Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№12 (257)/2014

МОНИТОРИНГ БИЗНЕС-ПРИЛОЖЕНИЙ: НОВАЯ РЕАЛЬНОСТЬ

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:
Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Шедова Е.Л.

Дискина А.Л.
ashklyaeva@jet.msk.su

Дизайн и верстка:
Саблина М.А.

Корректура:
Макеева Е.И.

Над номером работали:
Касимов А.И.
Корниенко К.Н.
Николаев А.Б.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
www.jetinfo.ru

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Главный редактор Дмитриев В. Ю.

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

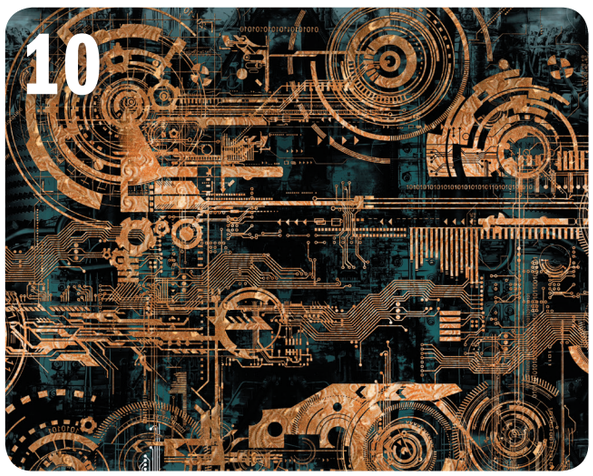
Подписной индекс по каталогу Роспечати **32555**

АЛЕКСЕЙ НИКОЛАЕВ,
руководитель департамента систем управления компании «Инфосистемы Джет»

Будущее наступает семимильными шагами. Вычислительные ресурсы из облака — пожалуйста. Программно-определяемые ЦОДы — уже вот-вот. Успех проектов интеграции реален как никогда. В одном из популярных фантастических фильмов очень серьезный товарищ по имени Нео руками извлекал практически из воздуха данные, необходимые ему для понимания природы сбоя в сложной системе — что произошло, где, что именно стало причиной. В определенной степени такая картинка — один из вариантов развития будущего интеллектуальных систем мониторинга в ИТ. Не просто увидеть, что процессор А на сервере АВС перегружен, но показать, что чувствует пользователь, насколько это нормально, какой вклад в работу системы вносит каждый из тысяч программных и аппаратных компонентов, предоставить всю эту информацию мгновенно и в нужном объеме — вот задача такой системы.

В сегодняшнем номере мы хотим начать рассказ о тех технологиях, которые приближают это будущее, — Customer Experience Management, Big Data и т.д. Думаем, что в дальнейшем мы еще не раз вернемся к этой теме.

СОДЕРЖАНИЕ



КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ» РАСШИРИЛА ЭКСПЕРТИЗУ ПО РЕШЕНИЯМ SAP HANA И SAP BusinessObjects

«Инфосистемы Джет» прошла специализированный аудит и получила статус SAP VAR Partner по продуктам SAP HANA и SAP BusinessObjects. Таким образом, интегратор получил право внедрять и интегрировать решения SAP в ИТ-инфраструктуру компаний-заказчиков, а также осуществлять их администрирование и техническую поддержку, в том числе в режиме 24x7.

Аудит проводился специалистами Центра сертификации партнеров SAP (Partner Center of Expertise) и затрагивал различные аспекты — от наличия необходимого технического оснащения до оценки внутренних регламентов предоставления поддержки.

Специалисты компании «Инфосистемы Джет» сдали необходимые квалификационные экзамены по разработке и администрированию SAP HANA и SAP BusinessObjects. В демо-лаборатории компании развернут стенд для демонстрации возможностей продуктов вендора и моделирования различных задач.

«В настоящее время рынок проявляет большой интерес к решениям SAP, особенно ритейлеры. Кроме полученных статусов, мы являемся партнером по сервису — SAP Service Partner — и осуществляем поддержку SAP Basis. Наш ВЦОД сертифицирован по программе SAP Certified Provider of Hosting Services, это означает, что вся инфраструктура и процессы обслуживания полностью удовлетворяют требованиям вендора и позволяют размещать как продуктивные, так и тестовые среды SAP любой сложности, — рассказывает **Мария Ушанова, руководитель центра компетенций страхования и розничной торговли Центра программных решений компании "Инфосистемы Джет".** — На базе нашего ВЦОД мы уже предоставляем заказчикам различные ландшафты SAP с их полной поддержкой, включая высокопроизводительные с использованием платформы SAP HANA». JI

КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ» НА БИЗНЕС-ФОРУМЕ IBM

4 декабря в Москве состоялся форум IBM «SolutionsConnect 2014: от стратегии к практике». Компания «Инфосистемы Джет» представила практические наработки в области построения динамической ИТ-инфраструктуры.

В сессии «Большие Данные и аналитика для современного предприятия» выступил **менеджер по развитию бизнеса Центра проектирования вычислительных комплексов компании «Инфосистемы Джет» Ильдар Абульханов.** На примере создания распределенного ЦОД для одного из розничных банков Ильдар рассказал о бизнес-эффектах от эксплуатации динамической инфраструктуры (доклад «Динамическая инфраструктура. Результаты, которые высоко ценит бизнес»).

«Тема, которую мы затронули, актуальна сегодня для многих крупных компаний из различных сфер экономики, — комментирует **менеджер по развитию бизнеса Центра проектирования вычислительных комплексов Андрей Иноземцев.** — Мы продемонстрировали наглядный пример того, как сочетание современных технологий позволяет эффективно использовать ИТ-ресурсы: обеспечить надежную защиту информационных активов компании, в разы сократить время простоев в ЦОД, повысить скорость реакции ИТ на бизнес-запросы и при этом снизить стоимость владения программно-аппаратной средой». JI

«ЛЕТО БАНК» И КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ» – ЛАУРЕАТЫ CNEWS AWARDS 2014

ОАО «Лето Банк» и компания «Инфосистемы Джет» стали лауреатами CNews AWARDS 2014. Совместный масштабный проект победил в номинации «Проект года в сфере аутсорсинга ИТ». Церемония награждения прошла 12 ноября 2014 года в рамках седьмого ежегодного мероприятия «CNews Forum 2014».

«Инфосистемы Джет» в полном объеме реализовала для «Лето Банка» модель «ИТ-сервисы и компетенции по требованию». Системный интегратор является генеральным ИТ-провайдером банка в части инфраструктуры и единым центром ответственности, заменяя своей службой эксплуатации и развития большую часть собственной ИТ-службы банка.

«Получение этой награды стало итогом двухлетнего аутсорсингового "марафона" в масштабах всей страны. Вместе с партнером мы взяли низкий старт: банк начал полноценно функционировать буквально через несколько месяцев после принятия решения о его создании. Мы работаем в тесной связке, в определенном смысле являясь первооткрывателями: впервые в России проект комплексного аутсорсинга характеризуется такими высокими темпами развития, разнообразием типов работ, широчайшим

географическим охватом», – комментирует **Сергей Чиков, руководитель службы ИТ «Лето Банка».**

КОНФЕРЕНЦИЯ QLIK VISUALIZE YOUR WORLD 2014

11 ноября 2014 г. компания «Инфосистемы Джет» приняла участие в конференции Qlik Visualize Your World 2014. На мероприятии эксперты и партнеры компании Qlik продемонстрировали решения на платформе QlikView и поделились опытом реализации отраслевых проектов. Также был официально представлен новый продукт Qlik Sense для самостоятельной визуализации и исследования данных.

Андрей Байбутов, руководитель практики BI компании «Инфосистемы Джет», рассказал о том, какая аналитическая информация важна для топ-менеджеров и как помочь им ее получать (доклад «Рука на пульсе, или Один день из жизни руководителя»). На примере реальных кейсов на стенде компании были представлены решения для руководителей компаний финансовой и производственной отрасли, крупных страховых, торговых и ресторанных сетей.

«Вопросы от посетителей нашего стенда побудили нас расширить демонстрационное "меню" и показать также разработанные нами аналитические модели для страхования и ритейла. В большинстве случаев интерес к продукту уже перешел от фазы "Каковы функциональные возможности и как это устроено?" к фазе "Как именно вы реализовали тот или иной отчет и

как при этом использовали особенности QlikView?", а также "Как оптимизировать производительность и грамотно организовать поддержку?". Поступали и достаточно специфичные вопросы по тематике BI: например, компании фармацевтической и телекоммуникационной отраслей интересовались опытом использования платформы для построения хранилища информации о клиентах», – рассказывает **Мария Ушанова, руководитель центра компетенций страхования и розничной торговли Центра программных решений компании «Инфосистемы Джет».**

В JSOC ЗАПУЩЕН СЕРВИС ПО КОНТРОЛЮ ЗАЩИЩЕННОСТИ

«Инфосистемы Джет» расширила линейку услуг, предоставляемых собственным коммерческим центром мониторинга (JSOC): теперь клиентам JSOC доступны сервисы по контролю защищенности внешнего периметра сети компании, а также инвентаризации и аудита внутренних информационных систем на соответствие отраслевым стандартам или внутренним требованиям информационной безопасности. Сервисы оказываются в режиме 24/7 или по требованию.

«Во многих компаниях сегодня уже внедрены и функционируют системы, позволяющие контролировать защищенность ИС и их соответствие стандартам. Однако наш опыт показывает, что при всей мощи используемых инструментов многие уязвимости, подчас даже в критичных системах компании, остаются открытыми на протяжении долгого времени, — рассказывает **Владимир Дрюков, руководитель направления аутсорсинга ИБ Центра информационной безопасности компании "Инфосистемы Джет"**. — Одна из ключевых причин этого — крайне непростой и трудоемкий процесс обработки отчета по уязвимостям внутри компании. Также сюда накладывается необходимость контроля и проверки сроков устранения уязвимостей, запуск повторных сканирований и обслуживание систем по контролю уязвимостей. И в совокупности получается, что уровень трудозатрат на реализацию одного из ключевых процессов в обеспечении ИБ компании зачастую превышает реальные возможности собственного подразделения».

Ответом на сложившуюся ситуацию стал запуск сервиса JSOC по контролю защищенности клиентов, обеспечивающего полный цикл управления уязвимостями инфраструктуры компании, который включает:

- первичный анализ и выявление незащищенных систем;
- классификацию уязвимостей в соответствии со спецификой ИТ-архитектуры компании-заказчика и функциональных задач каждой из сканируемых систем;
- подготовку рекомендаций по устранению выявленных уязвимостей (в том числе компенсирующими мерами) и сопровождение процесса их устранения;
- контроль общего индекса защищенности ключевых сервисов.

Данная услуга может предоставляться в «чистом» варианте облачного сервиса (когда оборудование и ПО предоставляются пользователю в аренду) и с использованием уже существующих у компании-клиента средств по контролю защищенности. Для повышения уровня защиты внешнего периметра сервис может быть расширен периодическими тестами на проникновение, выполняемыми ведущими экспертами компании «Инфосистемы Джет» в области эксплуатации уязвимостей и защиты приложений.

КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ» – ЗОЛОТОЙ ПАРТНЕР TREND MICRO

«Инфосистемы Джет» получила статус Trend Micro Gold Partner. Он подтверждает высокий уровень компетенций компании в сфере информационной безопасности и соответствие всем сертификационным требованиям.

Интегратор также обладает специализацией «Cloud&Data Centre Security» по продуктам защиты виртуальных сред и дата-центров. На сегодняшний день такое сочетание статусов имеют всего три интегратора в России.

«Использование облачных инфраструктур и технологий виртуализации сегодня является стандартом для большинства компаний. Естественно, что перед нашими заказчиками встает вопрос комплексной защиты данных и приложений в облачной инфраструктуре, который наша компания успешно решает, в том числе с использованием продуктов Trend Micro», — отмечает **Юрий Чер-**

кас, руководитель направления инфраструктурных ИБ-решений компании «Инфосистемы Джет».

