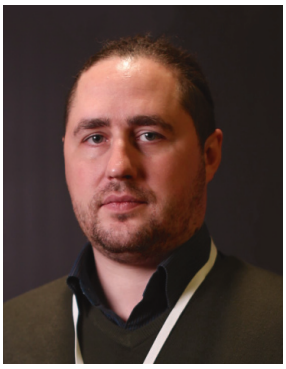
Hitachi: что нужно бизнесу сегодня?

Классика СХД



Виталий Смык – консультатнт-эксперт, Hitachi Data Systems

На данный момент на рынке хранения данных можно встретить несколько вариантов доступа к самим данным. Если идти от сложного к простому, то верхушкой айсберга хранения является объектное хранение данных. Объектный принцип обеспечивает значительно большие масштабируемость (на этих принципах построены, к примеру, Amazon, Google и т.д.). Разделение на ноды – программно-аппаратные части хранилища – позволяет добиться этой самой управляемости и масштабируемости. Но при имеющихся преимуществах такой вариант хранения имеет и минусы. Основным недостатком объектных хранилищ является необходимость иметь некоторое количество хранимых копий объектов, чтобы осуществить определённый уровень защиты данных. Но главным плюсом и одновременно недостатком на сегодня является доступ к данным по объектным протоколам (S3, Rest API). Если консьюмерский рынок потребления таких ресурсов только выигрывает, за счёт дешёвого хранения (использования компонентов массового производства – серверы, жесткие диски, коммутационное оборудование), то доступ к данным бизнес-приложений и прикладного ПО не имеют какой-либо поддержки объектных протоколов и имеют очень высокие требования по гарантированной производительности и задержкам к доступу данных.

Следующий вариант – это файловый доступ к данным. Тут мы имеем уже больше отработанных решений и технологий для корпоративного класса систем. При всех плюсах и возможностях файлового доступа к данным, он не везде требуется и не везде подходит.

Наверное, самым распространённым и востребованным является блочный доступ к данным. В рамках этого варианта мы можем разными путями осуществлять транспорт этих данных (разные технологии передачи и протоколы). Будет безошибочным предположение, что самым распространённым транспортом будет Fibre Channel.

Согласно опросу поставщиков систем хранения данных, Fibre Channel – это лучшая технология сетей хранения данных для заказчиков, использующих all flash массивы, а также гибридные системы. Восемь из 11 поставщиков систем хранения данных, присутствующих на мировом рынке производителей СХД, заявили, что большинство их корпоративных клиентов используют коммутаторы и адаптеры Fibre Channel с их all flash массивами и гибридными системами (которые объединяют твердотельные диски – SSD и жесткие диски). Некоторые вендоры (в том числе и Hitachi Data Systems) заявили, что многие заказчики переходят на FC с пропускной способностью 16 Гбит/с (с переходом на all flash массивы). Данная инфраструктура FC-сети (SAN) уже давно сложившаяся часть центра обработки данных любого заказчика. Через этот сегмент сети передаётся всё больше и больше данных. Ввиду внедрения аналитических систем и накопления больших объёмов данных (Big Data) данный процесс будет нарастать лавинообразно.

