45 K5e Jack, Cat 5e, UTP, white (Emerson)
6. Программное обеспечение Nform 4.0 Standard Edition (Emerson)
7. Лицензия для нескольких устройств ПО NForm 4.0 (Emerson)
8. Шкаф диспетчеризации (ОВЕН)

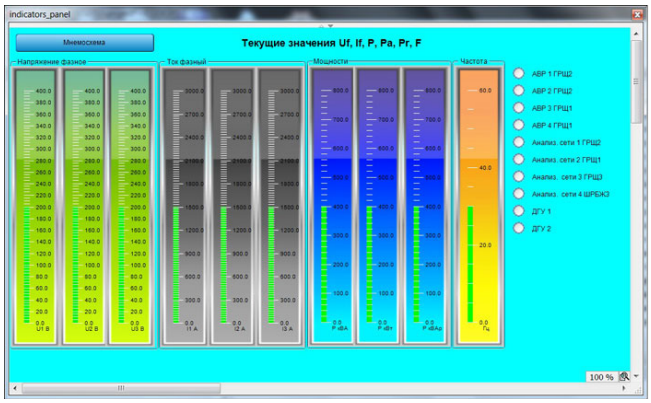


Рис. 20. Панель сводных индикаторов состояния электрической сети

ЗАКЛЮЧЕНИЕ

В заключение хочется отметить, что при всей свободе и всем разнообразии инструментария и программно-аппаратных средств при построении систем мониторинга необходимо находить оптимальное сочетание:
1. Качественных аппаратных средств. В качестве средств контроля состояния серверных шкафов и зала ЦОДа желательно приобретать аппаратуру и программное обеспечение ведущих производителей (SE, Emerson и т.д.). Эта аппаратура обеспечивает надежные способы сбора и отображения параметров работы и состояния серверных шкафов и микроклимата в помещении ЦОД. Также она обладает дружелюбными и свободно конфигурируемыми интерфейсами пользователей.
2. Гибких, более дешевых по сравнению с ведущими вендорами, но функциональных и надежных средств диспетчеризации и мониторинга инженерной инфраструктуры.
3. Простых в конфигурации и настройке средств отображения информации, рассылки информационных сообщений. Это могут быть как базовые средства SCADA, так и основные оболочки, поставляемые ведущими производителями систем мониторинга ЦОД. С4IT

HP и Emerson сотрудничают в сегменте DCIM

Emerson Network Power расширяет возможности ПО для управления инфраструктурой центров обработки данных Trellis Data Center Management через партнерство с HP. Совместный проект предполагает объединение функционала Trellis в области управления инфраструктурой ЦОД с возможностями консалтинговых сервисов HP в области управления ЦОДами, которые имеют название Converged Management. Они являются основой для интеграции DCIM-решений с ITSM-платформами. В итоге специалисты по управлению ИТ-инфраструктуры ЦОДов получат лучшее понимание рационального использования свободного пространства, повышения эффективности систем электроснабжения и охлаждения. С4IT

БЕЗОПАСНОСТЬ ТРАДИЦИОННЫХ И ВИРТУАЛИЗИРОВАННЫХ ЦОДов С БРАНДМАУЭРАМИ НОВОГО ПОКОЛЕНИЯ

По материалам Группы компаний БАКОТЕК

Виртуализация помогает компаниям использовать аппаратную инфраструктуру ЦОДа более эффективно, что позволяет достигнуть снижения затрат и улучшения операционной эффективности. В большинстве случаев инициативы виртуализации берут свое начало изнутри, в собственной аппаратной и сетевой инфраструктуре, дополненной инструментами, такими как VMware или KVM и OpenStack для управления виртуализированной средой.

КРАТКИЙ ОБЗОР

Популярное сейчас частное облако – это проект, который нуждается в расширении в так называемое общедоступное (публичное) облако, которое представляет собой использование «встроенных» инфраструктур, например, Amazon Web Services (AWS), что позволяет подписаться или платить за вычислительные, сетевые сервисы, а также услуги хранения по мере их необходимости. Преимущество данной модели в том, что она позволяет снизить объем управленческих работ, совокупные капиталовложения, а также позволяет быстро реагировать на изменение или рост потребностей. Подтверждающие доказательства этого таковы:

- по оценкам Gartner, почти 50% всех серверных ИТ-активов x86 виртуализированы, но ожидается, что это цифра вырастет до 77% в 2015 году;
- технология облачных вычислений быстро развивается, ведь сегодня 64% ИТ-директоров рассматривают ее как важнейший элемент для их бизнеса, а это более чем в два раза выше, чем в 2009 году;
- 67% опрошенных IBM ИТ-директоров активно изучают, как облачные технологии могут быть полезны для их пользователей;
- к 2017 году примерно $217 млрд долларов будут потрачены на технологии облачных вычислений, и эта сумма почти в три раза больше затрат в 2014 году, а именно, $75 млрд.

В большинстве случаев физический ЦОД не исчезнет, вместо этого он будет развиваться – это и есть гибридный метод, где сочетаются физические и частные или публичные технологии облачных вычислений. Этот процесс уже запущен, и так же, как большинство сталкивается с проблемой защиты физических ЦОДов, похожие проблемы будут возникать в среде облачных вычислений.