«Мы продуктивно сотрудничаем с компанией "Инфосистемы

Джет" с 2011 года. Наш партнер обладает высочайшим уровнем практических знаний в области защиты виртуальных инфраструктур, результатом чего стала победа компании в номинации "Лучшая техническая компетенция по итогам 2013 года". Также мы отмечаем весомый вклад экспертов компании в динамику продвижения наших технологий на рынке России и стран СНГ, – говорит **Карен Карагедян, менеджер по работе с партнерами, Trend Micro.** – Мы искренне поздравляем нашего партнера с заслуженным получением золотого партнерского статуса и надеемся, что наше сотрудничество будет укрепляться и развиваться в будущем».

За время партнерства экспертами компании «Инфосистемы Джет» реализовано более 20 проектов на базе технологий Trend Micro. Наиболее масштабные из них выполнены в компаниях банковской, промышленной и телекоммуникационной отраслей. JI

УВИДЕТЬ ТО, ЧТО ДЕЛАЕТСЯ ПО ТУ СТОРОНУ СТЕНЫ

Исследователи из Университетского колледжа в Лондоне (University College London) разработали и продемонстрировали работу опытного образца системы, которая при помощи сигналов беспроводных сетей передачи данных Wi-Fi может отслеживать движущиеся объекты, находящиеся по ту сторону стен или других препятствий. Разработанное устройство по принципу действия во многом похоже на обычный радар, но в отличие от активного радара, который сам излучает радиоволны, новая система абсолютно пассивна, она лишь способна разобраться в том «супе» из радиоволн, источниками которых являются точки доступа и устройства, подключенные к беспроводной сети.

Разработанная технология имеет очень большое количество областей применения – от наблюдения за захватившими заложников террористами до реализации систем распознавания жестов. Система также может использоваться для контроля над пожилыми и больными людьми и вызова помощи в случае падения или длительного бездействия контролируемого пациента. JI

В США ИЗОБРЕЛИ СЕНСОР, ПОСЫЛАЮЩИЙ НА ТЕЛЕФОН СИГНАЛ ОБ ИСПОРЧЕННОЙ ЕДЕ

Ученые из Массачусетского технологического университета разработали датчик, который может сообщать смартфону, когда еда в холодильнике начинает портиться. Чтобы он начал работать, его необходимо синхронизировать со смартфоном, а затем установить в холодильнике. Крошечный беспроводной датчик фиксирует момент истечения срока годности пищи.

Разработанный сенсор с виду похож на «наклейку», которую крепят к товарам в магазинах, чтобы предотвратить кражу. Однако это устройство не запускает механизм сигнализации, а обнаруживает определенные химические вещества. Как сообщают разработчики новинки, она также может быть использована для распознавания взрывчатых веществ. JI

JET TOOLBAR ИНФОРМИРУЕТ НАСЕЛЕНИЕ В ПИЛОТНЫХ ЗОНАХ ГОРОДСКОГО Wi-Fi МОСКВЫ

«Инфосистемы Джет» развернула во ФГУП «Российские сети вещания и оповещения» (РСВО) платформу Jet Toolbar для таргетированной коммуникации с абонентами пилотной зоны проекта «Городской Wi-Fi». Решение позволяет проводить массовое и таргетированное информирование пользователей сети о мероприятиях в зоне их пребывания, о городских и культурных событиях, предоставлять информацию о работе городских служб, магазинов, торговых центров, кафе, показывать контент от внешних рекламодателей, проводить опросы и т.д. Необходимая информация выводится платформой Jet Toolbar на мобильные устройства абонентов поверх просматриваемой в браузере web-страницы. За первый месяц функционирования в 4 пилотных зонах система позволила провести онлайн-опрос о качестве Wi-Fi, в котором приняло участие около 30 тысяч москвичей.

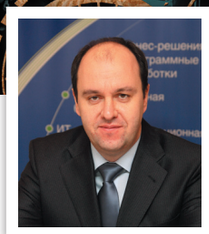
Платформа Jet Toolbar устанавливается в Центре управления сетью РСВО, где концентрируется трафик всех созданных организацией Wi-Fi сетей. Сегодня реализуются 3 сценария взаимодействия с пользователями: «Приветствие в системе», «Опрос» и «Оповещение».

«Jet Toolbar дает нам широкие возможности как для широковещательного информирования, так и для персональной коммуникации с пользователями городской сети», – комментирует **Заместитель Генерального директора – Главный инженер ФГУП РСВО Валерий Артюшин.**

«Функционал системы позволяет использовать ее для самых разных целей. Например, можно помочь правоохранительным органам в поиске пропавших людей, показывая их фотографии. Кроме того, при интеграции Jet Toolbar с порталами муниципальных органов у пользователей появится возможность в один клик оплачивать городские услуги, регистрировать заявки на обслуживание, отслеживать их статус и др. При этом наш продукт не требует никаких дополнительных установок на мобильных устройствах», –

поясняет Елена Фоминская, директор Центра телекоммуникационных продуктов и решений компании «Инфосистемы Джет».

МАТРИЦА: ЭВОЛЮЦИЯ



АЛЕКСЕЙ НИКОЛАЕВ,
руководитель департамента систем управления компании «Инфосистемы Джет»

В первой «Матрице» есть эпизод, в котором оператор в режиме реального времени мониторит многочисленные показатели системы и дает Нео совет: «Информации, получаемой из Матрицы, гораздо больше, чем ты можешь расшифровать. Нужно адаптироваться к этому». Собственно, о необходимости адаптироваться, модернизировать мониторинг под новые условия мы и хотим поговорить в этой статье.

Системы мониторинга и современные технологии — для многих из тех, с кем мы обсуждаем перспективы и задачи развития подобных решений, это сочетание является, как минимум, странным. Что может быть нового в столь понятной и давно разработанной области? Ведь главное — измерить значение и сообщить о нарушении заданных порогов. А дальше работают люди. И существует огромное количество коммерческих и бесплатных продуктов, с той или иной степенью полноты реализующих эти функции.

С одной стороны, это действительно так. С другой — сложность информационных систем растет, а вместе с ней увеличиваются и масштабы финансовых и репутационных потерь от простоев. Большинству компаний уже недостаточно просто обнаружить симптомы неисправности: слишком много драгоценного времени и сил уходит на анализ ситуации, локализацию и диагностику проблем.

В прошлых номерах Jet Info мы описывали современные тенденции развития систем мониторинга, смещение фокуса от инфраструктуры к приложениям и качеству сервисов, предоставляемых пользователям. За прошедшее время многое изменилось — появились новые технологии, решения и подходы

к построению этих систем. Для себя мы определяем два типа изменений: технологические и изменения формы. В первом случае речь идет о технологиях и инструментах, позволяющих сократить время на локализацию/диагностику проблем.

К ним, например, принадлежат решения класса End User Experience Management. Они позволяют не только «посмотреть» на приложение глазами пользователя, но и выявить те его действия, которые приводят к ошибкам и повышению нагрузки на систему. Есть реальные примеры, когда «поверья» пользователей, активно переключавших окна приложения для ускорения транзакции, приводили именно к таким последствиям. С одной стороны, это звучит довольно забавно, с другой — как выявить подобные ситуации и снять негатив со стороны бизнес-пользователей без контроля реальных транзакций? Требуется ли для решения подобной проблемы проводить глубокий анализ приложений и модернизировать инфраструктуру?

Второй инструмент относится к модной теме анализа Больших Данных. 10 лет назад попытка выгрузки истории событий мониторинга за месяц приводила к зависанию системы длительностью до нескольких десятков минут. А ведь это касалось только событий, «сырые» данные и журнальные файлы не учитывались, притом сами системы были проще. Достаточно и одной технологии виртуализации с динамическим переездом гостевых машин из одного ЦОД в другой, для того чтобы представить, во сколько раз увеличился объем информации, требующей анализа. С появлением решений Big Data Analytics возможности «сканирования» огромных массивов информации в режиме, близком к реальному времени, стали реальностью (см. статью «Шерлок против Big Data» на стр. 27).

В случае же изменения формы речь пойдет о новых подходах к развертыванию систем мониторинга. Не секрет, что комплексные полнофункциональные решения сложны как в развертывании, так и в сопровождении. Что такое SaaS в области систем мониторинга? Какие существуют решения и какие мы видим в них плюсы и минусы — об этом пойдет речь в статье «Мониторинг приложений в стиле SaaS» на стр. 12.

Среди других значимых тенденций, относящихся, скорее, к изменениям формы, чем к технологическим изменениям, можно отметить появление на Enterprise-рынке свободно распространяемых решений типа Zabbix. Обладая несколькими значимыми преимуществами: низкой ценой, простотой администрирования и поддержкой сообщества, эти средства по функционалу уже практически не уступают коммерческим системам мониторинга инфраструктуры. Кроме того, на базе Zabbix уже реализованы проекты упрощенного мониторинга приложений и бизнес-процессов.

Все более вероятным видится вытеснение коммерческих средств с поля инфраструктурного мониторинга, это окажет значительное влияние на архитектуру создаваемых систем. В будущем нас ждут большая гетерогенность решений, появление новых интеграционных стыков на уровне как передачи данных мониторинга, так и управления конфигурацией систем. Но это, скорее, темы наших следующих номеров. JI

Что же остается за рамками номера? На самом деле, многое. В первую очередь – технологии, сращивающие мониторинг ИТ, приложений и бизнес-процессов. Именно они, наконец, приближают нас к построению целостной системы контроля автоматизированных бизнес-процессов: от уровня логики и ошибок выполнения отдельных экземпляров процесса до уровня приложений и технологий, обеспечивающих их автоматизацию.

В данном случае можно обратить внимание на недавно появившиеся средства мониторинга бизнес-процессов, ориентированные на выполнение следующих основных задач в режиме, близком к реальному времени:

- обнаружение сценария выполнения конкретного экземпляра бизнес-процесса, оценка его соответствия типичным или эталонным сценариям;
- сбор данных о событиях из различных источников (БД, шины и др.), их корреляция и интерпретация в виде информации о статусе выполнения экземпляра бизнес-процесса;
- расчет сводных KPI по процессу в целом с возможностью детализации до показателей отдельных экземпляров;
- прогнозирование изменения значений KPI, оценка их соответствия типичным значениям.

Отличие подобных средств от классических, ИТ-ориентированных систем мониторинга бизнес-процессов состоит, во-первых, в оперативном режиме их работы, обеспеченном за счет активного применения технологий анализа Больших Данных. Во-вторых, у них есть возможность детализации информации до конкретного экземпляра, а не только до уровня KPI всего бизнес-процесса в целом.

МОНИТОРИНГ ПРИЛОЖЕНИЙ В СТИЛЕ SAAS

КОНСТАНТИН КОРНИЕНКО,
старший инженер-проектировщик систем управления департамента систем управления компании «Инфосистемы Джет»

Сегодня инструменты мониторинга приложений, предоставляемые по модели SaaS (есть даже термин MaaS, Monitoring As A Service), не очень востребованы крупными и средними российскими компаниями. При этом лидеры рынка средств мониторинга приложений (по версии Gartner Application Performance Management Magic Quadrant 2014) — компании New Relic, AppDynamics, Compuware — предоставляют возможность обрабатывать данные мониторинга в облаке. Для New Relic это вообще единственный вариант использования продукта. В этой статье мы попытаемся разобраться, насколько облачные решения по мониторингу могут быть востребованы в России. Для начала выясним, какие возможности они предоставляют.

Синтетический мониторинг

«Синтетика» — простой и при этом эффективный инструмент для анализа доступности и производительности приложений. «Облачная синтетика» позволяет быстро начать получать данные о качестве работы вашего приложения с точки зрения потенциальных пользователей, выполняя тестовые проверки из различных сетевых локаций, предоставляемых вендором. Ее функционал включает:

- базовую проверку доступности хостов (ping) и веб-страниц (HTTP GET);
- проверку корректности разрешения DNS-имён, доступности TCP-портов;
- расширенное, «сценарное» тестирование веб-приложений,

Рис. 1. Магический квадрант Gartner – Application Monitoring (октябрь 2014 г.)