Уже достаточно давно на рынке FC-сетей доминирует компания Brocade. По данным Dell'Oro Group (*http://www.delloro.com/products-and-services/san*), Brocade занимает более 70% всего рынка SAN. Динамично развиваясь и быстро реагируя на потребности рынка, компания на данный момент предлагает уже 6-е поколение оборудования для коммутирования с FC-интерфейсом. Предвосхищая рынок и потребности заказчиков, компания уже сейчас предлагает воспользоваться скоростью передачи данных 32 Гбит/с. Являясь основным партнёром компании Brocade и технологическим лидером рынка систем хранения данных, компания Hitachi Data Systems сразу вывела на рынок СХД с интерфейсом FC 32 Гбит/с. Будучи лидером рынка (по данным Gartner – *https://www.hds.com/ext/magic-quadrant-for-general-purpose-disk-arrays.html*), компания HDS, как никто другой, понимает возросшую важность пропускной способности канала данных от хоста к СХД, так как это напрямую влияет на те объёмы и скорости обработки, которые требуются современному бизнесу. Fibre Channel изначально разрабатывался как высокоскоростная сеть, пригодная для работы в реальном времени. Если заглянуть более глубоко в технику, то в отличие от Ethernet, Fibre Channel при подключении порта обязательным является выполнение login, так что коммутатор о всех портах сети всегда знает, какой порт где находится и что может. Когда в коммутатор Fibre Channel приходит кадр данных, то коммутатор уже знает, где находится адресат и куда этот кадр маршрутизировать. Ethernet коммутатор после прихода кадра сначала ищет, где находится адресат, и только после его ответа посылает ему этот кадр, и, если истекло время старения, коммутатор Ethernet вновь будет искать маршрут для другого кадра данных от того же источника к тому же адресату. Все эти накладные расходы приводят к повышению задержек (latency), что на корпоративном рынке доступа к данным является не только всё более ужесточающим фактором, но и в некоторых случаях недопустимым. Здесь стоит наверно упомянуть отдельный класс БД для которых это основное свойство, так называемые in-memory БД (один из распространённых примеров – SAP HANA). Для такого подхода пришлось пересматривать структуры таблиц, технологии индексирования, механизмы оптимизации запросов и т. д. В некоторых случаях, таких как анализ потоковых данных и работа с Big Data, выгоднее вообще отказаться от реляционной модели. Но поскольку традиционные СУБД были оптимизированы для дисковых систем хранения и это уже есть в наличии у всех заказчиков, а новый подход требует новой инфраструктуры и стоимость ОЗУ для размещения данных по-прежнему еще дорогое «удовольствие», то сильного изменения рынка хранения и обработки данных мы не наблюдаем. При этом текущие технологии тоже не стоят на месте, а постоянно модернизируются и улучшаются.

Заглядывая в будущее, уже сейчас можно говорить, что FC-сети – хорошая инвестиция, так как Big Data требует, помимо объёма хранилищ, еще и скоростей и эффективности передачи данных. Развивающаяся сейчас технология NMVe (*Non-Volatile Memory Express*) – протокол доступа к твердотельным накопителям (SSD), подключенным по шине PCI Express – позволит еще быстрее обеспечить доступ к данным и при этом гарантировать минимальные задержки (что для сети FC является основополагающей характеристикой – в отличие от Ethernet). Здесь оборудование Brocade позволит сразу перейти к этой технологии и использовать FC-сеть как транспорт для NVMe.

Благодаря тесному сотрудничеству Brocade и Hitachi Data Systems, а также значительному опыту не только по построению решений для хранения больших объёмов данных, но и возможности по применению аналитических инструментов для обработки (ПО HDS – Pentaho), мы можем с уверенностью предложить готовый бизнес-инструмент для любого заказчика.

Аналитика "больших данных"

Петр Травкин – руководитель направления Big Data, Hitachi Data Systems

Учитывая высокие темпы роста рынка аналитических инструментов для обработки Big Data и решений в области промышленного интернета (IoT), Hitachi Data Systems является активным участником данного направления, предлагая современные системы на базе программного обеспечения Pentaho. Данный комплекс ПО позволяет не только собрать и обработать любые данные, но и провести глубокий анализ с применением передовых технологий, в том числе масштабируемой обработки на кластере Hadoop.

Перед организациями стоит сложнейшая задача, связанная с управлением растущими объемами все более разнообразных данных и извлечением из них ценных знаний. Система интеграции данных Pentaho Data Integration позволяет получать доступ к данным из комплексных и разнородных источников и комбинировать их с имеющимися реляционными данными для получения высококачественной готовой к анализу информации – и все это без единой строчки кода.

Помимо возможностей обработки данных, Pentaho предлагает самые передовые и мощные алгоритмы машинного обучения, а также инструменты визуализации данных. Это позволяет рядовым специалистам и аналитикам выявлять важные закономерности и корреляции, которые остаются незамеченными при использовании обычных средств анализа и создания отчетов.

