



Методика повышения эффективности управления облачными ресурсами накопления и обработки данных в банковской сфере

Питкевич Павел Игоревич

Белорусский государственный университет информатики и радиоэлектроники

Аннотация: В статье рассматриваются методы повышения эффективности управления информационными ресурсами в банковской среде. Проведено обоснование необходимости перехода к облачным решениям. В качестве примера одного из решений приведена гибридная модель работы банковского предприятия в облачной среде. В статье также описан сценарий работы с облачным сервисом Amazon Web Services. Сделано заключение о целесообразности перехода банков в облачную среду. Намечен путь такого перехода.

Ключевые слова: управление, облачные технологии, облачные ресурсы, банковский сектор, финансовый сектор, гибридные облака.

Введение

Последние годы облачные вычисления [1,2] стали важным технологическим фактором для развития инновационных услуг в банковском секторе [3 — 5]. Облако позволяет отрасли задействовать новые модели, решения и механизмы обслуживания [6 — 8], используя технологический прогресс для нового и лучшего предоставления услуг клиентам [6 — 8], повышения производительности труда, рентабельности и гибкости бизнес-процессов [9]. В конечном итоге облачные вычисления могут обеспечить фундамент для цифровой трансформации рассматриваемой отрасли [10 — 12].

Финансовый сектор находится в процессе принятия облачных вычислений, чтобы воспользоваться вышеупомянутыми преимуществами. Новые возможности для предоставления услуг клиентам, удовлетворение их потребностей и ожиданий, так же актуальны, как и улучшение безопасности [13, 14] снижение затрат и повышение гибкости в ведении бизнеса. Облако также открывает новые рынки предоставления финансовых услуг.

Платформа облачной безопасности быстро развивается. Публичное облако дает возможность масштабирования. Устойчивость, скорость и

безопасность — это основные положения для области управления облачными вычислениями.

Обзор облачных сервисов

Чтобы получить более глубокое понимание преимуществ и особенностей облачных вычислений, необходимо сначала взглянуть на существующее облако, его состав и модели обслуживания [15].

Публичное облако (Public Cloud) — это среда облачных вычислений, где облачные решения расположены за пределами периметра банка. Следовательно, в публичном облаке настройки, не все элементы управления будут управляться в самом заведении. Это не меняет ответственности клиентов облачных сервисов (CSC) согласно применимой правовой базе. Для логического доступа компании предоставлены контрольные функции с помощью общедоступных облачных сервисов (например, через механизмы аутентификации), любая другая компания может подписаться на те же услуги, доступные через Интернет.

Частное облако (Private Cloud). Решения частного облака расположены внутри собственного периметра банка и, следовательно, используется установленный контроль соответствующего банка. Вычислительные ресурсы используются исключительно одной организацией, либо физически в локальных центрах обработки данных компании.

Гибридное облачное решение (Hybrid Cloud) — это интегрированный в облако сервис, использующий как частные, так и публичные облака, который выполняет различные функции в рамках одной и той же организации. Внедрение гибридного облака отражает общий для всех финансовых институтов макроэкономический тренд и рассматривается как ключевой фактор для следующего поколения технологий, свободного перемещения данных и интеграции в экосистему.

В данной статье гибридное облако определяется как среда для облачных вычислений, которая использует комбинацию частного облака и общедоступных облачных сервисов, они могут включать сторонние предложения услуг, такие, как платформа как услуга (Paas), инфраструктура как услуга (IaaS) и программное обеспечение как услуга (SaaS). Эти платформы связаны программными средствами в единое целое.

Модели облачных сервисов

Существует много моделей облачных сервисов. Важно понимать, что потенциал облачных вычислений не ограничивается простым размещением данных во внешнем хранилище, а скорее состоит из быстроразвивающихся моделей обслуживания.

При подходе к оценке облачных решений с позиции оценки рисков возможны различные технологические решения.

Таблица №1

Модели взаимодействия с облачными ресурсами

Инфраструктура как услуга (IaaS)	Платформа как услуга (PaaS)	Контейнер как услуга (CaaS)	Программное обеспечение как сервис (SaaS)
1	2	3	4
Снабжает клиентов информационной инфраструктурой, предоставленной и управляемой через Интернет на основе оплаты по мере использования, например, серверы и хранилища.	Предоставляет клиентам среду по запросу для разработки, тестирования, доставки и управления программным приложением через Интернет. Финансовое учреждение управляет своими данными и	Предложение для виртуализации на основе контейнеров, в которых поставщики услуг связи предлагают для клиентов развертывание и управление контейнерами приложений и кластеров.	Позволяет клиентам подключаться к использованию облачных приложений через Интернет на основе подписки, например, используя инструмент для онлайн-сотрудничества.