например, проверка входа в приложение по специальному тестовому логину/паролю, работоспособности выбранных сервисов — получения выписки со счёта в интернет-банке или подключения новой услуги в личном кабинете интернет-провайдера;

- предоставление дополнительной информации в случае проблем, например, кодов ошибок HTTP, маршрута (trace route) до вашего сервера, информации о проблемах с разрешением имён (DNS).

При этом развёртывание традиционной, не облачной, «синтетики» для качественного мониторинга современных веб-приложений — достаточно затратное мероприятие, т.к. придётся решать вопросы с размещением тестирующего ПО в различных сетевых локациях.

Полнофункциональный мониторинг приложений

Все основные производители предоставляют возможность глубокого мониторинга современных приложений, работающих на Java или .NET (некоторые поддерживают и другие платформы — PHP, node.js и др.).

Обычно все выглядит так: агентское ПО для соответствующей платформы интегрируется в приложение в соответствии с пошаговыми инструкциями вендора. После перезапуска приложения агент начинает собирать большое количество данных, которые отправляются в облако в режиме реального времени. Также некоторые вендоры предоставляют возможность установки дополнительных агентов для сбора данных о работе ОС, БД и другого ПО.

На этом взаимодействие между приложением и ПО мониторинга заканчивается, вся дальнейшая обработка данных выполняется уже в облаке. Оператор мониторинга получает информацию через веб-консоль системы, которая обычно обновляется практически в режиме реального времени, важные события также отправляются ему по электронной почте или посредством SMS.

Ниже перечислены основные возможности современных облачных систем мониторинга приложений:

- анализ метрик производительности виртуальной машины (Java JVM/.NET CLR);
- анализ метрик производительности ОС с помощью установки дополнительного агентского ПО. Обычно обеспечивается базовый набор метрик, которого, впрочем, достаточно во многих случаях: утилизация CPU, памяти, дисков, сетевых интерфейсов, базовые метрики работы процессов (CPU, диск, IO);
- сбор подробной информации о выполненных транзакциях (в том числе полное время выполнения транзакции, количество вызовов за период времени, ошибки времени выполнения, трассировка стека, выявление блоков кода, выполнение которых занимает наибольшее время). Кроме того, проводится анализ запросов к БД, осуществленных приложением, и взаимодействия приложения с очередями сообщений и внешними сервисами;
- расчёт baseline («базовых линий» — нормальных значений метрик). Рассчитанные значения используются для мониторинга нескольких сценариев:

- сравнение релизов — как изменилась производительность приложения после обновления версии;
- поиск первопричины — при изучении проблем можно провести анализ метрик всех компонент, участвующих в выполнении транзакции. Например, анализируя ошибки приложения вида «Сервис временно недоступен», можно посмотреть, какие показатели ОС, JVM или БД в это время выходили за пределы своих нормальных значений. ПО от некоторых вендоров может выполнять такую аналитику автоматически;
- оповещение — отправка уведомлений в случае выхода ключевых метрик из коридора нормальных значений;

• мониторинг действий реальных пользователей. Чтобы выяснить, насколько быстро и качественно работает веб-приложение с точки зрения конечных пользователей, инструменты облачного мониторинга обычно полагаются на вставку дополнительного кода в генерируемые приложением HTML-страницы. Внедряемые скрипты замеряют время отрисовки страниц и исполнения клиентских скриптов, отправляя полученные данные напрямую из браузера пользователя в облако. Эта информация помогает проанализировать работу приложения «из конца в конец» — выявить проблемы у пользователей и связать их с проблемами в инфраструктуре или коде приложения;

• мониторинг мобильных приложений (iOS, Android). Для анализа их функционирования разработчик приложений может воспользоваться предоставляемым SDK (Software Development Kit) — после перекомпиляции мобильного приложения с внедрённым кодом вендора в облако могут отправляться следующие данные: подробная информация о мобильном устройстве, о географическом местоположении пользователя и используемом операторе связи для выявления проблем, специфичных для региона или конкретного оператора, о блоках кода, время выполнения которых занимает наибольшее время. Также в облако идут данные об ошибках, падениях мобильного приложения и проблемах взаимодействия с back-end'ом по сети.

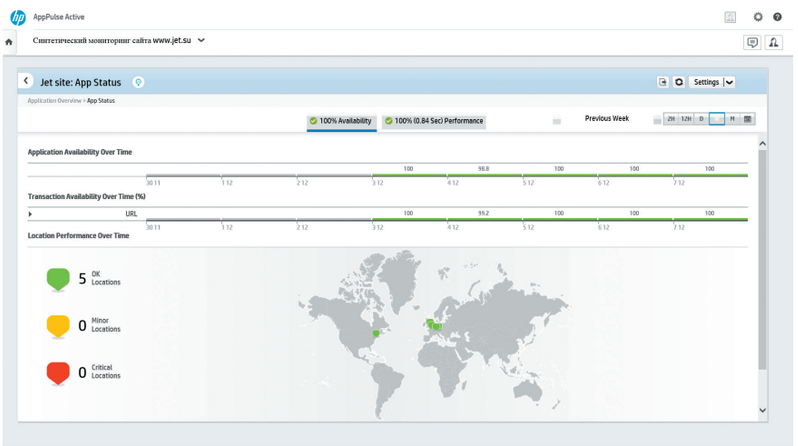


Рис. 2. Страница статуса приложения в HP AppPulse Active

ОБЛАЧНЫЕ РЕШЕНИЯ ПО МОНИТОРИНГУ

Российским компаниям доступно большое количество облачных систем мониторинга, рассмотрим лишь некоторые из них.

HP AppPulse

Линейка продуктов HP AppPulse (ранее — HP Performance Anywhere) состоит из облачного ПО, доступного к использованию на портале Pronq (www.pronq.com). Линейка постоянно расширяется и на данный момент состоит из большого числа отдельных продуктов, однако к нашей теме имеет отношение лишь их часть.

HP AppPulse Active — наверное, один из самых функциональных продуктов синтетического мониторинга на рынке: поддерживается тестирование веб-страниц, доступности хостов и TCP-портов, серверов DNS и FTP. Даже в базовом режиме тестирования веб-сайта есть возможность проверки содержимого: вы можете убедиться, что в тексте страницы, которую увидит пользователь, отсутствует, например, слово «ошибка».

Сценарное тестирование веб-приложений реализовано с помощью выполнения скриптов, записанных в среде разработки HP Vugen. HP Vugen позволяет записать действия пользователя, выполняемые в браузерах Firefox и IE, после этого среда разработки сгенерирует скрипт, который впоследствии легко можно доработать.

Тестовые скрипты можно выполнять как из множества облачных локаций, располо-

женных по всему миру (в России, впрочем, пока их нет), так и из закрытого сетевого контура компании (для этого требуются скачивание и установка дополнительного модуля). На основе собранных значений метрик доступности и производительности веб-ресурсов ПО позволяет создавать SLA, а также автоматически выявлять отклонения от нормы (Predictive Analytics).

Судя по всему, «под капотом» HP AppPulse Active трудится старый знакомый — HP Business Process Monitor, поэтому если у вас уже есть готовые скрипты, созданные для HP BPM или HP LoadRunner, их можно загрузить в ПО и сразу начать мониторинг. Поддерживаются, впрочем, не все типы скриптов, а только те, которые имеют отношение к тестированию интернет-ресурсов.

HP AppPulse Diagnostics обеспечивает мониторинг приложений Java/.NET/Python. Возможности продукта практически повторяют функционал обычного, не облачного HP Diagnostics. Поддерживаются профилирование транзакций, выявление отклонений в скорости их выполнения от нормы (Predictive Analytics), автоматический поиск первопричин задержек в работе транзакций (проблемы ОС/среды исполнения, внешних сервисов, БД или конкретных блоков кода).

В целом функционал достаточен для постоянного отслеживания качества работы приложения, но для комплексного мониторинга всей его инфраструктуры обязательно потребуется использование дополнительного (и уже, скорее всего, не облачного) ПО.

HP AppPulse Mobile отвечает за мониторинг мобильных приложений. AppPulse Mobile SDK легко внедряется в ПО для смартфонов и не требует модификации кода. После перекомпиляции и распространения приложения на странице AppPulse Mobile станут доступны данные о его работе на устройствах пользователей. Собирается информация о задержках в реакции на пользовательские действия и фактах падения приложения. На основе этих данных рассчитывается интегральный показатель FunDex (по аналогии с широко используемым Apdex), который показывает, насколько среднестатистический пользователь может быть доволен работой мобильного ПО.

В случае падения приложения AppPulse Mobile предоставит пошаговый сценарий действий пользователя, которые привели к такому печальному результату, что, безусловно, поможет в поиске и исправлении ошибок. Собранная информация о конфигурации смартфонов пользователей поможет узнать, например, на каких версиях ОС проблемы случаются чаще всего.

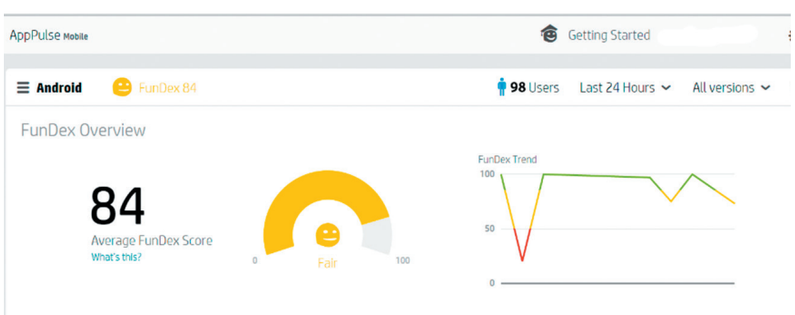


Рис. 3. Страница статуса мониторинга мобильного приложения в HP AppPulse Mobile

Каждый продукт из линейки HP AppPulse работает сам по себе, интеграции между ними не предусмотрено. Например, потенциально вы сможете узнать, что первопричина «задумчивости» мобильного приложения заключается в медленной генерации данных back-end'ом, но корреляцию вам придётся провести самостоятельно, заглядывая поочередно в консоли HP AppPulse Diagnostics и HP AppPulse Mobile.

New Relic

Облачное ПО мониторинга от компании New Relic включает в себя полный набор инструментов для синтетического мониторинга, мониторинга приложений Java/.NET/PHP/Python/Ruby/Node.js, ОС серверов, ПО для смартфонов, действий реальных пользователей. В нем реализованы практически все современные возможности, включая мониторинг распределённых (между несколькими приложениями) транзакций, построение карты приложения, профилирование потоков и др.

Стоит отметить, что New Relic поддерживает расчёт интегрального индекса Apdex как для приложений целиком, так и для отдельных транзакций. Apdex отражает степень удовлетворённости реальных пользователей скоростью и стабильностью работы приложения. При уменьшении индекса можно сделать вывод о наличии проблем с мобильным ПО, что предполагает дальнейшие шаги по выявлению их корневых причин.