Сегодня предиктивная аналитика для оптимизации работы оборудования, использующая показатели функционирования конкретных устройств, уже широко используется крупными промышленными предприятиями и транспортными компаниями. Имея в своём портфеле мощные инструменты аналитики, Hitachi Data Systems уже помогает своим заказчикам, таким как Caterpillar Marine и UK Rail, оптимизировать процессы и снижать затраты за счёт анализа Big Data и решений в области промышленного интернета (IoT) на базе платформы Pentaho. К примеру, проект Caterpillar Marine показал, что даже на первых этапах уже можно получить измеримую отдачу в $3,6 млн за год всего с 8 судов за счёт экономии топлива, своевременного ремонта, сокращения времени простоя и эксплуатации бортового оборудования в наиболее экономичном режиме.

(начало – стр. 29)

сэкономил. Чтобы написать конкурентоспособный продукт, часто приходилось пренебрегать безопасностью. Таким же образом сформировался весь современный Интернет – создание его протоколов и спецификаций породили аналогичные проблемы.

В прошлом году эти проблемы достигли критического уровня. Фактически, мы стали свидетелями беспрецедентных изменений ситуации с безопасностью Сети в целом. Хорошая иллюстрация этому – возникшая осенью 2016 года угроза Mirai, ботнета небывалой мощности, который был построен на устройствах Интернета вещей – от домашних маршрутизаторов и IP-камер до смешной «экзотики» уровня чайников с Wi-Fi. Опасность Mirai оказалась вполне реальной: на блог исследователя Брайна Кребса пришли вполне осязаемые 620 Гбит/с volumetric-атаки, а французский хостер OVH выдержал 990 Гбит/с.

Сильнее всего от Mirai пострадал DNS-провайдер Dyn, к услугам которого прибегают многие компании из списка Fortune 500. В результате атаки water torture на DNS-серверы, трафик TCP и UDP на порт 53, мощность в 1,2 Тбит/с со 100 тысяч узлов на несколько часов ушли в оффлайн крупнейшие веб-сайты мира. Защищать DNS особенно сложно. Обычно мусорный трафик приходит с десятка портов (53, 123 и т.д.). В случае с DNS-сервером закрытие 53 порта означает приостановку нормальной работы сервиса.

Сам ботнет Mirai состоял из подключённых к Интернету устройств с парами “логин пароль” по умолчанию и достаточно простыми уязвимостями. Мы полагаем, что это – лишь “первенец” в целом поколении ботнетов на основе Интернета вещей. Даже решение проблемы одного Mirai не поможет. Злоумышленники сначала просто перебирали пароли, теперь ищут уязвимости и бэкдоры, доходит до изучения кода свежей прошивки устройства на предмет возможных «дырок» с последующей их эксплуатацией в течение считанных часов.

Бум стартапов и последующий рост числа подключённых устройств — это новое поле богатых возможностей, где можно создать не один ещё более крупный и опасный ботнет. В 2016 году внезапно появился считавшийся недостижимым терабит в секунду.

Одновременно заметно упал уровень необходимого опыта и знаний для организации DDoS атак. Сегодня для осуществления удачной атаки даже на крупные сайты и приложения достаточно видеоинструкции на YouTube или немного криптовалюты для оплаты услуг сервиса типа booter. Поэтому в 2017 году самым опасным человеком в сфере кибербезопасности может оказаться, например, обычный подросток с парой биткойнов в кошельке.

Амплификация

Для увеличения мощности атак злоумышленники амплифицируют атаки. Атакующий увеличивает объём отсылаемого «мусорного» трафика путём эксплуатации уязвимостей в сторонних сервисах, а также маскирует адреса реального ботнета. Типичный пример атаки с амплификацией – это трафик DNS-ответов на IP-адрес жертвы.

