Гибридные облака на мощностях провайдера

как оптимальная сервисная модель

Максим БЕРЕЗИН,
директор по развитию бизнеса, КРОК Облачные сервисы

Гибридное облако – технология не новая, но не теряющая своей популярности в крупном корпоративном сегменте. Ее суть состоит в совместном использовании разных типов ресурсов: публичного облака (Infrastructure-as-a-Service – IaaS) и физического оборудования.

Сочетание мощностей провайдера и оборудования в дата-центре заказчика долгое время считалось компромиссным вариантом. К этому прибегали, как правило, когда клиент либо резервировал данные на случай сбоя информационных систем, либо снижал потребность в администрировании оборудования, которое использовалось в менее критичных для бизнеса сервисах. Подобной стратегии, кстати, до сих следуют некоторые консервативно мыслящие компании или организации, в которых силен авторитет служб безопасности. Правда, по мере развития облачных услуг таких клиентов становится все меньше, даже среди заказчиков из госсектора.

Сейчас многие крупные компании используют гибридные облака, в основе которых на 100% лежит инфраструктура аутсорсера без учета собственного оборудования заказчика. Иными словами, в этих гибридных инфраструктурах в разном соотношении используются совместно ресурсы публичного облака и аренда выделенного виртуализированного оборудования в дата-центре провайдера, которое иногда еще называют частным облаком. Спрос на такие среды в Enterprise-сегменте растет уже на протяжении нескольких лет. В структуре выручки КРОК Облачные сервисы пик пришелся на 2019 г. – гибридные среды сейчас применяются в каждом третьем масштабном проекте.

Почему так происходит? На наш взгляд, потому, что клиенты стали настоящими профессионалами, которые умеют до копейки считать затраты на каждый сервис. Благодаря этому они могут строить такие комбинации на мощностях провайдера, которые приносят наибольшую выгоду. CIO компаний новой формации прекрасно понимают, что публичное облако – это уже не панацея. Да, это действительно удобный и финансово интересный инструмент при эксплуатации сервисов с динамической нагрузкой – в остальных случаях публичное облако может терять экономическую привлекательность, например, на фоне частных облаков.

В каких сценариях гибридное облако с использованием по максимуму ресурсов провайдера оказывается наиболее востребованным?

Линейное масштабирование в облако на случай пиковых нагрузок

Это классика жанра: компании размещают свою инфраструктуру и бизнес-сервисы на выделенном оборудовании в дата-центре, но в контракте прописывают возможность оперативного подключения ресурсов публичного облака. Такую схему выбирают в большинстве случаев организации из сектора ритейл, например сеть детских магазинов «Кораблик». Строгую сезонность в их бизнесе сложно заметить, однако в течение года случается несколько точек роста – крупных распродаж, во время которых посещение онлайн-магазинов увеличивается в разы (рис 1).

Также растет нагрузка на прикладные и офисные системы, онлайн-кассы. Торговые сети из числа наших клиентов заблаговременно готовятся к пикам: заранее масштабируют ресурсы, чтобы наплыв покупателей не стал причиной сбоя в работе сервисов.

Разработка ИТ-продуктов как сопутствующая задача

Часто компании размещают на выделенном оборудовании приложения со статичной нагрузкой, а публичное облако подключают для задач test/dev (тестовые среды и среды разработки). На тестовые среды и среды разработки одновременно может уходить столько мощности, что, размещая их в одной физической инфраструктуре с бизнес-сервисами, компании рискуют столкнуться с простоями ключевых клиентских приложений. Профиль нагрузки на ИТ меняется драматически при существенном расходе ресурсов на задачи ИТ-разработки – их может не хватить на другие задачи.

В Туту.ру это понимают лучше, чем где-либо еще. Сервис путешествий минимум два раза в неделю вносит изменения в архитектуру своей платформы и использует для этого Облака КРОК, чтобы все обновления не влияли на доступность и производительность работы сайта, через который клиенты заказывают туристические продукты. И если Туту.ру использует облако для этой задачи на постоянной основе, так как ИТ-разработки идут нон-стоп, то многие другие клиенты обращаются к облаку разово – например, чтобы проверить одну из гипотез. Подключение публичного облака удобно еще и тем, что оно позволяет контролировать затраты по каждой задаче и каждой команде продактов. Для этого в Облаке КРОК была специально доработана система биллинга, чтобы клиенты могли получать максимально детализированные отчеты.

