

Основы расследования киберинцидентов

Windows® IT Pro/RE

№9 СЕНТЯБРЬ 2018 | WWW.WINDOWSITPRO.RU | ИНФО ДЛЯ ИТ-ПРО

Мобильная
версия

App Store



Google play



ИЗУЧАЕМ поведение данных

ISSN 1563-101X



18009



9 771563 101008

Издание для специалистов, интересующихся технологиями компании Microsoft.

Главный редактор: Д. Ю. Торопов (toropovd@osp.ru)
Ответственный редактор: Е. Петровичева
Корректор: Л. Терemenko
Верстка и дизайн: О. Шуранова
Номер также готовили: Е. Овсянников
Т. Евдокимова, А. Китаев, А. Федотов,
Н. Басалова, Ю. Власов, Д. Шепкин, А. Адзиев

Адрес для писем: 123056, Москва, а/я 82
Телефоны: (495) 725-4780/83, (499) 703-1854
Факс: (495) 725-4783
E-mail: windowsitpro@osp.ru

© 1999-2018 Издательство «Открытые системы»
© 1999-2018 Penton Media, Inc.

Журнал зарегистрирован в Роскомнадзоре.

Свидетельство о регистрации средства массовой информации ПИ № ФС 77-63737 от 16 ноября 2015 г.

Дата выхода в свет — 18.09.2018 г.

Цена свободная. Выходит 12 раз в год.



ОТКРЫТЫЕ СИСТЕМЫ
Open Systems Publications

Адрес редакции и издателя:

ООО «Издательство «Открытые системы»
127254, Москва, пр-д Добролюбова, д. 3,
стр. 3, комн. 13.

Президент М. Е. Борисов

Генеральный директор Г. А. Герасина

Директор ИТ-направления П. В. Христов

Коммерческий директор Т. Н. Филина

Подписные индексы:

Объединенный каталог «Пресса России» — 38185,
«Каталог российской прессы» — 99483,
ФГУП «Почта России» — П2337
Отпечатано в типографии ООО «Антарес»
107113, г. Москва, ул. 2-я Рыбинская,
д. 13, оф. 42

Тираж: 6900 экз. — печатная версия,
3280 экз. — PDF-версия

Редакция не несет ответственности за содержание рекламных материалов. Все права защищены. Полное или частичное воспроизведение или размножение каким бы то ни было способом материалов, опубликованных в настоящем издании, допускается только с письменного разрешения ООО «Издательство «Открытые системы».

Windows®, Windows Vista® и Windows Server® — зарегистрированные торговые марки корпорации Microsoft. Название Windows IT Pro используется Penton Media, Inc. в соответствии с соглашением с владельцем торговой марки. Название Windows IT Pro/RE используется ООО «Издательство «Открытые системы» по лицензионному соглашению с Penton Media, Inc. Windows IT Pro/RE — независимое от корпорации Microsoft издание. Корпорация Microsoft не несет ответственности за редакционную политику и содержание журнала.

Редакция оставляет за собой право не вступать в переписку.

Отобранные для публикации письма редактируются в соответствии с терминологическими нормами, принятыми в издательстве.

Названия продуктов и компаний, упомянутых в журнале, могут быть товарными знаками их владельцев.



Penton Media, Inc.

ИТ И БИЗНЕС

2 Cloudflare делает ставку на ARM-серверы

МЭРИ БРАНСКОМ

4 Почему мейнфреймы не скоро уйдут в прошлое

КРИСТИН ХОЛЛ

7 Добытчики криптовалюты присматриваются к Docker

ТОМ ХЕНДЕРСОН

8 Как монетизировать открытый проект

КРИСТИН ХОЛЛ

ТЕМА НОМЕРА

12 Области в PowerShell

СЕРГЕЙ ВАСИН

27 Хранение данных в «облаке»

БРАЙЕН ПОУСИ

ПЛАНИРОВАНИЕ

28 Сети 5G: чего ожидать и как подготовиться к внедрению

КРЕЙГ МАТИАС

ВВОДНЫЙ КУРС

30 Основы расследования киберинцидентов

ВЛАДИМИР БЕЗМАЛЫЙ

WINDOWS ИЗНУТРИ

34 Добавляем новые возможности в контекстное меню Windows

ДМИТРИЙ БУЛАНОВ

ЛАБОРАТОРИЯ

41 Оптимизация производительности Office 365 и больших профилей

ИЛЛЮСТРАЦИЯ НА ОБЛОЖКЕ TOMASZ WOZNIAK® (FOTOLIA.COM)



Cloudflare

делает ставку на ARM-серверы

По мнению главного управляющего, для рабочих нагрузок Cloudflare архитектура ARM обойдется дешевле, даже если процессоры x86 будут бесплатными

Компания Cloudflare, которая эксплуатирует сеть доставки контента, используемую также для служб защиты от DDoS для веб-сайтов, взялась за расширение своей глобальной сети центров обработки данных (CDN). Такие сети обычно состоят из компактных узлов, которые должны быть расположены во многих местах по всему миру.