«Синтетика» в базовом варианте может только проверять

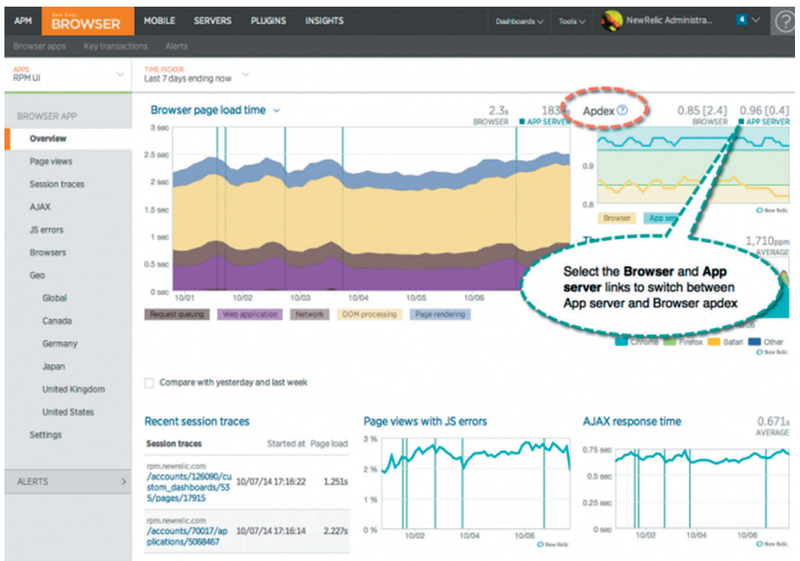


Рис. 4. Основная страница «синтетики» в New Relic

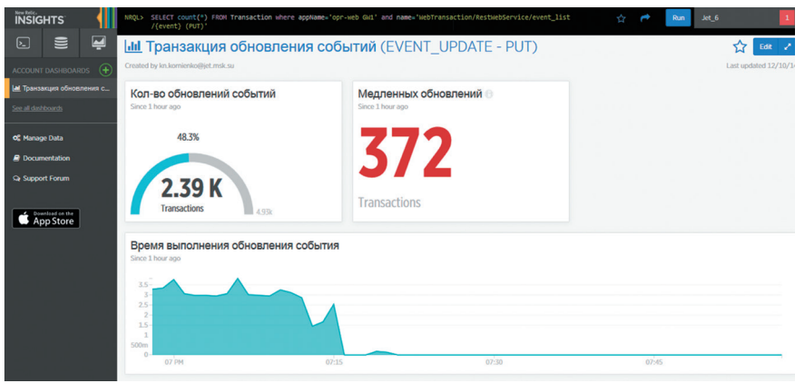


Рис. 5. Разработка dashboard в New Relic

доступность страниц (опционально доступна загрузка всех их элементов). Для сценарного тестирования сайтов придётся создавать скрипты на JavaScript (используется скриптовый браузер Selenium), возможность записать действия пользователя не предусмотрена. Локаций, откуда могут запускаться тесты, пока тоже не очень много — порядка десятка, ближайшая к нам находится в Германии. «Синтетика» работает обособленно и никак не связана с мониторингом работы приложений.

Конструктор dashboard'ов нам понравился — простой и гибкий, он позволяет визуализировать достаточно сложные данные (по логике расчёта). Для получения данных мониторинга необходимо построить SQL-запрос в полуавтоматическом режиме, при этом система подсказывает все возможные варианты ключевых слов и значений колонок таблиц.

Мониторинг мобильного ПО, помимо стандартных возможностей для продуктов такого рода, предоставляет подробную сетевую статистику, что может быть важно для бизнес-приложений, где вся логика обработки действий пользователя производится на сервере.

В ПО мониторинга New Relic можно отправлять собственные метрики и события с помощью API системы. На этой возможности основываются расширения (plugins), которые используются для включения в контур мониторинга дополнительных элементов ИТ-инфраструктуры, таких как ПО веб-серверов или баз данных. На момент написания статьи на сайте New Relic было размещено уже более 100 расширений, созданных партнёрами компании.

AppDynamics

ПО обеспечивает мониторинг приложений Java/.NET/PHP/Node.js, мобильных приложений, ОС серверов, баз данных. Для синтетического мониторинга AppDynamics не предоставляет своего решения, опираясь на интеграцию с продуктами компании Apica. Мониторинг реальных пользователей воз-можен либо через внедрение дополнительного кода в веб-страницы, либо через интеграцию с ПО BMC End User Experience Management.

Это ПО также может выполнять роль оркестратора — запускать различные действия на серверах мониторинга как в ручном, так и в автоматическом режиме (при получении определенных событий). Кроме того, есть интересная возможность по управлению виртуальной инфраструктурой поддерживаемых облачных провайдеров, например, при получении события об увеличении нагрузки на приложение вы можете запустить процесс по перенастройке виртуальных машин серверов приложений.

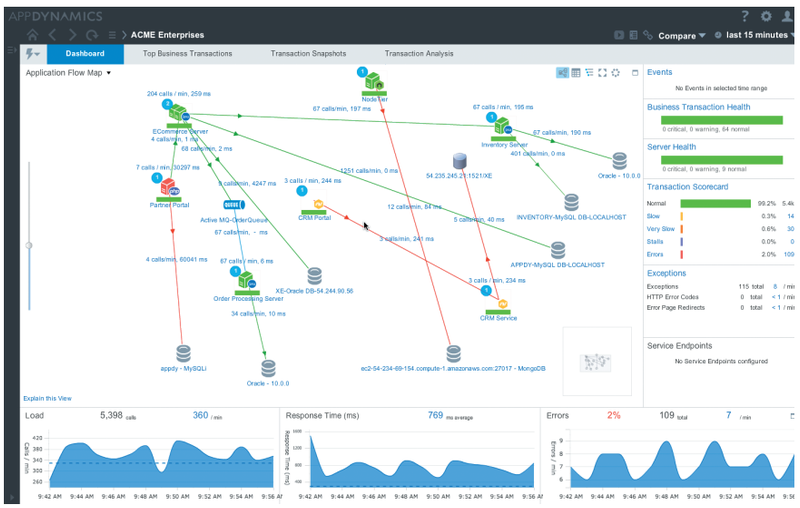


Рис. 6. Карта и основные метрики приложения в AppDynamics

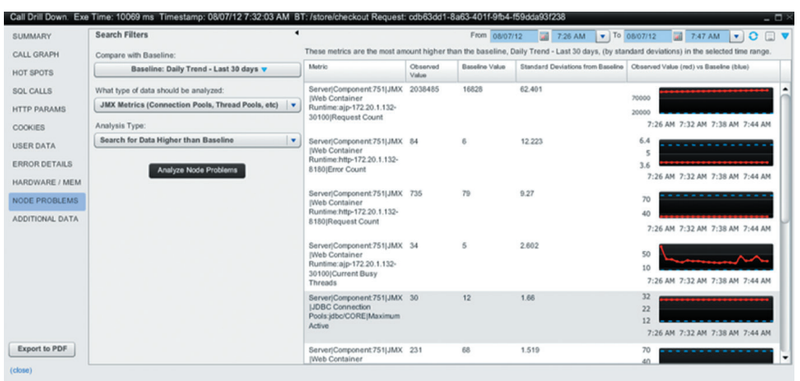


Рис. 7. Автоматический поиск метрик с аномальными значениями в AppDynamics

Отличительной особенностью платформы от AppDynamics является возможность ее работы как в облачном, так и в обычном (on-premise) режиме: вы можете скачать серверное ПО и установить его на своей виртуальной или физической инфраструктуре, решив много проблем с безопасностью и при этом не потеряв в функциональности.

При мониторинге приложений компания AppDynamics, в отличие от New Relic, не использует индекс Apdex для интегральной оценки качества работы программ (она даже опубликовала критическую статью[1] о самой идее этого индекса). Вместо этого ПО рассчитывает базовые линии для всех метрик, а механизм выявления аномалий постоянно сравнивает текущие показатели с нормальными, выявляя проблемные элементы. ПО предоставляет возможность эффективного исследования проблем с производительностью: в случае обнаружения аномального поведения какого-либо компонента приложения автоматически выявляются все метрики связанных элементов инфраструктуры, которые тоже ведут себя не так, как обычно. Этот удобно реализованный функционал позволяет быстро и точно выявлять корневые причины проблем доступности и производительности.

В модуле мониторинга приложений AppDynamics удалось реализовать очень удачное, на наш взгляд, их основное представление — карту. Она отображает текущие взаимосвязи между модулями распределенных приложений (аналог сервисно-ресурсной модели, только обновляющейся в режиме реального времени), включая экземпляры БД, очереди сообщений и серверы. Карта содержит большое количество интерактивной диагностической информации, при этом не выглядит перегруженной и может быть использована как основное представление для операторов мониторинга.

Еще одной «фишкой» ПО является корректный анализ работы асинхронных транзакций и транспорта Web Sockets — эти технологии всё чаще используются в современных веб-сервисах.

Модуль мониторинга мобильного ПО выгодно отличает интеграция с основным модулем — мониторинга приложений. В случае задержек в работе мобильного приложения вы получите информацию о том, как вели себя соответствующие транзакции в back-end'е.

Дополнительные возможности предоставляют war rooms — коллективные обсуждения данных мониторинга с другими пользователями системы в режиме чата. Очень полезно, когда информация, которой обмениваются сотрудники по ходу решения проблем, остаётся в системе с привязкой к конкретной временной точке и компоненту приложения.

AppDynamics предлагает воспользоваться расширениями, которые разрабатывают как компании, так и частные разработчики.

[1] http://www.appdynamics.com/blog/apm/apdex-is-fatally-flawed/

Можно найти, например, расширения для мониторинга VMware WebSphere MQ.

ПЛЮСЫ И МИНУСЫ ОБЛАЧНОГО МОНИТОРИНГА

Чем отличаются облачные продукты мониторинга от своих традиционных собратьев, требующих развёртывания на площадке компании? К плюсам SaaS ПО для мониторинга приложений стоит отнести несколько факторов.

Быстрое развёртывание. В нашей тестовой лаборатории, как правило, уходило менее часа на то, чтобы получить первые данные мониторинга с помощью типичного представителя облачного ПО. Еще 60 минут было достаточно, для того чтобы познакомиться с интерфейсом и основными компонентами системы, а в течение третьего часа мы уже были способны создавать свои представления (dashboards), настраивать под себя схему оповещений и определять SLA.

Постоянное наращивание функционала, удобный интерфейс, полная документация. Новые возможности в ПО появляются регулярно и, что немаловажно, не требуют от пользователей никаких дополнительных действий, вроде миграции данных или изменения настроек, как это случается в традиционном ПО при обновлении мажорной версии.

Между «облачниками» наблюдается серьезная конкуренция, поэтому борьба за клиента идёт по всем направлениям, производители не могут позволить себе «задумчивость» интерфейса и поверхностную, отстающую от реальности документацию (это, увы, мы пока сплошь и рядом встречаем у традиционных продуктов мониторинга). Интерфейс ПО всех вендоров, упомянутых в статье, очевиден, понятен, современен. Продуктами пользоваться удобно (а значит, эффективно) и попросту приятно.

Отсутствие проблем с поддержкой ПО, обновлениями, резервным копированием. Их берёт на себя вендор облачного решения, снижая затраты компании на поддержку системы мониторинга. Большая часть работ по обновлению ПО проходит для пользователей совершенно незаметно. Некоторые вендоры выделяют 2–3 часа в месяц на обслуживание, когда ПО может быть недоступно или работать с ограничениями.

Минусы у облачного ПО тоже, к сожалению, есть.

Первый из них касается безопасности. Далеко не все компании морально готовы внедрять в свои приложения закрытое агентское ПО, которому необходим доступ в интернет, к тому же организация этого доступа из закрытых сегментов сети может вызвать большие затруднения.

Задача по настройке аутентификации и авторизации операторов облачной системы мониторинга с использованием корпоративных серверов LDAP/AD также не выглядит легко решаемой.

Еще один фактор: мониторинг приложений реализуется с помощью агентского ПО, которое внедряется в среды исполнения (Java/.NET и др.) и потенциально имеет доступ ко всем внутренним данным приложения. От потери клиентов по этой причине вендоры пытаются защищаться путём проведения периодических внешних аудитов, которые осуществляют авторитетные организации.