Недавние громкие атаки на личные данные показали, что киберугрозы будут скрываться за общими приложениями для обхода контроля, затем, когда попадут в сеть, двигаясь с небольшим сопротивлением, вообще пропадают из вида. После того как их цель обнаружена, они выводят ее наружу либо через известные приложения, такие как FTP, или через зашифрованные, такие как SSL. Виртуализированная среда менее защищена от нарушений безопасности, чем физический ЦОД. Все потому, что ИТ-активы, некоторые из которых используют разные уровни доверия, и связанные с ними данные – централизованы, без каких-либо защитных барьеров между ними, и не смогут делиться на сегменты.

Если виртуальная среда находится под угрозой, злоумышленник имеет доступ ко всему объему данных. Дополнительной проблемой для обеспечения безопасности ИТ-активов ЦОДа является тот факт, что политика безопасности и соответствующие обновления не могут идти в ногу со скоростью изменений рабочих мощностей (VM), в результате чего ослабевают средства безопасности.

В этом техническом документе описываются основные проблемы обеспечения безопасности ЦОДа и среды облачных вычислений, а также объясняется, как решить эти проблемы брандмауэром нового поколения.

ИЗМЕНЕНИЕ ХАРАКТЕРИСТИК ЦОДов

Сейчас ЦОДы стремительно развиваются от традиционного, замкнутого пространства со статическими, аппаратными вычислительными ресурсами к гибриду традиционных и

облачных технологий вычислений. Преимуществом перехода к такой модели облачных вычислений является то, что она улучшает эффективность работы и снижает капитальные затраты для организации:

• Оптимизация существующих аппаратных ресурсов: вместо модели «один сервер – одно приложение» несколько виртуальных приложений можно запустить на одном физическом сервере. Это означает, что организации могут использовать существующую аппаратную инфраструктуру, запустив несколько приложений в рамках одной системы.
• Сокращение затрат на удержание ЦОДа: уменьшение количества серверного оборудования не только сокращает физическую инфраструктуру, но также снижает затраты на электропитание, охлаждение и пространство в стойке.
• Увеличение эксплуатационной гибкости: благодаря динамическому характеру резервов виртуальных машин приложения могут быть предоставлены быстрее, чем при традиционном методе их реализации. Это помогает улучшить гибкость ИТ-организации.

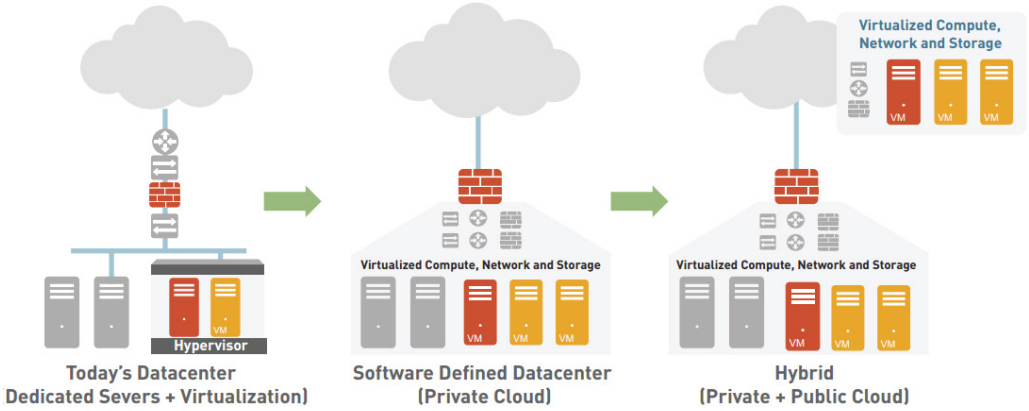


Рис.1. ЦОД – комбинация из аппаратных и облачных технологий

• Максимизация эффективности ресурсов ЦОДов: поскольку приложения могут испытать нагрузки асинхронного или пакетного спроса, виртуализация обеспечивает более эффективный способ для решения вопросов конкуренции за ресурсы, а также помогает максимизировать эффективность использования серверов. Также это лучший способ для обслуживания серверов и резервного копирования задач.

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ ЗАВИСЯТ ОТ ВИРТУАЛИЗАЦИИ

Облачные вычисления, в отличие от распространенных заблуждений, не место, а, скорее, пул ресурсов, которые могут автоматически и быстро перемещаться предусмотренным методом. Американский Национальный институт стандартов и технологий (NIST) дает следующее определение облачным вычислениям в специальной публикации 800-145: информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, ЦОДам, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру. Потребители облачных вычислений могут значительно уменьшить расходы на ИТ-инфраструктуру и гибко реагировать на изменения вычислительных потребностей, используя свойства вычислительной эластичности облачных услуг. Это верно как для частных, так и для публичных облаков. Вместо множества независимых и часто недостаточно используемых серверов, развернутых для бизнеса, пулы ресурсов агрегируются, объединяются и разрабатываются, чтобы быть достаточно эластичными и масштабироваться вместе с потребностями бизнес-запросов.

Переход к облачным вычислениям не только сокращает эксплуатационные затраты, но также имеет технологические преимущества. Данные и приложения легко доступны для пользователей, независимо от того, где они проживают, проекты могут легко масштабироваться, а потребление трафика отслеживается эффективнее. Виртуализация является важной частью облачной вычислительной архитектуры, что в сочетании с программным обеспечением и инструментами управления позволит склеивать разнородные процессы бесшовным способом, так, что они могут быть автоматизированы, легко воспроизводиться и запрашиваться по мере необходимости.