1	2	3	4
Две общие модели доставки для IaaS чисто технического обеспечения и инфраструктура виртуального сервера (VSI). В случае чистого технического обеспечения финансовое учреждение или его представитель управляет серверами, хранилищем, виртуализацией, ОС, промежуточным программным обеспечением, средой обработки данных и приложений. В VSI моделируется финансовым учреждением управление ОС, промежуточным программным обеспечением, средой обработки данных и приложений.	приложениями.	СаaS предлагает полностью включенный контейнер служб развертывания с безопасностью и управление и контроль за ИТ-менеджментом.	Весь стек управляется поставщиком услуг.

На рынке облачных технологий применяются много моделей взаимодействия, например, срочные контракты, открытые модели, оплата по

факту использования. Приведем пример такой модели использования в гибридной облачной среде (рис.1).

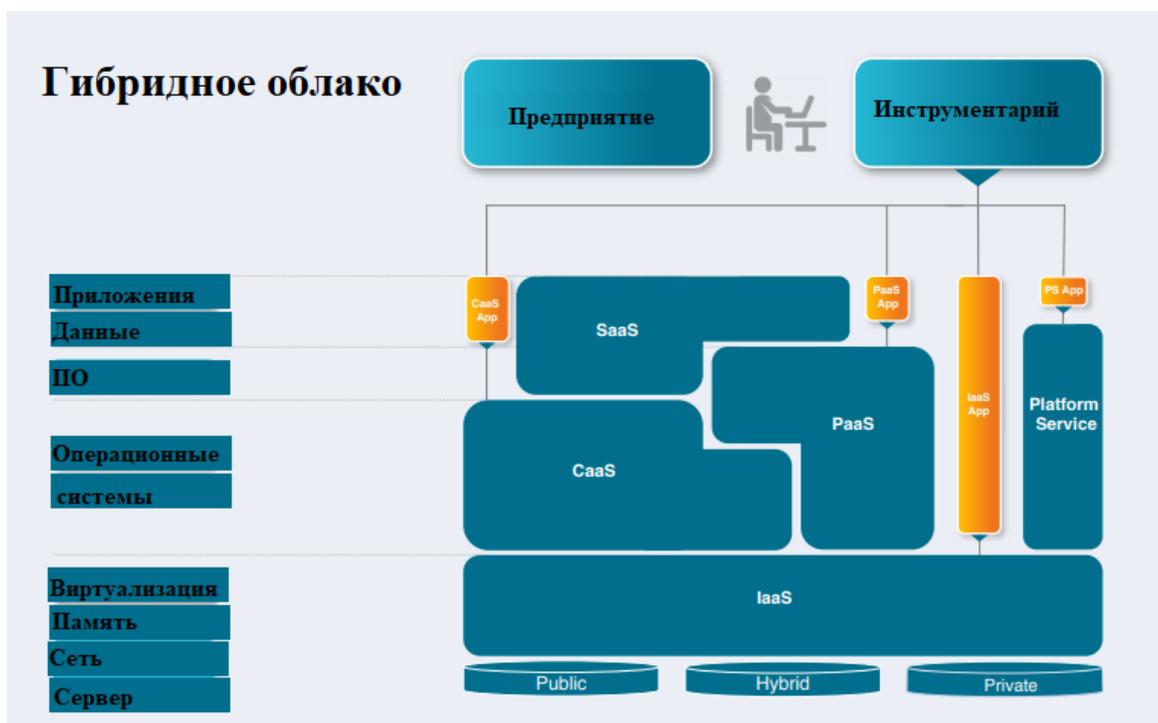


Рис. 1 — Пример модели работы предприятия в облачной среде

На рис. 1 представлена работа предприятия банковского сектора в гибридной облачной среде. Имеются частные, публичные и гибридные данные. Гибридное облако дает набор инструментов данных из этих сред для работы в режиме IaaS, SaaS, Caas, Paas.

Методика работы с облаком

В качестве конкретного примера нами была апробирована работа с облачным сервисом Amazon Web Services (далее AWS). AWS предоставляет вычислительную мощность, хранилища баз данных, доставку контента и другие функциональные возможности для создания сложных приложений с высокой гибкостью, масштабируемостью и надежностью.

AWS Identity and Access Management (далее IAM) — это веб-сервис, который помогает безопасно контролировать доступ к ресурсам AWS. IAM

контролирует, кто аутентифицирован (вошел в систему) и авторизован (имеет разрешения) на использование ресурсов.

Этот сервис предоставляет пользователям права индивидуального доступа в виде ключей доступа, паролей и устройств многофакторной аутентификации. Также возможна установка ролей для каждого пользователя.

При создании учетной записи AWS, формируется единый идентификатор для входа, который имеет полный доступ ко всем сервисам и ресурсам AWS в этой учетной записи. Это удостоверение называется корневым пользователем учетной записи AWS, и доступ к нему осуществляется путем входа в систему с адресом электронной почты и паролем, который используется для создания учетной записи.