Еще одно узкое место — это необходимость **наличия доступа в интернет.** Для полноценной работы как самой системы мониторинга (отправка данных в облако), так и операторов системы необходим надёжный канал в интернет, работающий в режиме 24/7. Отсутствие доступа во «внешний мир» приведёт к остановке мониторинга даже внутренних приложений, что недопустимо во многих случаях.

Негативное влияние имеет и тот факт, что кастомизация поведения различных аспектов облачного ПО, как правило, выливается в **создание своих расширений,** что технически не так уж просто. Традиционные системы мониторинга основных вендоров могут предложить более широкие возможности для небольших доработок функционала.

И наконец приходится констатировать **ограниченность функционала** подобных продуктов для решения комплексных задач мониторинга корпоративных ИТ-систем.

Остановимся подробнее на последнем пункте. В настоящее время во многих средних и крупных российских компаниях сложилась тенденция к внедрению комплексных (мы называем их «зонтичными») систем мониторинга. Правильно внедрённый «зонтик» позволяет консолидировать данные мониторинга большого количества различных систем в одном месте, что дает ряд преимуществ:

- всесторонний анализ работоспособности бизнес-сервисов и инфраструктуры, учитывающий проблемы на всех уровнях (приложение, ИТ-инфраструктура, инженерное оборудование дата-центров и др.), что позволяет качествен-

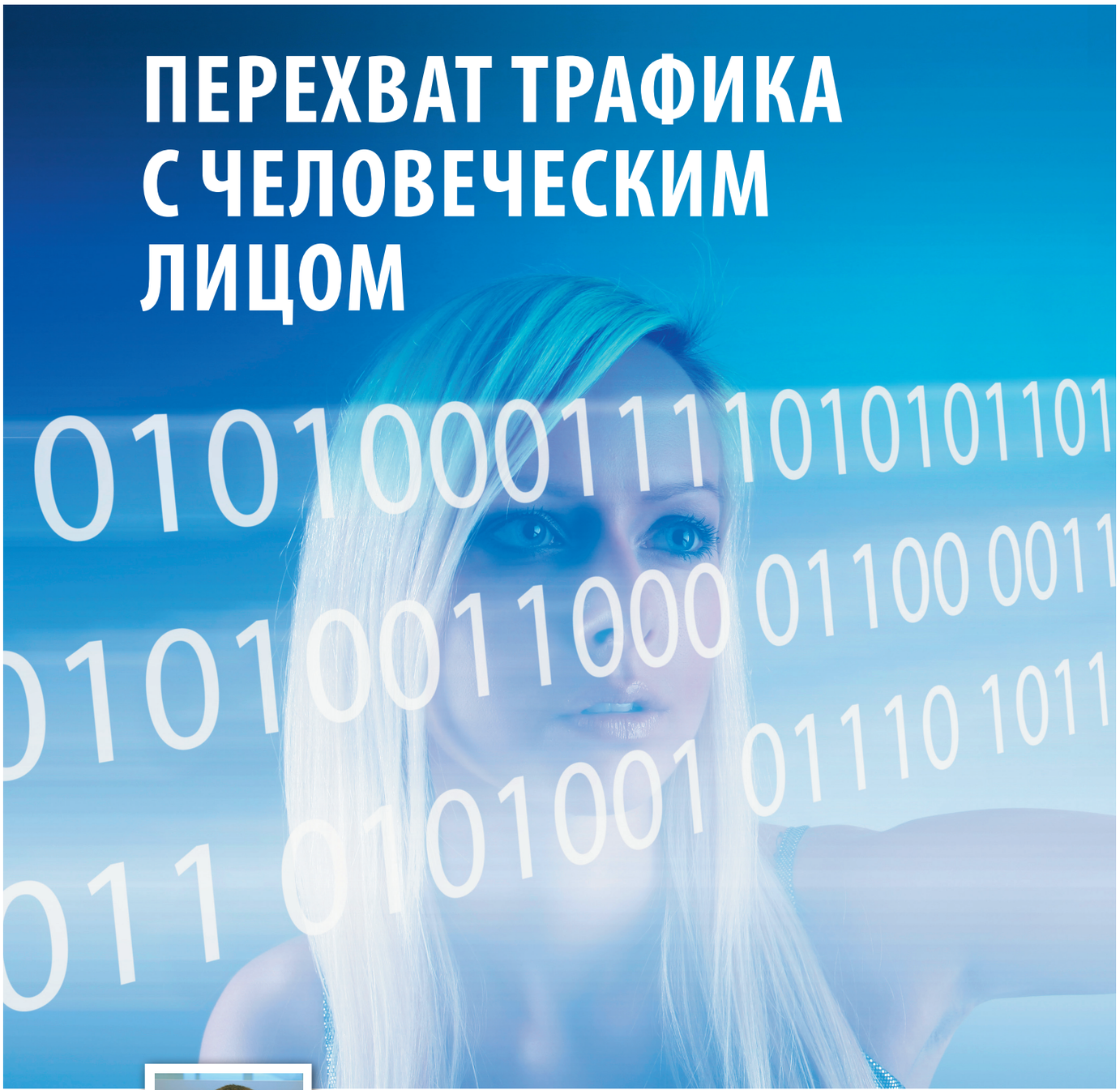
но выполнять аналитику и решать вопросы приоритизации возникающих инцидентов;
- наличие единой точки интеграции с системами оповещения и управления инцидентами;
- наличие единого долговременного хранилища данных для расчёта SLA, формирования отчётности, Capacity Management;
- эффективное взаимодействие с базами данных конфигурационных элементов (постановка на мониторинг, ресурсно-сервисные модели, анализ влияний, оркестрация);
- наличие основы для создания центра компетенции (автоматическое обогащение событий мониторинга инструкциями по устранению проблем, формируемыми исходя из опыта прошлых аварий и т.д.), что потенциально позволяет снизить требования к квалификации операторов мониторинга/дежурной смены, а также уменьшает время обработки аварий.

К сожалению, ни один из существующих облачных продуктов по мониторингу пока в роли «зонтика» выступить не может. Возможности даже самых функциональных решений заканчиваются, в лучшем случае, на уровне виртуализации, проблемы сети, СХД, инженерного оборудования дата-центров и т.д. остаются за кадром.

Интеграция же облачного ПО мониторинга приложений с «зонтичными» системами, как правило, технически проблематична. Максимум, на что можно рассчитывать без создания полнофункциональных интеграционных пакетов, — это включение интерфейса облачной системы в единую консоль «зонтика» и трансляция событий, которые генерирует облачное ПО, в «зонтик».

Тем не менее возможность выбора — это априори неплохо, поэтому если мы увидим, что для решения задачи компании больше всего подходит именно облачная система, мы с удовольствием поможем ее внедрить. Для компаний, которым не подходит облачное ПО мониторинга, мы можем предложить вариант с традиционным ПО, предоставляемым клиенту по облачной схеме. Это может оказаться оптимальным решением, так как в подобном случае снимается большинство вопросов с безопасностью и остаётся доступным функционал «зонтичных» систем мониторинга. JI

ПЕРЕХВАТ ТРАФИКА С ЧЕЛОВЕЧЕСКИМ ЛИЦОМ



АНТОН КАСИМОВ,
инженер-проектировщик систем управления департамента систем управления компании «Инфосистемы Джет»

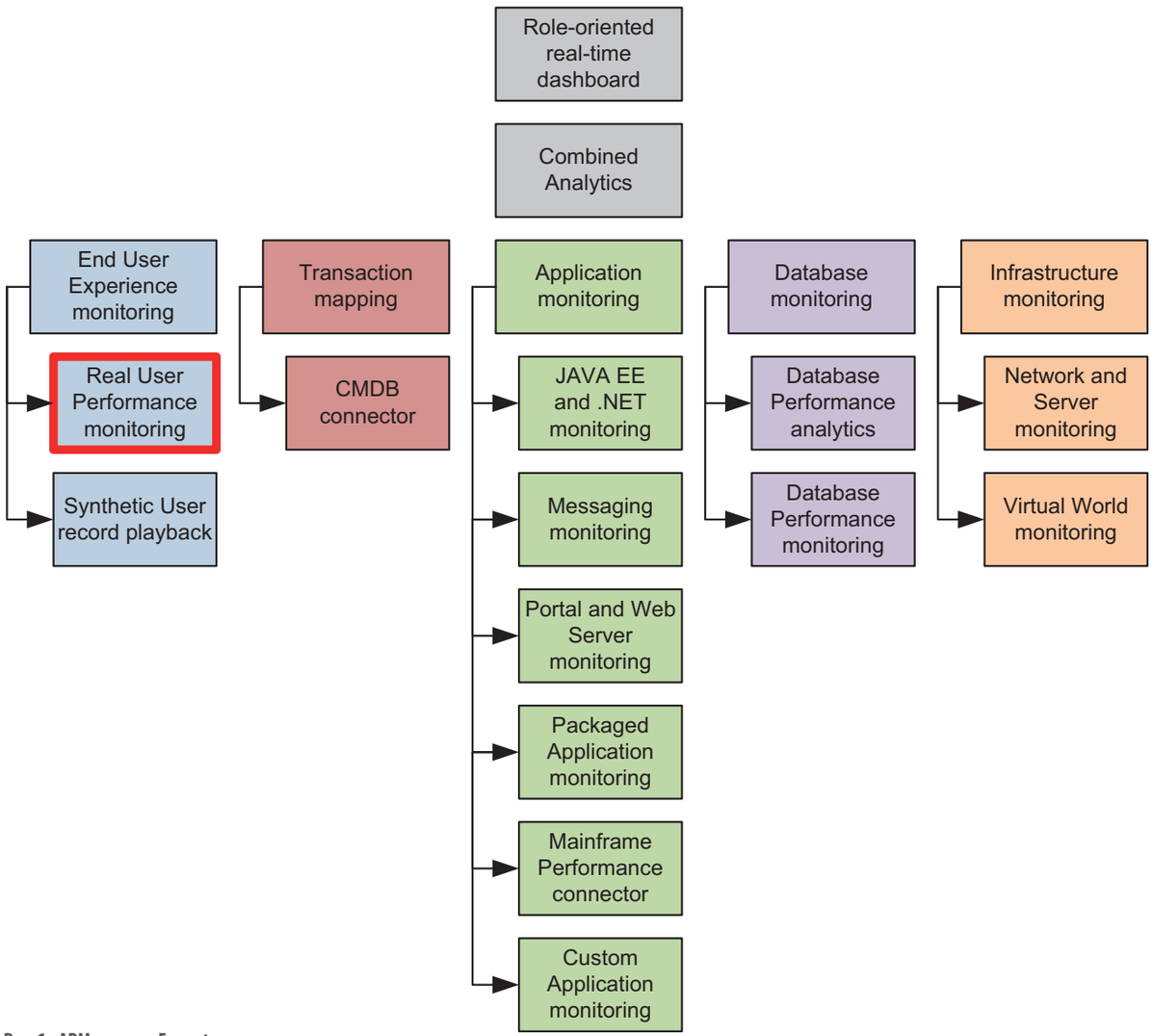


Рис. 1. APM-модель Forrester

Какие мысли возникают у вас в голове при произнесении словосочетания «перехват трафика»? Предотвратить и наказать? Скорее всего, да, но в некоторых случаях прослушивание трафика кем-то, помимо получателя, может быть и полезным, причем и для получателя, и для отправителя. Речь идет об относительно новой категории программного обеспечения по управлению производительностью бизнес-приложений, а именно – о ПО класса Customer Experience Management (CEM). Этот термин имеет достаточно широкий смысл. В данном случае он предполагает мониторинг и анализ реального трафика, действий настоящих пользователей, словом, реальной среды, где происходит все самое интересное для владельца приложения, разработчика и администратора. CEM является компонентом APM-модели (Application Performance Management Model), предложенной аналитической компанией Forrester. По классификации Forrester, это Real User Performance Monitoring (см. рис. 1).