МЕРЫ ПРЕДОСТОРОЖНОСТИ И ТРЕБОВАНИЯ К ОБЛАЧНЫМ ВЫЧИСЛЕНИЯМ

С технологиями облачных вычислений среда ЦОДов может эволюционировать от фикси-

рованной, где приложения выполняются на выделенных серверах, в динамичную и автоматизированную среду, где пулы вычислительных ресурсов доступны для поддержки ИТ-активов и приложений, которые могут быть доступны в любом месте, в любое время, с любого устройства.

Безопасность по-прежнему остается серьезной проблемой, если вы приняли новую динамичную среду облачных вычислений. Многие из принципов, которые делают облачные вычисления привлекательными, идут вразрез с наилучшими практиками сетевой безопасности:

• Облачные вычисления не уменьшают существующие риски для безопасности сети. Риски безопасности, которые угрожают сети сегодня, не уменьшаются при переходе на облако. В некотором смысле, при переходе на облако риски даже увеличиваются. Многие приложения для ЦОДов используют широкий диапазон портов, что делает традиционную безопасность неэффективной. Киберпреступники организуют сложные, независимые от порта атаки, которые используют несколько векторов для достижения своих целей, и, чтобы скрыться с виду, используют наиболее часто применимые приложения.
• Безопасность требует разделения и сегментации – облако опирается на общие ресурсы. Лучшие меры обеспечения безопасности диктуют, чтобы критически важные приложения и данные были разделены на безопасные сегменты в сети с использованием принципа Zero Trust («нулевого доверия»), что означает: доверяй, но проверяй. В физической сети принцип Zero Trust является относительно простым для выполнения с помощью брандмауэров и политики, основанной на идентификационных данных пользователя. В среде облачных вычислений в сервере постоянно происходит прямая связь между виртуальными машинами, что в случаях с низким уровнем доверия делает сегментацию трудной задачей.
• Развертка системы безопасности, ориентированная на процесс – среда облачного вычисления является динамичной. Создание или изменение виртуальных ИТ-активов часто может быть сделано в течение нескольких минут, в то время как настройка безопасности для этой рабочей нагрузки может занимать несколько часов, дней или недель. Задержки безопасности не целенаправленны, они являются результатом процесса, который предназначен для поддержания высокого уровня безопасности. Изменения политики должны быть утверждены, соответствующие брандмауэры – идентифицированы, а соответствующие обновления политики – определены.

В отличие от этого, команды виртуализации работают в динамичной среде, ИТ-активы добавляются, удаляются и изменяются динамическим образом. Как результат – несоответствие между политикой безопасности и разверткой виртуализированных ИТ-активов, а также ослабление уровня безопасности.

Поскольку организация использует облако, то отделы сетей, безопасности и виртуализации имеют два варианта, когда речь заходит о защите критически важных приложений и данных от современных киберугроз. Первый вариант заключается в игнорировании безопасности не потому, что она не нужна, а потому, что поддержание политик безопасности в актуальном состоянии не может идти в ногу со скоростью перемен в облаке. Второй вариант заключается в реализации традиционных технологий сетевой безопасности, базирующихся на контроле портов, что означает, что они не могут контролировать приложения и неэффективны для блокировки современных атак. Ни один из этих вариантов не решает критически важные задачи, которые необходимы для защиты облачных сред. Основные требования для обеспечения безопасности облака включают в себя:

• Последовательную безопасность в физических и виртуальных форм-факторах. Для контроля приложений и предотвращения угроз должны использоваться одинаковые уровни защиты как для среды облачных вычислений, так и для физической сети. Во-первых, нужно подтвердить подлинность приложений ЦОДа, проверить их достоверность и заставить использовать только свои стандартные порты. Нужно также блокировать вредоносные приложения от доступа к ЦОДу и одновременно искать и блокировать неправильно сконфигурированные приложения. Наконец, специальную политику в области предупреждения угроз нужно применять, чтобы блокировать как известные, так и неизвестные вредоносные программы от перемещения в и через ЦОД.
• Сегментацию бизнес-приложений, используя принципы Zero Trust («нулевого доверия»). Для того чтобы максимизировать использование вычислительных ресурсов в полном объеме, теперь достаточно распространенной практики смешивания разных уровней доверия ИТ-активов, приложений на одном вычислительном ресурсе. В то время как это эффективно на практике, смешанные уровни доверия больше угрожают безопасности при несанкционированном вторжении снаружи. Решения для безопасности в облаке должны реализовывать политику безопасности, основанную на принципе Zero Trust, как основной

контроллер трафика между ИТ-активами для предотвращения «бокового» передвижения угроз.
• Централизованное управление разверткой безопасности; рационализация обновлений политики. Физическая безопасность сети все еще реализуется в каждой организации, и это очень важно, так как есть возможность управлять этим как аппаратно, так и развертывать виртуальные форм-факторы из централизованного места, используя одну и ту же инфраструктуру управления и интерфейс. Gartner выступает в пользу поставщиков систем безопасности, которые охватывают физические и виртуальные среды с постоянной политикой управления. Чтобы обеспечить высокий уровень безопасности, нужно не отставать от скорости изменения ИТ-активов, то есть решения, связанные с безопасностью, должны включать в себя функции, которые уменьшат количество, а в некоторых случаях и полностью устранят ручную обработку данных, которую зачастую требуют обновления политики безопасности.