Группа — это совокупность пользователей IAM. Группы позволяют назначать разрешения группе пользователей, что может упростить управление разрешениями для этих пользователей. Например, у вас может быть группа под названием «Администраторы» и нужно предоставить этой группе типы разрешений, которые обычно требуются администраторам. Любой пользователь в этой группе автоматически получает разрешения, назначенные группе. Если новый пользователь присоединяется к вашей организации и должен иметь права администратора, вы можете назначить соответствующие разрешения, добавив пользователя в эту группу. Точно так же, если человек меняет работу в вашей организации, вместо изменения разрешений этого пользователя вы можете удалить его или ее из старой группы и добавить в новую группу.

Удостоверение IAM вы можете создать в своей учетной записи с определенными разрешениями. Роль IAM имеет некоторое сходство с пользователем IAM. Роли и пользователи — это удостоверения AWS с политиками разрешений, которые определяют, что удостоверение может и не

может делать в AWS. Однако вместо того, чтобы однозначно ассоциироваться с одним человеком, роль предназначена для того, чтобы ее мог взять на себя каждый, кто в ней нуждается. Кроме того, роль не имеет стандартных долгосрочных учетных данных, таких, как пароль или ключи доступа, связанные с ней. Вместо этого, когда вы берете на себя роль, он предоставляет вам временные учетные данные безопасности для вашего сеанса роли.

Сервисная роль AWS – это роль, которую служба берет на себя для выполнения действий в вашей учетной записи от вашего имени. Когда вы настраиваете некоторые сервисные среды AWS, вы должны определить роль, которую будет выполнять сервис. Эта роль службы должна включать все разрешения, необходимые для доступа службы к нужным ресурсам AWS. Роли службы различаются от службы к службе, но многие позволяют выбирать разрешения, если вы соответствуете задокументированным требованиям для этой службы. Роли служб предоставляют доступ только в пределах вашей учетной записи и не могут использоваться для предоставления доступа к службам в других учетных записях. Вы можете создавать, изменять и удалять роль службы из IAM.

Роль, связанная с сервисом AWS - уникальный тип роли сервиса, который напрямую связан с сервисом AWS. Роли, связанные с сервисом, предопределены сервисом и включают все разрешения, которые требуются сервису для вызова других сервисов AWS от вашего имени. Связанная служба также определяет, как вы создаете, изменяете и удаляете связанную со службой роль. Служба может автоматически создавать или удалять роль. Это может позволить вам создавать, изменять или удалять роль как часть мастера или процесса в службе. Или может потребоваться использование IAM для создания или удаления роли. Независимо от метода, роли,

связанные со службой, упрощают настройку службы, поскольку вам не нужно вручную добавлять необходимые разрешения.

Нами были созданы три функциональные группы для конкретных пользователей в соответствии с существующими бизнес – процессами. Отдельные полномочия получили группы администраторов, разработчиков и тестировщиков (рис. 2).



Рис. 2. — Структура назначения ролей

Администраторы имеют доступ ко всем ресурсам аккаунта AWS. Были созданы пользователи Иван и Марья, и они были добавлены в группу администраторов. Чтобы войти в консоль управления AWS, каждый пользователь создал пароль. Группа администраторов имеет разрешение на доступ ко всем доступным ресурсам аккаунта AWS.

Важным моментом использования системы является создание политики безопасности, которая определяется в несколько шагов.

Шаг 1. Создание политики

По умолчанию у пользователей IAM нет разрешений на какие-либо действия. Они не могут получить доступ к Консоли управления AWS или управлять данными в ней, если вы этого не разрешите. На этом этапе вы создаете управляемую клиентом политику, которая позволяет любому подключенному пользователю входить в консоль.

Шаг 2. Прикрепите политику

Когда вы прикрепляете политику к пользователю, он наследует все права доступа, связанные с этой политикой. На этом этапе вы прикрепляете новую политику к тестовой учетной записи пользователя.

Шаг 3. Проверьте доступ пользователей

После присоединения политики вы можете войти в систему как пользователь и протестировать политику.

Включенные в систему пользователи могут менять пароли и методы проверки доступа. После настройки системы можно приступить к ее использованию.

Заключение

Сегодня использование облака — новаторское, и постоянно развивающееся на технологическом уровне решение. Использование облачных вычислений предприятиями банковского сектора быстро растет. Банки активно приобретают услуги облачных вычислений.

Переход от локальных ИТ-решений к облаку — это осознанный и необходимый путь для банков. Он начинается с развития существующих ИТ структур и услуг банков. Постепенно можно создавать частные облачные решения, преобразовывать их в комбинации облачных моделей и, наконец, внедрять в разнообразную облачную среду.