Предлагаем вместе рассмотреть разновидности таких решений, их преимущества и ограничения, которые они накладывают. Сразу же оговоримся, что существуют также средства мониторинга, подразумевающие модификацию исход-

ного кода веб-приложения (или установку агента на веб-сервер), отправляющие статистику в подсистему аналитики (на рынке наиболее распространены облачные решения). По замыслу вендоров они могут относиться к классу CEM, однако мы не будем рассматривать их в статье.

РЕШАЕМЫЕ ЗАДАЧИ

Бизнес-приложение — это комплекс программных средств, которые поддерживают определённый бизнес-процесс компании (CRM, ERP и т.п.). Чаще всего в этот комплекс входят веб-сервер, сервер приложений и сервер базы данных, которые определенным образом взаимодействуют между собой. Задача мониторинга пользовательских транзакций заключается в поиске узких мест приложения и диагностике проблем при ситуациях, когда метрики его прикладных составляющих в норме, но пользователи жалуются на его производительность или уровень доступности. Спектр заинтересованных в таких системах лиц достаточно широк: это и ИТ (контроль работы, обнаружение проблем, возможность восстановить сессию пользователя), и бизнес (результативность работы бизнес-подразделения, оптимальность процессов и логики работы систем). Системы CEM предлагают следующую концепцию мониторинга: наличие или отсутствие проблем определяется производительностью приложения для каждого пользователя в отдельности (что, кстати, вовсе не отменяет контроль отдельно взятых компонент) в разрезе времени выполнения транзакции и реакции приложения. Логика информационного обмена между пользователем и приложением в общем случае представлена на рис. 2.

Для случаев, когда необходимо анализировать HTTP/HTTPS-трафик между пользователем и front-end'ом приложения, на промежуточном

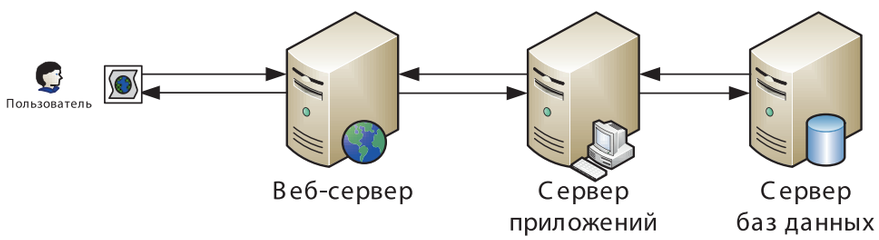


Рис. 2. Логика информационного обмена между пользователем и приложением

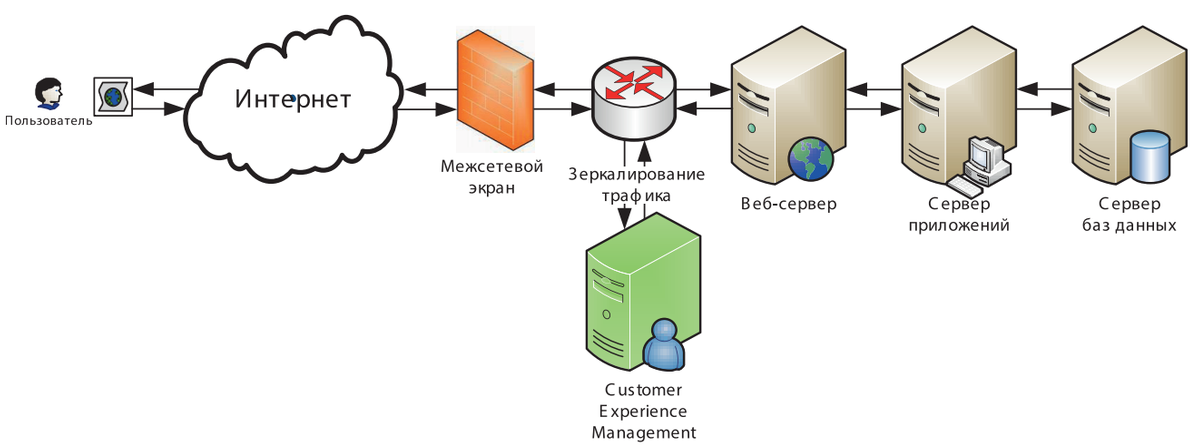


Рис. 3. Принципиальная схема зеркалирования трафика на CEM-приложение

маршрутизаторе настраивается зеркалирование трафика на сервер с CEM-приложением подобно тому, как изображено на рис. 3.

В свою очередь сервер CEM может быть расположен как на физической, так и на виртуальной инфраструктуре. Абсолютное большинство CEM-систем поставляется в виде appliance, т.е. решения, полностью готового к имплементации. Для зеркалирования трафика на физический сервер чаще всего используется «железный» коммутатор, в виртуальной среде — соответственно, виртуальный. По опыту можем сказать, что последний вариант наиболее распространен в среде VMware, да и веб-серверы бизнес-приложений тоже, как правило, виртуализированы. На рис. 4 схематично изображен механизм зеркалирования трафика на виртуальный и физический

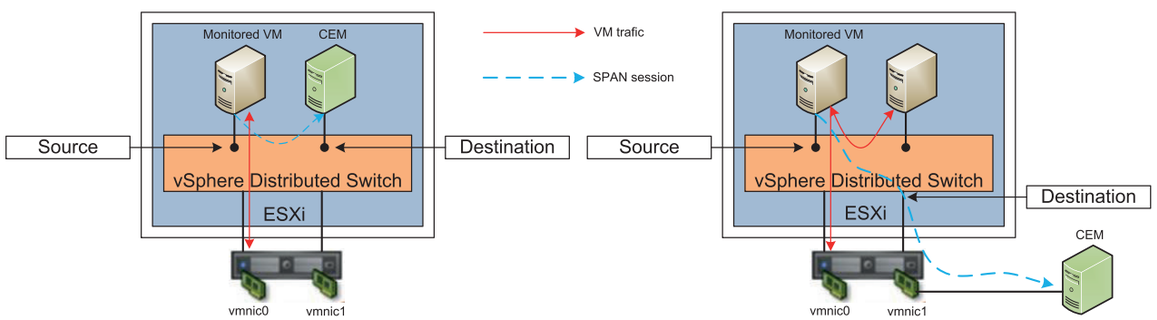


Рис. 4. Схема зеркалирования трафика в среде виртуализации для физического и виртуального размещений CEM-приложения

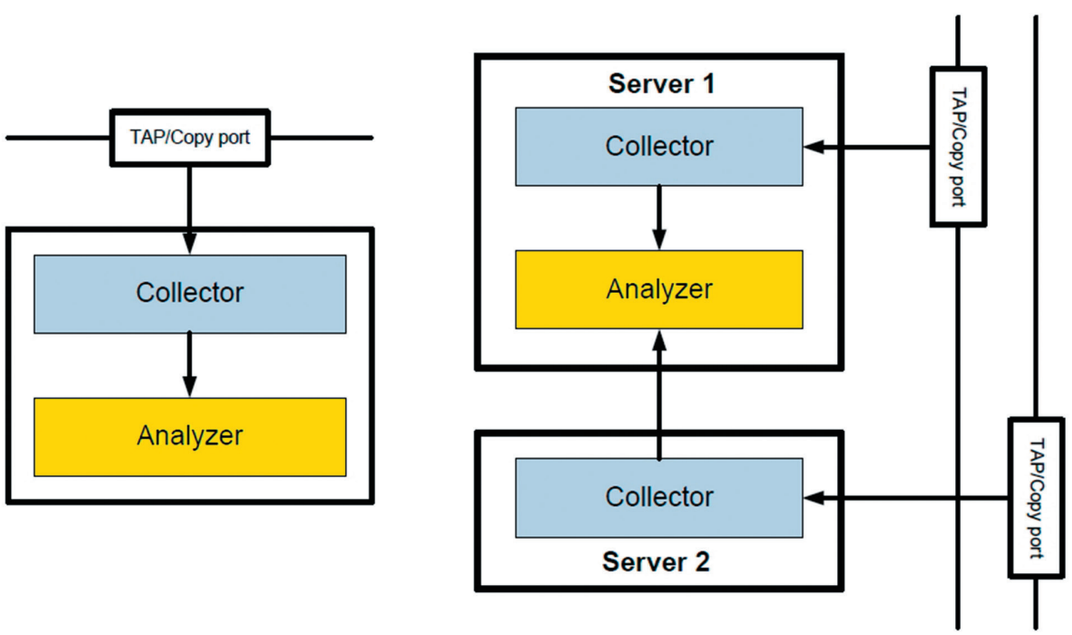


Рис. 5. Пример масштабирования CEM-приложения

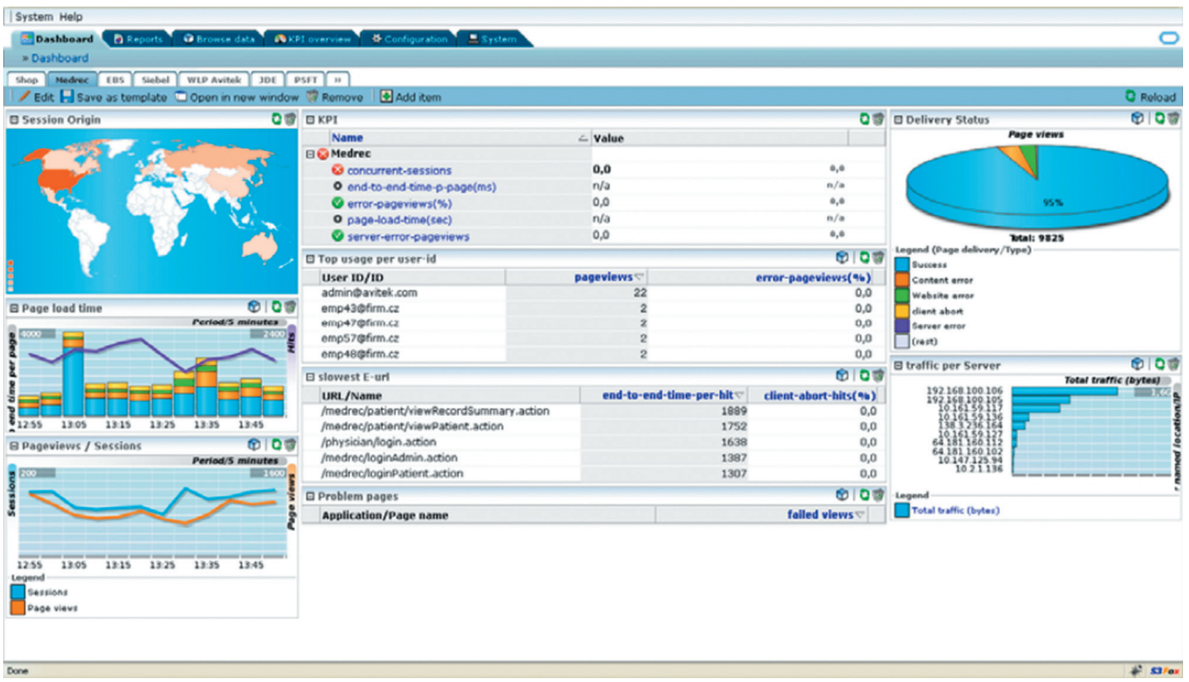


Рис. 6. Пример dashboard'а CEM-приложения

серверы CEM, когда в рамках виртуального свитча (vDS) включен смешанный режим (Promiscuous Mode). Его включение позволяет перенаправить на сервер CEM трафик со всех порт-групп, определенных на этом свитче.

Нельзя не упомянуть о том, что средства CEM могут масштабироваться в соответствии с требованиями компании. На рис. 5 приведены CEM-приложения, состоящие из нескольких компонент (в данном случае анализатор и коллектор), которые могут быть расширены. При значительном объеме поступающего трафика (или его приеме с различных веб-серверов) коллектор выносится на отдельный сервер.