СУЩЕСТВУЮЩИЕ НЕДОСТАТКИ БЕЗОПАСНОСТИ ЦОДов

Существующие решения безопасности ЦОДов имеют те же недостатки, что и шлюзовые решения на периметре физической сети – это управление трафиком, на основе контроля портов «statefull inspection», после чего следует ряд последовательных операций (IPS, URL filtering). У этого подхода есть серьезные недостатки:

• Первичные порты ограничивают видимость и контроль. Сфокусированность на первичных портах ограничивает способность видеть весь трафик на всех остальных портах, а это означает, что неопределенные или зашифрованные приложения и любые соответствующие угрозы, которые могут или не могут использовать стандартные порты, имеют шанс проскользнуть незамеченными. Например, многие приложения ЦОДов, такие как Microsoft Lync, Active Directory и SharePoint используют широкий спектр смежных портов для правильной работы. Это означает, что нужно открыть все эти первичные порты, подвергая их воздействию других приложений или киберугроз.
• Недостаток информации о неизвестном трафике. Неизвестный трафик составляет около 20% в любой сети. Неизвестный трафик может быть пользовательским приложением, неизвестным коммерческим приложением или угрозой. Блокирование всего этого принесет вред бизнесу, а разрешение – большой риск. Приходится систематически управлять неизвестным трафиком с помощью встроенных средств управления политиками, таким образом снижая свои риски для безопасности.
• Многокомпонентная политика – политика неприменения инструментов. Последовательный анализ трафика (контроль портов «statefull inspection», контроль приложений, IPS, AV и т.д.) требует соответствующей политики безопасности или профиль, чаще всего с использованием нескольких инструментов управления. Результат политики безопасности будет запутанным, так как происходит создание и управление политикой брандмауэра с исходными, целевыми, пользовательскими правилами, политикой контроля приложений в дополнение к другим правилам предотвращения угроз. Надежность многокомпонентной политики заключается в том, что тут сочетаются положительная (брандмауэр) и негативная (контроль приложений, IPS, AV) модели управления, без каких-либо инструментов согласования политик, дыр в безопасности или неустановленного трафика.
• Затруднительный процесс обновления безопасности. Наконец, существующие решения обеспечения безопасности не учитывают динамичный характер облачной среды и не могут адекватно отслеживать политику дополнений, удалений или изменений данных в виртуальной машине.

Многие предложения по облачной безопасности – это просто виртуализированные версии безопасности, типа порт-протокол, и имеют такие же недостатки, что и их физические аналоги.

БЕЗОПАСНОСТЬ ЦОДа С PALO ALTO NETWORKS

Palo Alto Networks позволяет защитить ЦОД, будь то физический или облачный, используя согласованный набор брандмауэра нового поколения и дополнительных функций предотвращения угроз, развертываемых в любом физическом устройстве или виртуальной среде. Инструменты управления помогут упростить реализацию политики и устранить временный зазор, который возникает между разверткой виртуальных ИТ-активов и обновлением политики безопасности, что позволяет работать на скорости облака.

ДОВЕРЕННОЕ ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ В ЦОДе ПО ПРИНЦИПУ ZERO TRUST

Часто вопрос о том, является ли управление приложениями приемлемым в ЦОДе, возникает из-за ограниченного числа известных приложений, которые обычно используются.

Теория заключается в том, что мы знаем, какие приложения используются в ЦОДах, поэтому можем легко обеспечить их безопасность. Но реальность такова, что несколько последних громких взломов частных данных показали, что злоумышленники будут использовать приложения, которые обычно встречаются в сети, чтобы реализовать свои атаки и извлечь данные. Некоторые примеры:

- В докладе iSight Partners по объектам нападения FTP, Netbios и Webdav говорится о приложениях, которые используются злоумышленниками для навигации по сети, в то время как на самом деле они используются для кражи данных кредитных карт и личных данных пользователей. Это пример того, как злоумышленники скрываются с виду, используя общие приложения. С помощью Palo Alto Networks 2014 Application Usage and Threat Report такие приложения были найдены в каждой из 5500 сетей, проанализированных нами.
- RDP и другие средства удаленного доступа, как известно, используются злоумышленниками для навигации по сети, о чем свидетельствует годовой «Отчет о нарушении данных» Verizon. Согласно 2014 Application Usage and Threat Report, в среднем девять инструментов удаленного доступа находятся в пользовании 90% сетей, которые мы анализируем.
- Многие бизнес-приложения, такие как Microsoft Lync, SharePoint и Active Directory, используют порты 80,443 и широчайший ряд других портов, что делает невозможным решение такой задачи, к примеру, как дать возможность Lync использовать необходимые порты, а другим приложениям запретить.
- В среднем происхождение 8-10% трафика неизвестно: это может быть внутреннее применение; неопределенное коммерческое приложение, готовое к использованию; или же угроза. Критическая функциональность, которая нужна, – это способность систематически контролировать неизвестный трафик, быстро анализировать неизвестные, определяя, что это, где это и откуда, управлять с помощью политики пользовательских приложений или профилей предотвращения угроз.