Литература

1. Максимов К.В. Эффективность использования облачных вычислений: методы и модели оценки // Прикладная информатика. 2016, №1. С 106-113.
 2. Foster I., Gannon D.B. Cloud Computing for Science and Engineering. 2017. P. 29.
 3. Криворучко С.В. Национальная платежная система: структура, технологии, регулирование. 2013. с. 103-114.
-

4. Voobier T. AI and the Future of Banking. 2020. pp. 168-175.
 5. Романова Ю.Д., Шайтура С.В. Безопасность банковских технологий. Сборник научных трудов и результатов совместных научно-исследовательских проектов. 2016. С. 527-531.
 6. Питкевич П.И., Одинец Д.Н. Методика виртуализации вычислительных ресурсов масштаба предприятия //Цифровая трансформация. 2021;(3):40-46.
 7. Thi M. H., Withana C., Quynh N. T. H. and Vinh N. T. Q. A Novel Solution for Anti-Money Laundering System. 2020, pp. 1-6.
 8. Ramachandran M., Chang V. Towards performance evaluation of cloud service providers for cloud data security. 2016. pp. 618-625.
 9. Голкина Г.Е., Шайтура С.В. Безопасность бухгалтерских информационных систем. 2016. С. 136
 10. Пономарева Е.И. Совершенствование процесса обработки данных при помощи облачных вычислений. // Инженерный вестник Дона, 2012, №1. URL: ivdon.ru/ru/magazine/archive/n1y2012/628.
 11. Taifi. M. Banking on Decoupling: Budget-Driven Sustainability for HPC Applications on EC2 Spot Instances. 2012. pp. 442-447.
 12. Marriwala N., Tripathi C.C., Kumar D., Jain S. Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, 2021.
 13. Клименков С.В., Николаев В.В., Харитонов А.Е., Гаврилов А.В., Письмак А.Е., Покид А.В. Применение семантической сети для хранения слабоструктурированных данных. // Инженерный вестник Дона, 2020, №2. URL: ivdon.ru/ru/magazine/archive/N2y2020/6339.
 14. Протасова А.А., Шайтура С.В. Анализ методов защиты баз данных. 2017. с. 290 - 298.
 15. Kara, N., Soualhia, M., Belqasmi, F. et al. Genetic-based algorithms for resource management in virtualized IVR applications. 2014.
-

References

1. Maksimov K. Methods and models for assessing the effectiveness of the use of cloud computing. *Prikladnaya Informatika — Journal of Applied Informatics*, 2016, №1. Pp 106 – 113.
 2. Foster I., Gannon D.B. *Cloud Computing for Science and Engineering*. 2017. p 29.
 3. Lopatin V., Krivoruchko S. Nacional'naja platezhnaja sistema: struktura, tehnologii, regulirovanie. *Mezhdunarodnyj opyt, rossijskaja praktika*. 2013. pp. 103-114
 4. Boobier T. *AI and the Future of Banking*. 2020. pp. 168-175.
 5. Romanova J. Shaitura S. Bezopasnost' bankovskih tehnologij. *Sbornik nauchnyh trudov i rezul'tatov sovmestnyh nauchno-issledovatel'skih proektov*. 2016. pp. 527-531
 6. Pitkevich P.I., Adzinets D.N. Enterprise-scale Computing Resource Virtualization Methodology. *Digital Transformation*. 2021, №3. pp. 40-46
 7. Thi M. H., Withana C., Quynh N. T. H. and Vinh N. T. Q. A Novel Solution for Anti-Money Laundering System. 2020, pp. 1-6.
 8. Ramachandran M., Chang V. Towards performance evaluation of cloud service providers for cloud data security. 2016. pp. 618-625.
 9. Golkina E., Shaitura S. Bezopasnost' buhgalterskih informacionnyh sistem. 2016. p. 136.
 10. Ponovareva E. *Inzhenernyj vestnik Dona*, 2012, №1. URL: ivdon.ru/ru/magazine/archive/n1y2012/628.
 11. Taifi. M. Banking on Decoupling: Budget-Driven Sustainability for HPC Applications on EC2 Spot Instances. 2012. pp. 442-447.
 12. Marriwala N., Tripathi C.C., Kumar D., Jain S. *Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems*, 2021.
-



13. Klimenkov S., Nikolaev V., Haritinova A., Gavrilov A., Pismak A., Pokid A. Inzhenernyj vestnik Dona, 2020, №2. URL: ivdon.ru/ru/magazine/archive/N2y2020/6339.

14. Protasova A., Saitura S. Analiz metodov zashhity baz dannyh. 2017. pp. 290 – 298.

15. Kara, N., Soualhia, M., Belqasmi, F. et al. Genetic-based algorithms for resource management in virtualized IVR applications. 2014.