По мере расширения компания делает ставку на архитектуру ARM, альтернативу архитектуре процессоров Intel x86, которая занимала господствующее положение на рынке центров обработки данных в течение многих десятилетий.

Cloudflare только что открыла новый центр обработки данных в Макао, Рияде и Рейкьявике. Действуют центры в Стамбуле, Катманду, Пномпене, Бейруте и родном городе главного управляющего Мэттью Принса, Солт-Лейк-Сити. «Наша цель в ближайший месяц — 31 новый сайт в течение 31 дня, и 22 из них уже оснащены оборудованием и почти готовы к запуску в эксплуатацию», — заявил он. Это амбициозная цель, которой, как признает управляющий, компания может и не достичь: в 2012 году в рамках аналогичного проекта появилось 10 центров обработки данных за 30 дней, но Принс ожидает, что будет достигнут по крайней мере близкий результат. Добавление многих новых центров позволит компании построить сеть, устойчивую в отношении любой атаки типа «отказ в обслуживании» (DDoS), нацеленной против GitHub, вроде случившейся в феврале ([https://www.](https://www.wired.com/story/github-ddos-memcached/)

[wired.com/story/github-ddos-memcached/](https://www.wired.com/story/github-ddos-memcached/)). Это была крупнейшая из когда-либо зарегистрированных атак такого типа, но Cloudflare регулярно сталкивается с масштабными атаками против своих клиентов, как утверждает Принс.

Один из способов, применяемых Cloudflare для сокращения затрат, состоит в соединении узлов сети с локальными поставщиками услуг Интернета. «Доставка оборудования в удаленные районы обходится немного дороже, поэтому капитальные затраты слегка возрастают, но стоимость полосы пропускания безусловно перекрывает этот изъяс. И если вы приедете туда, то сможете напрямую подключиться к поставщикам услуг Интернета и обмениваться трафиком бесплатно», — поясняет Принс.

Расходы также снижаются благодаря предварительной настройке маршрутизаторов в новых центрах обработки данных (обычно на существующих площадках для размещения серверов заказчика), благодаря которой инженеры могут дистанционно настраивать и эксплуатировать серверы, выполняя загрузку PXE через VPN из ближайшего сайта Cloudflare. Многие площадки, используемые компанией, никто из сотрудников никогда не посещает.

К концу 2018 года, как отмечает Принс, компания планирует иметь центры обработки данных в 200 городах по всему миру (в начале марта их было 125). «На этом этапе примерно 95% населения мира будет жить в городах с центрами обработки данных Cloudflare, — считает Принс. — Мы постоянно приближаем оборудование



Главный управляющий Cloudflare Мэттью Принс и управляющий производственной деятельностью Мишель Цатлин на конференции TechCrunch в Сан-Франциско

к потребителю. Мы выясняем, где находится крупный населенный центр, и движемся туда».

С появлением беспроводных сетей 5G такой подход приобретает еще большее значение, так как приложения следующего поколения раздвигают границы возможностей мобильных устройств. «Возникает вопрос, в какой степени мобильные устройства способны воспользоваться окружающей вычислительной инфраструктурой, чтобы расширить свою функциональность», — говорит Принс.

Отказ от Intel

Чтобы упростить дальнейшее расширение, специалисты Cloudflare запланировали крупное архитектурное изменение. В скором времени компания начнет развертывать в центрах обработки данных серверы на базе ARM. Принс ожидает, что альтернативу x86 будет дешевле приобрести и эксплуатировать благодаря меньшему энергопотреблению и особенностям рабочей нагрузки Cloudflare.

Компания уже отказалась от SSD-накопителей Intel, выяснив, что их рабочие характеристики не соответствуют ее требованиям. Все серверы Cloudflare используют SSD-накопители для кэширования данных с защищаемых веб-сайтов. «Скорее всего, к четвертому кварталу 2018 года мы уже не будем ничего покупать у Intel, — полагает Принс. — Думаю, в настоящее время мы достигли такого состояния, что можем полностью перейти на ARM. Как выяснили наши аналитики, даже если бы компания Intel давала нам микросхемы бесплатно, переход на ARM все равно был бы целесообразен благодаря экономии энергии».