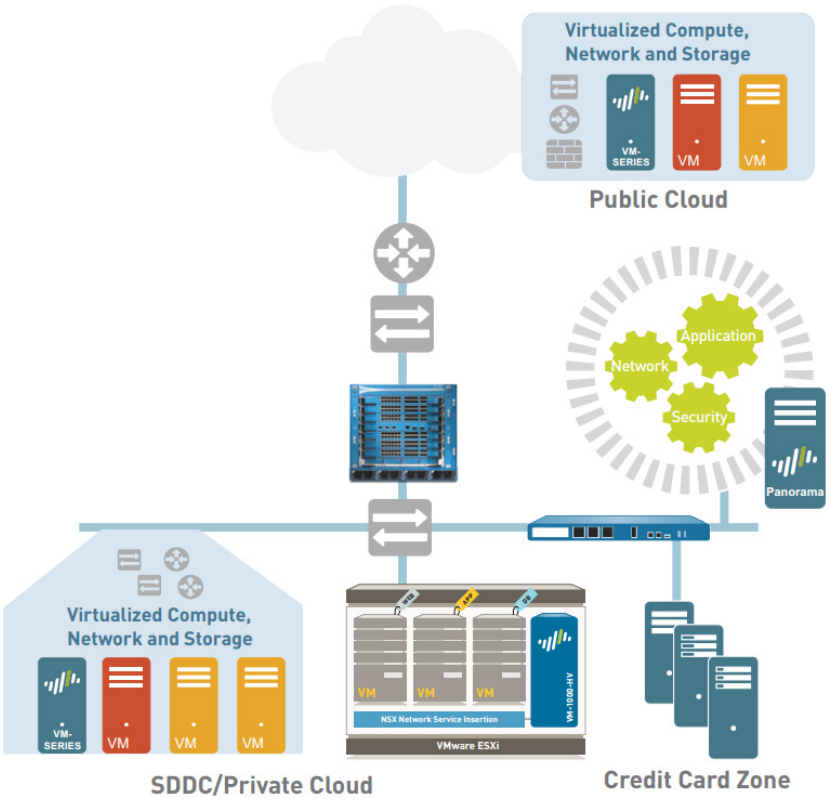


Рис. 2. Защита традиционных ЦОД, облачных приложений и данных с помощью решений Palo Alto Networks

В каждом из приведенных выше примеров наши брандмауэры позволяют реализовать политику безопасности, основанную на принципах Zero Trust, в результате чего уровень безопасности повышается. Концепция Zero Trust расширяет практику сегментации сети на уровне предоставления доступа на основе определенных приложений, обеспечивая пользователю доступ в рамках своих полномочий. Контролируется передача контента между узлами сегментации. Доверяй, но проверяй.

- Подтвердите, что SharePoint используется, находясь над своими стандартными портами, и косвенно блокирует все остальные приложения от использования.
- Предоставьте доступ к клиентскому веб-интерфейсу для SharePoint для определенного набора портов и применения конкретных стратегий профилактики угроз.
- Ограничьте доступ к базе данных Microsoft SQL для самого приложения SharePoint, косвенно блокируя клиентский веб-интерфейс от подсоединения к базе данных.
- Разрешите отделам маркетинга, в зависимости от их членства в группах, подключать только SharePoint Docs и никакие другие функции. Включите только ИТ-группу для использования SharePoint Admin во время диагностики трафика, используя специальное приложение политики предотвращения угроз.
- Идентифицируйте и блокируйте неправиль-

ные или вредоносные приложения, такие как RDP или TeamViewer, используя запрет всего иного доступа к потоку брандмауэра или блокировку их политикой.

СИСТЕМАТИЧЕСКОЕ УПРАВЛЕНИЕ НЕИЗВЕСТНЫМ ТРАФИКОМ ПОСРЕДСТВОМ ПОЛИТИКИ

Создание пользовательского App-ID для внутренних приложений позволяет контролировать доступ в зависимости от пользователя, проверять их на наличие известных и неизвестных вредоносных программ: неопознанные, коммерческие приложения могут быть заблокированы в соответствии с политикой или получить App-ID; наконец, инструменты экспертизы и отчетности могут помочь устранить неизвестный трафик, возможно связанный с угрозой. Практика обеспечения безопасности ЦОДа, основанная на принципах Zero Trust, применяется к традиционным ЦОДам и средам облачных вычислений, что позволяет контролировать доступ, на основе применения или вычисления ресурсов ИТ-активов, идентифицировать пользователей, блокируя потенциальных «изгоев» или неправильные приложения, а также предотвращать угрозы ЦОДам и их перемещение в «боковом» направлении.

БЛОКИРОВАНИЕ ВСЕХ ИЗВЕСТНЫХ И НЕИЗВЕСТНЫХ, ВХОДЯЩИХ ИЛИ СКВОЗНЫХ КИБЕРУГРОЗ

Сегодняшние киберугрозы обычно компрометируют сеть посредством действий на ничего не подозревающего работника: вредоносные ссылки, загрузка зараженного файла или любой из многих других способов. После того как эти инструменты атаки попадут в сеть, они будут двигаться по ней в поисках цели. В ЦОДе киберугрозы могут потенциально двигаться «поперек» ваших физических или виртуальных ИТ-активов, подвергая критически важные приложения и данные опасности. Ключевым фактором защиты ЦОДов является реализация методов профилактики (см. рис 3).

Контроль приложений между ИТ-активами снижает влияние угрозы и одновременно сегментирует трафик ЦОДа на основе принципа Zero Trust. Конкретные стратегии профилактики угрозы могут предотвратить известные и неизвестные угрозы и уберечь ЦОДы.