Выше мы говорили только о решениях по захвату HTTP/HTTPS-трафика, однако стоит упомянуть и о технологиях

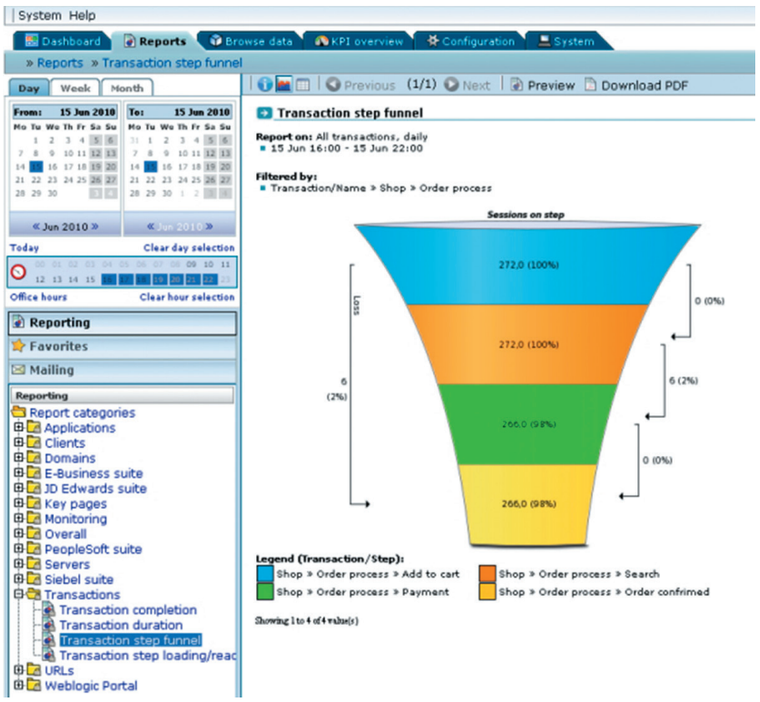


Рис. 7. Пример визуализации сценария пользовательской активности

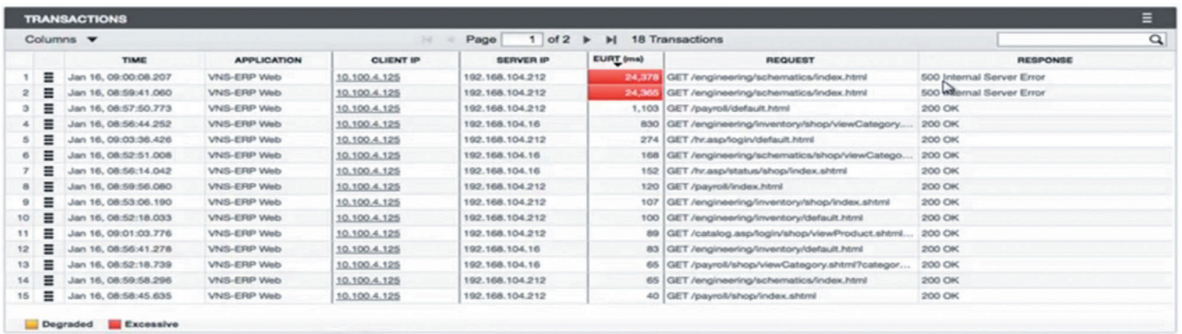


Рис. 8. Табличное пошаговое представление активности пользователя

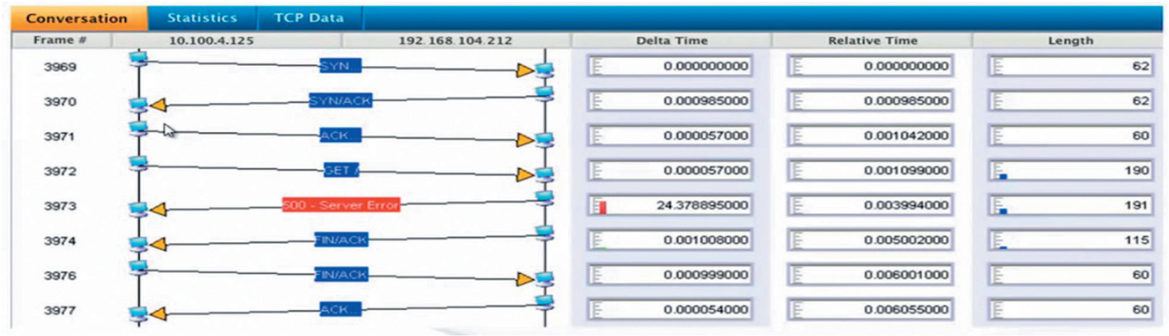


Рис. 9. Детализированное представление пользовательского действия

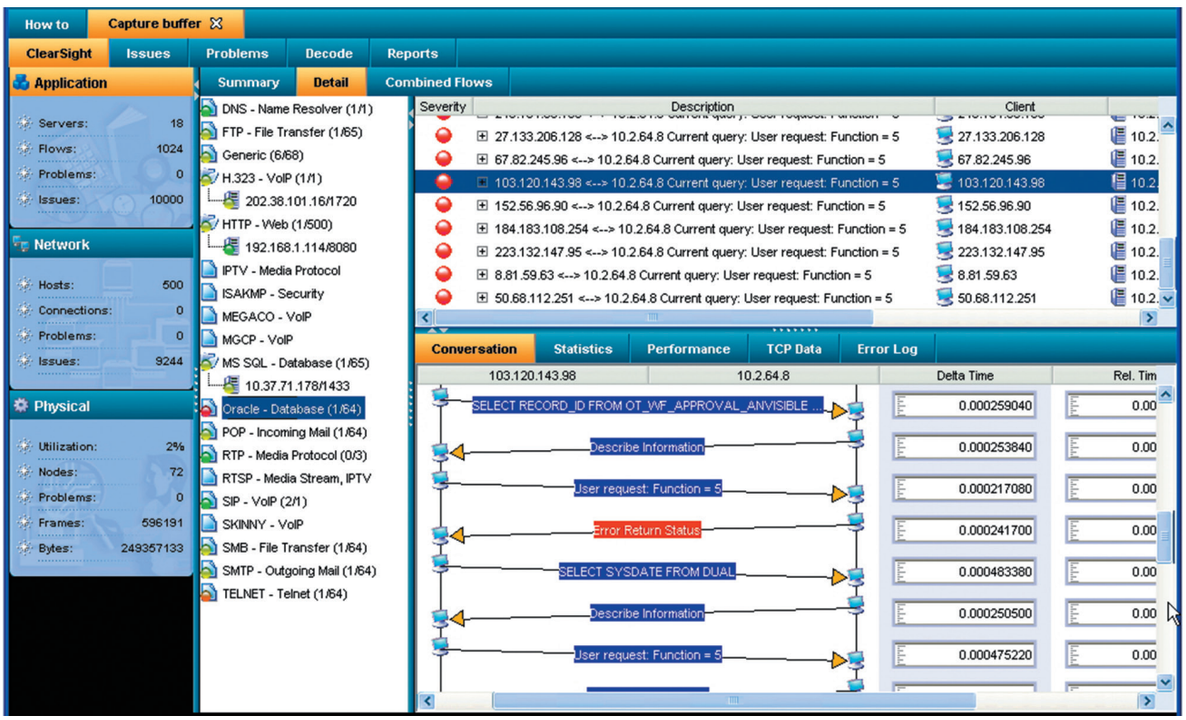


Рис. 10. Пример интерфейса AANPM-приложения

AANPM — Application-Aware Network Performance Management. Это ориентированные на приложения средства сетевого мониторинга, которые являются продвинутой версией CEM-решений и могут захватывать не только HTTP/HTTPS-трафик, но и, например, запросы к БД или VoIP-пакеты (что немаловажно, с дальнейшим воспроизведением разговора).

ВИЗУАЛИЗАЦИЯ РЕЗУЛЬТАТА

Теперь, когда с механикой приема данных все более-менее понятно, перейдем к описанию логики работы подобных решений. Для снижения паразитной нагрузки на приложение мониторинга перед началом его использования обязательно задаются адреса источника и получателя трафика, а также сетевой порт. После начала приема трафика можно приступать к созданию dashboard'ов. В этом плане всё ограничивается только требованиями к контролируемым метрикам, т.к. для построения dashboard'ов можно обращаться к разнообразной статистике (тип браузера, местоположение пользователя, ID сессии пользователя, количество ошибок при загрузке и многое другое, что характеризует сессию). Пример такого dashboard'а представлен на рис. 6.

Также существует возможность задавать заранее определенный сценарий пользовательской активности, т.е. создавать так называемый «стакан» (см. рис. 7). По нему мы можем определить, например, какое количество пользователей положило заказ в корзину и дошло до этапа его оплаты, какова сумма покупки, почему клиент покинул страницу перед оплатой и т.п.

Таким образом, можно заглянуть в одну из сессий и пошагово увидеть пользовательские действия (см. рис. 8).

Затем мы можем определить, на каком именно этапе у пользователя возникла, например, ошибка 500, когда он покинул сценарий и не стал заказывать товар или услугу (рис. 9).

Вернемся к AANPM. На рис. 10 в центральном фрейме можно увидеть примеры поддерживаемых типов трафика, в частности, приведен проблемный запрос в БД Oracle, который в итоге является причиной замедления работы всего бизнес-приложения. Таким образом, CEM можно назвать «кирпичиком», который в числе прочих закладывает крепкий фундамент теплых отношений конечного пользователя и ИТ. Среди таких «кирпичиков» решения:

- Real User Monitor, HP
- AppVisibility Manager, BMC Software
- Application Delivery Analysis, CA
- Dynatrace User Experience Management, Compuware
- nGenius Performance Manager, NetScout
- Visual TruView, Fluke Networks
- SteelCentral, Riverbed Technology
- Real User Experience Insight, Oracle

Ключевыми отличиями этих продуктов являются наличие набора поддерживаемых протоколов для анализа, а также поддержка специфических приложений. По первому критерию считаем нужным выделить AANPM-решение Visual TruView, которое, помимо обычных HTTP/HTTPS, позволяет анализировать протоколы IP-телефонии, потокового видео, SMTP, SMB и др. А решение Real User Experience Insight от Oracle позволяет создавать специальные dashboard'ы, учитывающие логику работы таких специфичных бизнес-приложений, как Siebel, E-business Suite, Fusion, PeopleSoft.

В заключение отметим, что CEM-решения являются логичным технологическим продолжением сетевых анализаторов трафика, в том числе NetFlow-анализаторов, которые в большинстве своем предоставляют возможность логировать трафик в хранилище и этим ограничиваются. CEM-системы в отличие от них имеют понятную визуализацию, которую с легкостью можно оптимизировать под требования компании. В подавляющем большинстве случаев они позволят решить множество ИТ- и бизнес-задач и в итоге дадут возможность разговаривать с пользователем на одном языке. Во многих спорных ситуациях именно благодаря этому инструменту можно будет четко понимать, где и что именно происходит, не тратить дополнительное время на диагностику проблемы, а приступать к ее решению, как только о ней стало известно. JI

ШЕРЛОК ПРОТИВ BIG DATA

Шерлок Холмс: Но я-то не каждый, Ватсон, поймите: человеческий мозг — это пустой чердак, куда можно набить всё, что угодно. Человек тащит туда нужное и ненужное. И наконец наступает момент, когда самую необходимую вещь туда уже не запихнёшь. Или она запрятана так далеко, что ее не достанешь. Я же делаю всё по-другому. В моём чердаке только необходимые мне инструменты. Их много, но они в идеальном порядке и всегда под рукой. А лишнего хлама мне не нужно.

Художественный фильм «Шерлок Холмс и доктор Ватсон»

АЛЕКСЕЙ НИКОЛАЕВ,
руководитель департамента систем управления компании «Инфосистемы Джет»

Современный мир становится все сложнее, в том числе растут сложность информационных технологий и зависимость бизнеса от них. Это касается и эксплуатации современных распределенных многокомпонентных систем — она требует анализа больших объемов информации за короткое время.