Другой вектор — Wordpress, повсеместный и функциональный движок для блогов. Среди прочих функций в этой CMS есть функция Pingback, с помощью которой автономные блоги обмениваются информацией о комментариях и упоминаниях. Уязвимость в Pingback позволяет специальным XML-запросом заставить уязвимый сервер запросить любую веб-страницу из Интернета. Полученный злонамеренный трафик называют Wordpress Pingback DDoS.

Атака на HTTPS не сложнее, чем на HTTP: нужно лишь указать другой протокол. Для нейтрализации же потребуется канал шириной от 20 Гбит/с, возможность обрабатывать трафик прикладного уровня на полной пропускной способности соединения и расшифровывать все TLS-соединения в реальном времени – значительные технические требования, исполнить которые могут далеко не все. К этой комбинации факторов добавляется огромное число уязвимых серверов на Wordpress – в одной атаке можно задействовать сотни тысяч. У каждого сервера неплохое соединение и производительность, а участие в атаке для обычных пользователей незаметно.

Мы увидели первое использование вектора в 2015 году, но он до сих пор работает. Мы ожидаем, что в дальнейшем этот тип атак вырастет в частоте и мощности. Амплификация на Wordpress Pingback или DNS – это уже отработанные примеры. Вероятно, в будущем мы увидим эксплуатацию более молодых протоколов, в первую очередь, игровых.

BGP и утечки маршрутов

Отцы-основатели Интернета вряд ли могли предвидеть, что он вырастет до своих текущих объёмов. Та сеть, которую они создавали, была построена на доверии. Это доверие было утрачено в периоды бурного роста Интернета. Протокол BGP создавали, когда общее число автономных систем (AS) считали десятками. Сейчас их более 50 тысяч.

Протокол маршрутизации BGP появился в конце 1980-х как некий набросок на салфетке трёх инженеров. Неудивительно, что он отвечает на вопросы ушедшей эпохи. Его логика гласит, что пакеты должны идти по лучшему из доступных каналов. Финансовых отношений организаций и политики огромных структур в нём не было.

Но в реальном мире деньги – на первом месте. Деньги отправляют трафик из России куда-то в Европу, а затем возвращают обратно на Родину – так дешевле, чем использовать канал внутри страны. Политика не даёт двум поссорившимся провайдерам обмениваться трафиком напрямую, им легче договориться с третьей стороной.

Другая проблема протокола – отсутствие встроенных механизмов проверок данных по маршрутизации. Отсюда берут корни уязвимости BGP hijacking, утечек маршрутов и зарезервированных номеров AS. Не все аномалии злонамеренны по своей природе, часто технические специалисты не до конца понимают принципы функционирования протокола. «Водительских прав» на вождение BGP не дают, штрафов нет, зато доступно большое пространство для разрушений.

Типичный пример утечек маршрутов: провайдер использует список префиксов клиентов как единственный механизм фильтрации исходящих анонсов. Вне зависимости от источника анонсов клиентские префиксы всегда будут анонсироваться по всем доступным направлениям. Пока существуют анонсы напрямую, данная проблема остаётся труднодетектируемой. В один момент сеть провайдера деградирует, клиенты пытаются увести анонсы и отключают BGP-сессию с проблемным провайдером. Но оператор продолжает анонсировать клиентские префиксы во всех направлениях, создавая тем самым утечки маршрутов и стягивая на свою проблемную сеть значительную часть клиентского трафика. Разумеется, так можно организовывать атаки Man in the Middle, чем некоторые и пользуются.

Для борьбы с утечками в anycast-сетях мы разработали ряд поправок и представили их Инженерному совету Интернета (IETF). Изначально мы хотели понять, когда в такие аномалии попадают наши префиксы, и по чьей вине. Поскольку причиной большинства утечек оказалась неправильная настройка, мы поняли, что единственный способ решить проблему – устранить условия, в которых ошибки инженеров способны влиять на других операторов связи.

IETF разрабатывает добровольные стандарты Интернета и помогает их распространению. IETF – это не юридическое лицо, а сообщество. У такого метода организации есть множество плюсов: IETF не зависит от правовых вопросов и требований какой-