СОКРАЩЕНИЕ РАСХОДОВ НА УПРАВЛЕНИЕ

Необходимость в продолжении эксплуатации физической сети в сочетании с необходимостью эксплуатации облака означает, что сценарий развертки только нескольких брандмауэров редко встретишь. Сведение к минимуму расходов на управление и ускорение развертывания в сочетании централизованного управления и встроенных функций, которые могут помочь упорядочить обновления политики, становится необходимостью.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Panorama позволяет централизованно управлять всеми своими брандмауэрами нового поколения Palo Alto Networks, как физическими, так и виртуальными, тем самым обеспечивая согласованность и целостность политики. Используя тот же внешний вид, что и индивидуальное устройство управления интерфейсом, Panorama исключает кривую обучения, связанную с переходом от одного пользовательского интерфейса на другой. Panorama позволяет управлять всеми аспектами брандмауэра Palo Alto Networks, в том числе:

- Развертыванием политик безопасности, NAT, QoS, policy based forwarding, расшифровку SSL, портала авторизации “captive portal” и защиту от DoS.
- Политиками общего использования, которые используют пре- и пост-правила, развертываемые администратором Panorama. Позволяют редактировать политику локально. Правила, которые находятся между правилами пре- и пост-, могут быть отредактированы как локально, так и администратором Panorama.
- Программным обеспечением и обновлением содержимого, а также лицензией можно управлять во всех развернутых экземплярах из центрального пункта.

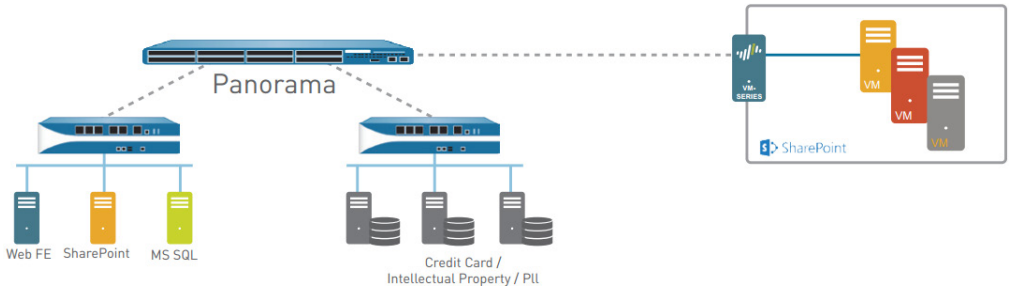


Рис. 3. Panorama управляет вашими фаерволами Palo Alto Networks, как аппаратными, так и виртуальными

• Агрегация логов, собранных из всех управляемых брандмауэров, и построение на их основе отчетности.

Panorama может быть развернута как в виртуальном приложении, так и на специальном устройстве. Специальное устройство M-100 может быть использовано для создания распределенной архитектуры управления. Отдельные M-100 устройства можно использовать для управления и протоколирования соответственно.

ОПТИМИЗАЦИЯ ПОЛИТИКИ РАЗВЕРТЫВАНИЯ И ОБНОВЛЕНИЯ

Физические и виртуальные сетевые среды сталкиваются с проблемой управления изменениями, которые могут произойти между дополнениями, извлечениями, модификациями ИТ-активов, а также проблемой быстродействия политики безопасности. Для минимизации задержек брандмауэры нового поколения обеспечивают богатым набором собственных функций управления, что упрощает политику развертки, а безопасность идет в ногу с изменениями в вычислительных ИТ-активах.

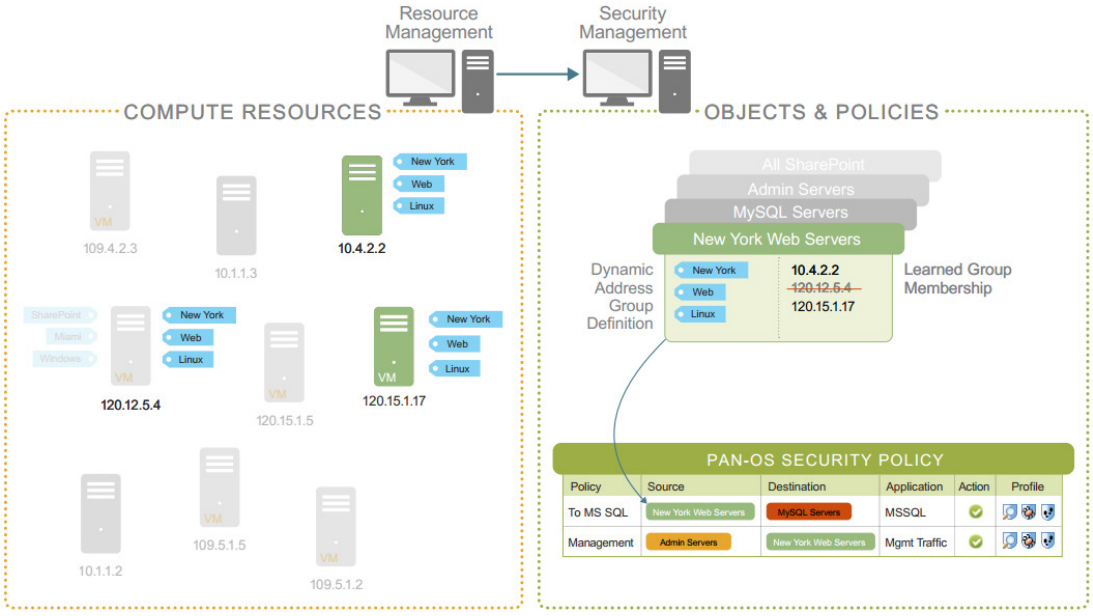


Рис. 4. Нативная функция управления – отслеживание изменений в ИТ-активах для упрощения актуализации политик

Рабочий процесс для автоматизации обновления политики состоит в следующем (см. рис 4):
1. Брандмауэр нового поколения будет связующим элементом ваших ИТ-активов.
2. Атрибуты ИТ-активов (операционная система, локация, приложение, IP-адреса), физические или виртуализированные, собираются и преобразовываются в теги.
3. Теги используются для создания Dynamic Address Groups, а также для мониторинга происходящих изменений в ИТ-активах.
4. Добавление, изъятие или изменения в ваших ИТ-активах отслеживаются, как и изменения в Dynamic Address Group, и с учетом этого динамически обновляются политики.