Допустим, мы определили проблему доступности приложения на стороне пользователя. При этом все контролируемые инфраструктурные метрики в

норме. Как решить задачу обнаружения корневой причины недоступности? Типичный сценарий — подключение одного или нескольких экспертов, осуществляющих поиск причины вручную, методом анализа предыдущей практики, журнальных файлов, моделирования ситуации и пр.

Классические средства мониторинга вряд ли помогут на этом этапе — собираемые ими данные ограничены, фрагментарны. Обычно на мониторинг ставятся компоненты ИТ-систем, выход из строя которых можно предположить заранее: мы не можем контролировать все возможные аспекты работы приложения, поскольку ограничены возможностями вычислительной платформы и объемом хранимых данных. Кроме того, у классических систем ограничены функции корреляции собираемой информации. Полнофункциональные детальные сервисно-ресурсные модели, которые необходимы для анализа данных мониторинга, крайне сложны в сопровождении и часто не используются.

Следствием всего этого является потеря времени на поиск причин проблем, на анализ и сопоставление дополнительной информации. Но не все так плохо — развитие, появление новых технологий не только усложняет жизнь системам, но и обогащает их новыми инструментами. В нашей статье мы хотим сосредоточиться на одном из подобных примеров — применении методов работы с Большими Данными в средствах мониторинга ИТ.

Для начала необходимо определиться с терминами. С появлением технологии анализа Big Data в жизнь профессионального сообщества вошло новое понятие — Operations Intelligence (OI). Это класс аналитических решений, обеспечивающих комплексную обработку и визуализацию данных (значений параметров, потоков событий, бизнес-операций) из различных источников в режиме, близком к реальному времени.

Системы OI многокомпонентны: за рамками нашей статьи останутся обработка сложных событий (Complex Event Processing), мониторинг бизнес-операций (Business Activity Monitoring) и др. Сосредоточимся на основных технологических решениях, обеспечивающих совместный оперативный анализ данных различных типов (временные ряды, текстовые события и т.д.). Специализированных игроков на данном рынке пока немного — это слишком молодая технология, требующая достаточно больших вложений в ее разработку и развитие. В качестве примера можно назвать решения, предлагаемые компаниями Splunk, Hewlett-Packard, IBM. Их общая черта — применение компонентов анализа Big Data в мониторинге ИТ.

> Отметим, что решения класса IT Operations Analytics не являются заменой оперативных средств мониторинга, сообщающих нам о явных и конкретных сбоях. Их место – над этими системами. Они являются инструментом аналитика, работающего с проблемами, но могут применяться и в операционном мониторинге.

Как уже было сказано, с момента создания систем мониторинга как класса программных решений и вплоть до сегодняшнего дня мы жили в условиях ограничения вычислительной мощности используемых платформ. Для оперативного мониторинга выбирались только те данные, влияние которых на целевую функцию контролируемой системы было понятно и известно. Попытки сбора и обработки всей доступной информации приводили к существенному увеличению времени анализа, т.е. фактически переводили систему в раздел offline-аналитики, а это, в свою очередь, нивелировало смысл её создания. В итоге мы получали ограниченное решение, позволяющее выявить и, возможно, отранжировать по значимости потенциальные причины возникновения проблем. Далее был необходим глубокий ручной

анализ журнальных файлов, сочетания нетипичных показателей и др.

Итак, что же изменилось? Ряд разработчиков, исторически или унаследованно занимавшихся технологиями анализа и обработки, обратили внимание на схожесть задач мониторинга и анализа Big Data (разные данные, большие объемы, требования к скорости). В результате были созданы системы нового типа — IT Operations Analytics. В качестве примера рассмотрим решение от компании Hewlett-Packard. Его основой являются два технологических компонента компании HP — аналитическая база данных HP Vertica и ПО управления журналами HP ArcSight. Обобщенная архитектура решения представлена на рис. 1.

Состав решения:

- OpsAnalytics Collector, обеспечивающий сбор данных из различных источников. В их роли выступают:
  - файлы CSV;
  - ПО мониторинга компании HP: HP SiteScope, HP Operations Manager и OMi, HP BPM и др.;
  - средства мониторинга журнальных файлов: HP ArcSight Logger (входящий в состав решения) и Splunk;
- HP ArcSight Logger, отвечающий за анализ журнальных файлов по различным принципам и предоставление структурированной информации в OpsAnalytics Collector (результаты мониторинга), а также, по запросу, серверу OpsAnalytics Server (в «сыром» виде при выполнении пользователями системы соответствующих поисков);
- HP Vertica Datawarehouse — БД, обеспечивающая долговременное хранение данных в виде, адаптированном к выполнению аналитических запросов различного типа. Стоит отметить, что эти данные сжаты, в результате чего обеспечивается ощутимая экономия дискового пространства по сравнению с традиционными базами данных;
- OpsAnalytics Server — модуль, отвечающий за предоставление функций HP Operations Analytics пользователям системы.

Основные характеристики OI-систем:

- мониторинг, обнаружение событий и визуализация информации в режиме, близком к реальному времени;
- многомерный анализ данных:
  - выявление корневых причин;
  - анализ временных рядов и прогнозирование;
- использование технологий анализа Big Data.

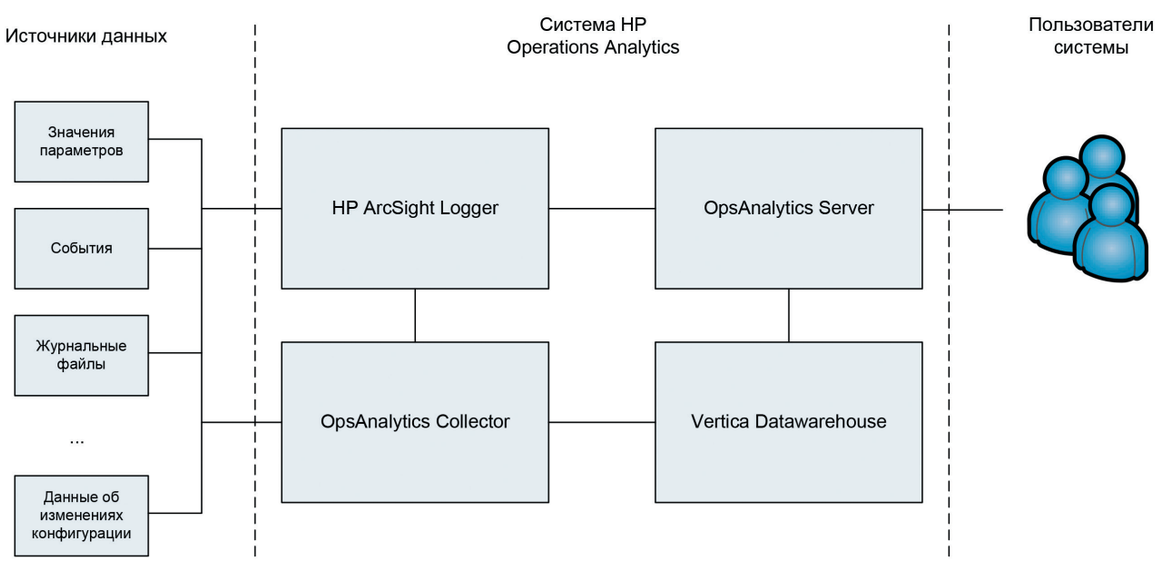


Рис. 1. Архитектура системы HP Operations Analytics

В соответствии с объемом предполагаемой к обработке информации компоненты решения могут масштабироваться на несколько узлов: новые могут быть добавлены по мере роста объема данных и количества выполняемых аналитических запросов.

Предоставляемый функционал включает в себя несколько основных блоков: поиск информации по различным критериям, визуальную и прогнозную аналитику, а также анализ журнальных файлов.

Визуально интерфейс пользователя представляет собой настраиваемый под конкретные задачи портал. Он может формировать состав представлений в процессе выполнения анализа и сохранять их для последующей работы. Одной из интересных особенностей решения является наличие так называемой «машины времени» (Time machine). С ее помощью можно оперативно получать требуемую информацию за заданный период времени без необходимости выполнения последовательных выборок для каждого блока данных. «Машина времени» применяется одновременно для всех выводимых на экран метрик и событий. Наличие подобной функции позволяет «на лету» выполнять совместный анализ необходимых данных.

В системе реализован поиск по различным контекстам. Например, можно одновременно выполнять выборки по большому количеству критериев: по приложению (с учётом топологии, полученной из внешних источников), серверу, географическому положению элементов инфраструктуры и т.д. Например, можно находить причины проблем в работе банкоматов за счет совместного анализа данных об их доступности, о работе сети передачи данных и изменениях погоды.

На основе метрик, собранных в базе данных HP Vertica Datawarehouse строятся прогнозы изменения их значений и визуализируются отклонения от нормальных значений за заданный период (baseline).

Возможности модуля HP ArcSight Logger по анализу журнальных файлов достаточно хорошо известны. Ключевой особенностью его применения в составе HP Operations Analytics является превращение неструктурированных или слабоструктурированных данных в измеряемые метрики, доступные для совместного анализа с метриками доступности и производительности.

Отметим, что с точки зрения «чистых» функций (поиск, прогнозирование, визуализация сводной информации) система не несет в себе ничего нового. Все эти задачи так или иначе решаются в большинстве классических средств мониторинга. Ключевые отличия систем, вобравших в себя опыт работы с Большими Данными, — возможность хранения огромного количества данных и высокая скорость выполнения аналитических запросов. Ранее анализ работы распределенного приложения занимал часы и дни, был связан с обработкой десятков тысяч событий и записей в журналах, значений сотен метрик. Теперь — с использованием технологий анализа Big Data — эти операции можно выполнять практически в реальном времени. JI

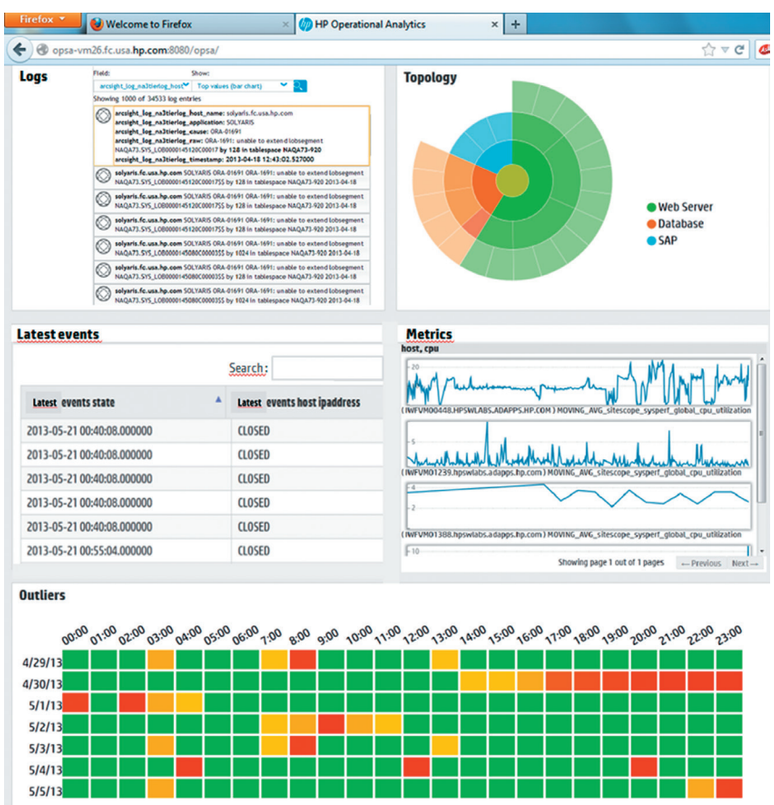


Рис. 2. Интерфейс системы