> CIO компаний новой формации прекрасно понимают, что публичное облако – это уже не панацея.

Работа с персональными данными согласно № 152-ФЗ

Многие компании прибегают к гибридным облакам провайдеров, если хотят работать с данными в соответствии со всеми требованиями регуляторов. Как известно, существуют четыре уровня защищенности, которые необходимо обеспечить для информационных систем с персональными данными в соответствии с законодательством РФ.

Например, для медицинских информационных систем, которые обрабатывают данные более 100 тыс. пациентов, необходимо обеспечивать минимально первый или второй уровень защищенности, а вот для бухгалтерских приложений, которые содержат только данные собственных сотрудников, – третий или четвертый уровень защищенности.

В последнем случае заказчики могут размещать такие сервисы в публичных облаках, построенных в соответствии с № 152-ФЗ. В частности, Облако КРОК (рис. 2) относится к таким инфраструктурам, в основе которых используются сертифицированные ФСТЭК средства защиты.

Но для информационных систем, где необходимо обеспечить первый и второй уровни защищенности, согласно нормам российских законов должно быть использовано выделенное оборудование в ЦОД, так как существующие средства защиты не могут обеспечить требуемый уровень безопасности в публичных облаках. Пример с медицинскими данными выбран нами не случайно. Именно медицинские организации, такие как KDL, особенно ценят выделенные инфраструктуры для работы с персональными данными. Упомянутая выше сеть лабораторий размещает в специально спроектированной инфраструктуре на базе ЦОД КРОК информационную систему, а в дополнение к этому получает услугу облачного резервного копирования (Backend-as-a-Service – BaaS) для защиты данных от потери в случае любых сбоев.

Рис. 1. *Возможная экономия при использовании гибридного облака на динамичных нагрузках*

Резервное копирование и катастрофоустойчивость

Создание «плана Б» на случай выхода из строя оборудования по идее должно быть стандартом при всех схемах работы

с данными: и с локальными ИТ, и в облаке, и в коммерческом дата-центре. Большинство компаний, конечно же, прислушиваются к рекомендациям провайдеров строить отказоустойчивые архитектуры, чтобы упростить устранение последствий любого форс-мажора, а от него не застрахован ни один провайдер, даже эксплуатирующий ЦОД уровня TIER IV.

Как правило, при этом резервировании применяются зеркально спроектированные архитектуры. То есть если клиент размещает сервис или инфраструктуру в облаке, он дублирует ее сразу на двух или трех облачных платформах одного и того же провайдера. Аналогично с дата-центрами: при использовании услуг colocation или выделенного оборудования в ЦОД переключение в случае сбоя происходит на аналогичное оборудование на второй площадке. По такому принципу выстроена инфраструктура в дата-центре КРОК для Avon, который сразу на двух сайтах размещает онлайн-магазин и другие клиентские сервисы. Подобная архитектура гарантирует высокую доступность и устойчивость к инцидентам всех приложений клиента.

Как избежать проблем с облаками

Гибридные облака, которые предлагают провайдеры на базе своих ЦОД и облаков, предоставляют клиентам целый ряд новых преимуществ и позволяют им построить кастомизированные и индивидуально спроектированные инфраструктуры под конкретные задачи каждого клиента.

Теоретически при этом могут использоваться платформы разных провайдеров, и в этом случае можно говорить о следовании мультиоблачной концепции. Такой подход, с одной стороны, позволяет «разложить яйца по разным корзинам». Но, с другой стороны, здесь появляется риск размытия ответственности. При возникновении сбоев провайдеры попытаются переложить проблему на плечи своего партнера. Кроме того, следить за такой инфраструктурой становится сложнее. Также труднее становится контролировать качество выполнения SLA, поскольку условия и структуры контрактов у поставщиков в редких случаях полностью повторяют друг друга.