Результатом является резкое сокращение задержки, которая может возникнуть между изменениями в процессах и инфраструктуре и обновлениями политики безопасности. В качестве средств дальнейшей оптимизации и автоматизации обновлений политики поможет API на базе REST, которое позволяет интегрировать стороннее ПО оркестрации, такое как OpenStack и CloudStack.

СПЕЦИАЛЬНО РАЗРАБОТАННЫЙ АППАРАТНЫЙ ФОРМ-ФАКТОР

Palo Alto Networks предлагает полный спектр специально разработанных устройств, которые варьируются от PA-200, предназначенных для корпоративных удаленных офисов, до PA-7050 – устройства для ЦОДа на базе высокоскоростного шасси. Базовая архитектура основана на однопроходном сканировании, которое сначала идентифицирует приложение, независимо от порта, и одновременно определяет наличие вредоносного ПО в контенте и пользователя. Эти 3 элемента – приложение, контент и пользователь – становятся основой политики безопасности, которая соответствует требованиям бизнеса. Единая пропускная архитектура не только повышает безопасность, но и устраняет избытки решений, регулирующих политики, тем самым минимизируя задержки и повышая производительность, стыкуясь с функцией особой обработки сетей, безопасности, предотвращения угроз и управления. Такие брандмауэры нового поколения и передовая функциональность предотвращения угроз, которые поставляются в виде

аппаратных платформ, также доступны в виртуальном брандмауэре VM-серии, который позволяет обеспечить виртуализированные и облачные вычислительные среды использованием тех же политик, которые проводятся на периметре или в удаленных офисах.

PA-7050: брандмауэр нового поколения, обладает высокоскоростными системами предотвращения вторжений в ЦОД без потери пропускной способности. Фаервол способен защитить целую сеть предприятия и не влиять на ее производительность. Брандмауэр справляется со скоростью 120 Гбит/с, а по сети распределено более чем 400 процессоров, которые управляют выключением и протоколированием. Оборудование обеспечивает передовой уровень безопасности в работе с приложениями. Новинка способна сканировать их на предмет атак, вредоносного софта и уязвимостей. Устройство оптимизирует производительность сети.

PA-5000 Series: брандмауэр нового поколения, обладает высокоскоростными системами предотвращения вторжений в ЦОД без потери пропускной способности. Эти высокопроизводительные устройства созданы специально, чтобы обеспечить защиту фаервола предприятия со скоростью потока до 20 Гбит/с. Они оснащены более чем 40 процессорами, которые распределяются по четырем функциональным направлениям: сеть, безопасность, контроль и управление контентом.

Серия PA-5000 состоит из трех моделей: PA-5020, PA-5050 и PA-5060 с пропускной способностью в 5 Гбит/с, 10 Гбит/с и 20 Гбит/с, с включенным App-ID.

СЕРИЯ VM КАК ВИРТУАЛИЗИРОВАННЫЙ БРАНДМАУЭР

Серия VM – виртуализированный брандмауэр нового поколения, расширяющий сферу применения безопасного разрешения доступа приложениям в виртуализированные среды, решая ключевые проблемы обеспечения безопасности в условиях виртуализации. Серия VM поддерживает широкий ряд гипервизоров.

Серия VM для VMware ESXi (автономный): Серия VM на серверах ESXi идеально подходит для сетей, в которых виртуальный форм-фактор может упростить развертывание и обеспечить большую гибкость. Общие сценарии развертывания включают:

- Частные или публичные облачные вычислительные среды, зависящие от виртуализации.
- Среды, где физическое пространство имеет большой спрос.
- Отдаленные места, куда доставка оборудования непрактична.

Серия VM для ESXi поддерживает широкий диапазон типов интерфейсов, включая L2, L3 и виртуальное соединение, что позволяет развернуть серию VM в своем режиме интерфейса для каждого виртуализированного сервера в зависимости от потребностей.

Серия VM для VMware NSX: автоматизирует развертывание брандмауэра нового поколения и профилактики угроз посредством тесной интеграции VM-серии, Panorama для централизованного управления и VMware NSX для виртуализации сети. Трафик приложений и соответствующего контента автоматически направляется в VM-серию для анализа и проверки на VMware NSX. Panorama постоянно контактирует с NSX, собирая контекстные изменения, которые затем подаются брандмауэром как динамические обновления политики.

Серия VM для Amazon Web Services: позволяет защитить публичные облачные развертывания брандмауэра нового поколения. Доступен как Machine Interface Amazon (AMI). Серия VM может быть развернута как экземпляр EC2 для защиты трафика, проходящего через VPC. Ключевые особенности политики и управления API на базе идут в ногу с изменениями в VPC, а Panorama позволяет централизованно управлять всеми своими брандмауэрами.

Серия VM для KVM: позволяет проводить обслуживание предприятий так, чтобы можно было комбинировать брандмауэры нового поколения и расширенные возможности по предотвращению угроз с их инициативами виртуализации на основе Linux и облака. KVM – это популярный гипервизор с открытым исходным кодом, который позволяет сервису предоставлять, а предприятиям развертывать и управлять Серией VM, целой линейкой систем Linux, включая CentOS/RHEL и Ubuntu. В дополнение к богатому набору функций управления политикой и API в рамках Серии VM, Серией VM для KVM можно управлять с помощью Panorama и OpenStack.