Это утверждение вряд ли справедливо для любого центра обработки данных, но ARM подходит для рабочей

нагрузки Cloudflare. Микросхемы с низким потреблением энергии также будут уместны в городах, где серверы размещаются на старом и менее эффективном оборудовании.

«Каждый запрос, поступающий в Cloudflare, независимо от остальных запросов, поэтому нам нужно как можно больше ядер на единицу мощности, — объясняет Принс. — Единственная метрика, которой мы уделяем внимание, — это число ядер на ватт и число запросов на ватт». По этому показателю ARM-процессоры Qualcomm Centriq выглядят очень хорошо. «У них очень высокое соотношение количества ядер к потреблению энергии в моделях поколения 1, и в поколении 2 их преимущество еще больше возрастет», — считает Принс.

Компания Qualcomm начала выпускать Centriq, предназначенный для гипермасштабируемых «облачных» платформ, в ноябре 2017 года. Гипермасштабируемые приборы, которые занимают огромную долю рынка микросхем для серверов, широко используют архитектуру ARM. Так, в 2017 году компания Microsoft заявляла, что в будущем эта архитектура сможет обеспечивать половину всей ее рабочей нагрузки.

Команда Cloudflare (в которую входят бывшие инженеры Intel) первоначально не предполагала, что процессоры ARM так хорошо подойдут для ее нужд, особенно учитывая, что служба построена на основе открытого программного обеспечения. «Инженеры начали тестировать рабочие нагрузки и были поражены. Все оказалось гораздо проще, чем мы думали, — подчеркнул в заключение своего выступления Принс. — Производительность уже стала выше, а экономия энергии просто невероятная».



Мэри Бранском

Почему мейнфреймы не скоро уйдут в прошлое

Бывший главный инженер корпорации IBM поясняет, в каких обстоятельствах решение о приобретении мейнфрейма имеет смысл и какие преимущества получает покупатель

Кристин Холл

В последнем отчете о доходах IBM наконец отмечается рост прибыли, впервые за последние пять лет. Как и следовало ожидать, отчасти эта тенденция определяется поступлениями от операций в «облаке», которые год от года росли на 24% и сейчас составляют 21% доходов корпорации. Однако рост подпитывается еще из одного важного источника: доходов от торговли мейнфреймами. По словам представителей компании, поступления от продажи мейнфреймов серии Z выросли на 70%.

Кто-то, возможно, уподобит такой поворот событий возвращению к электронным лампам там, где давно используются транзисторы. Но на самом деле это лишь одна из примет меняющегося ландшафта в мире информационных технологий.

Разумеется, современные мейнфреймы — это не те машины из прошлого века, которые управлялись перфокартами и занимали целые комнаты. В наши дни эти устройства, чаще всего функционирующие под управлением операционной системы Linux, нашли новую нишу в центрах обработки данных, где берут на себя наиболее трудоемкие операции. Вы знаете, на какой платформе выполняется самая мощная база данных Oracle? На мейнфрейме Linux! А самая крупная на нашей планете система SAP? Опять-таки на мейнфрейме с операционной системой Linux.

«До переселения Linux на мейнфреймы эти машины покупали прежде всего те компании, у которых подобные решения уже имелись, — разъяснил бывший главный инженер корпорации IBM Леонард Санталючия. — Они обычно дожидались выхода в свет новой версии и обновлялись до ее уровня, потому что после этого система обходится дешевле и работает быстрее».

Как рассказал Санталючия, когда появился Linux, открылись возможности для потребителей, которые в иных обстоятельствах не обратили бы на мейнфреймы никакого внимания: «Пожалуй, добрых три или четыре сотни новых клиентов, никогда до того не работавших с мейнфреймами, приобрели такие системы. У них в центрах обработки данных нет ни старых мейнфреймов, ни модернизированных. Они просто покупали новые».

Хотя Санталючия — главный инженер компании Vicom Infinity, занимающейся прежде всего продажей продуктов IBM, на конференции All Things Open он присутствовал в качестве председателя проекта Open Mainframe организации Linux Foundation. Санталючия знает мейнфреймы IBM, что называется, вдоль и поперек. Он проработал в корпорации 27 лет, причем последние восемь — в должности главного инженера входящей в состав компании группы по системам и технологиям.

«Операционная система Linux появилась на мейнфреймах еще в 1999 году