Наконец, решение проблем на стыках технологий занимает существенно больше времени из-за появления длинной цепочки исполнителей. При прочих равных реализацию гибридной модели стоит передать в работу одному провайдеру, который будет консолидировать экспертизу по услугам ЦОД и облака, а также станет единой точкой входа по всем вопросам интеграции, поддержки и развития сервиса в облачной инфраструктуре. ■

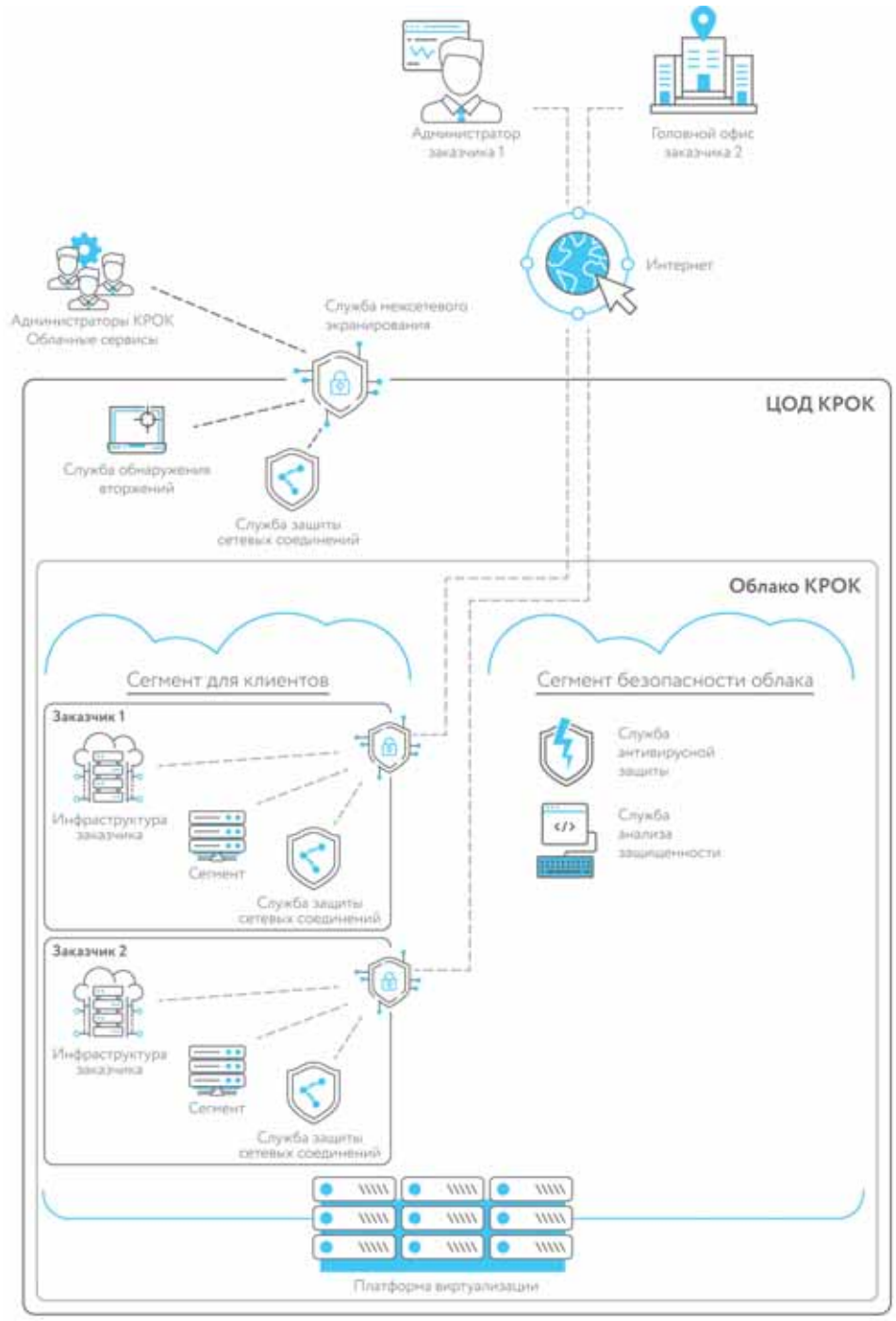

Рис. 2. *Архитектура защищенного сегмента Облака КРОК*