ЗАКЛЮЧЕНИЕ

Palo Alto Networks – межсетевые экраны нового поколения, которые обеспечивают архитектуру безопасности, масштабирующуюся и развивающуюся с потребностями ЦОДов физических и облачных вычислительных сред. Фаерволы нового поколения разработаны для безопасного подключения приложений и контента от пользователей без ущерба для производительности. С4ИТ

Конвергентное инфраструктурное решение Dell PowerEdge FX

Dell представила конвергентное инфраструктурное решение Dell PowerEdge FX, обеспечивающее новый уровень производительности при создании инфраструктуры, оптимизированной под конкретные задачи заказчика.

Рис. 1. Dell PowerEdge FX

Dell PowerEdge FX основано на единой модульной расширяемой платформе, предполагающей интеграцию серверных модулей, модулей хранения и сетевого оборудования. Реализована функция удаленного доступа и администрирования, а также общая система питания и охлаждения. Платформа характеризуется высокой плотностью размещения серверных ресурсов, характеризующей блейд-системы — до четырех двухсокетных серверов на 1U стоечного пространства, — приятно дополняемой доступной стоимостью. Непрерывность бизнес-процессов обеспечивается возможностью горячей замены компонентов.

Конвергентное решение предлагается в едином компактном корпусе PowerEdge FX2 высотой 2U, предназначенном для монтажа в стойку. Шасси FX2 позволяет установить до 4 двухпроцессорных серверных узлов Dell PowerEdge FC630 или до 8 двухпроцессорных серверных узлов FC430. Возможно использование четырехпроцессорных модулей FC830. Все вышеназванные серверные модули построены на основе процессоров Xeon семейства E5-2600 v3. Это делает для всех пользователей доступными такие ресурсоемкие приложения, как бизнес-аналитика, высокопроизводительные вычисления, оперативная обработка транзакциий и др. Модули Dell PowerEdge FC630 поддерживают память до 768 ГБ. Гипервизоры Citrix и VMware позволяют разворачивать виртуальные среды любой сложности и запускать облачные сервисы.

Система поддерживает микросерверные модули FM120x4, основанные на экономичных процессорах Atom. Каждый модуль содержит 4 однопроцессорных микросервера, и в корпус можно установить 4 модуля — то есть 16 микросерверов на 2U пространства. Dell PowerEdge FX поддерживает модули хранения данных прямого подключения (DAS) PowerEdge FD332, содержащие до 16 накопителей SSD или SATA. Установка одного модуля PowerEdge FC630 и трех модулей PowerEdge FD332 позволяет реализовать в корпусе 2U двухпроцессорный сервер с 50 накопителями горячей замены форм-фактора SFF. PowerEdge поддерживает коммутационную структуру PCIe с восемью слотами, размещенными с тыльной стороны шасси, и возможностью подключать их к устанавливаемым модулям. Возможна установка до двух агрегаторов ввода-вывода Dell Networking FN, что сокращает число кабельных подключений и адаптеров локальной сети/сети хранения данных, а также количество требуемых портов в коммутаторе на уровне стойки. C4IT

SanDisk — объект для поглощения?

Акции производителя твердотельных накопителей и флэш-карт SanDisk потеряли в цене 40% от рекордного значения в июле 2014 года, и компания стала потенциальной мишенью для конкурентов, желающих улучшить свое присутствие на корпоративном рынке. Падение акций связано со слабыми продажами корпоративных продуктов, недостаточно высокими поставками чипов памяти NAND flash и незапланированными расходами на организацию производства.

К закрытию биржи NASDAQ в понедельник, 6 апреля, акции SanDisk остановились на отметке 67,25 доллара при рыночной капитализации компании в 13,75 млрд долларов. Это сделало SanDisk отличным объектом поглощения для таких чипмейкеров, как Micron Technology или SK Hynix. Ведь, несмотря на сложности, SanDisk находится в наилучшем положении на рынке продуктов флэш-памяти корпоративного уровня, которые применяются в облаках, ЦОДах и сетевых системах. C4IT

ChannelForIT

Онлайн-издание ChannelForIT предназначено для профессионалов в области корпоративных информационных технологий. Наши читатели – ИТ-директора, технические директора, специалисты и эксперты в области информационных технологий и информационной безопасности.

ChannelForIT предлагает экспертные и аналитические материалы, интервью с ведущими профессионалами отрасли, подборку главных новостей из различных источников, информацию о вакансиях для ИТ-специалистов в ведущих компаниях Украины и ближнего зарубежья, приглашения к участию в очных и онлайн-мероприятиях, многое другое.

ChannelForIT News

Еженедельное email-издание, которое обеспечивает приоритетный доступ к эксклюзивным материалам и услугам сайта Channel4IT.com: премиум-контенту наших партнеров, приглашениям на очные и онлайн-мероприятия, а также наиболее интересным новостям и материалам ведущих онлайн-изданий в области корпоративных ИТ.

ChannelForIT Review

Инновационный электронный журнал о корпоративных ИТ. Каждый выпуск посвящен одной важной, масштабной и имеющей большое практическое значение теме. Благодаря электронному формату, материалам ведущих экспертов отрасли, современным каналам доставки и другим преимуществам, ChannelForIT Review является ведущим изданием в области корпоративных ИТ в Украине.

e-mail: publisher@channel4it.com; тел.: +38 (044) 384 09 96