DOI 10.37882/2223–2966.2022.12–2.10

МОНИТОРИНГ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

MONITORING THE SECURITY OF CLOUD SERVICES

V. Burygin

Summary. Cloud computing speeds up the process of developing and releasing software applications, but cloud services are becoming more complex and dynamic, using both PaaS and IaaS level resources. The purpose of the study is to monitor the security of cloud services. The proposed modular approach to building a security monitoring system will help specialists focus on abstract, not assigned to a specific cloud provider, concepts when setting up a control system in several clouds. It is shown that technologies for monitoring the security of cloud services in general have a positive impact on the functioning of the management system of business structures. It is concluded that when forming the structure of the cloud service security monitoring system, the proposed methods will allow the formation and control of a service level agreement (SLA) at the same time, along with a system of metrics and performance indicators for cloud services.

Keywords: monitoring, security, cloud services, efficiency, infrastructure, system.

Бурыгин Вячеслав Михайлович
Аспирант, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевич
slashburygin@gmail.com

Аннотация. Облачные технологии ускоряют процесс разработки и выпуска программных приложений, однако облачные сервисы становятся более сложными и динамичными, используя как ресурсы уровня PaaS, так и IaaS. Целью исследования является мониторинг безопасности облачных сервисов. Предложенный модульный подход к построению системы мониторинга безопасности поможет специалистам сосредоточиться на абстрактных, не закрепленных за конкретным облачным провайдером, концепциях при настройке системы контроля в нескольких облаках. Показано, что технологии мониторинга безопасности облачных сервисов в целом оказывают положительное влияние на функционирование системы управления предпринимательских структур. Сделан вывод о том, что при формировании структуры системы мониторинга безопасности облачного сервиса предложенные методы позволят формировать и контролировать одновременно соглашение об уровне сервиса (SLA) вместе с системой метрик и показателей эффективности работы облачных сервисов.

Ключевые слова: мониторинг, безопасность, облачные сервисы, эффективность, инфраструктура, система.

Быстрое развитие и распространение облачных технологий (cloud computing) сейчас является одним из ключевых трендов, которые в ближайшие 5–8 лет заметно повлияют на глобальное развитие IT-индустрии и на сферы бизнеса, финансов, государственного управления, медицины, образования и на многие другие сферы человеческой жизни. Международная исследовательская и консалтинговая компания IDC считает, что парадигма облачных вычислений — это фундамент для развития корпоративных информационных систем, и именно они будут главным драйвером развития рынка информационных технологий, как в мире, так и в отдельных государствах [1]. Облачные технологии ускоряют процесс разработки и выпуска программных приложений, однако облачные сервисы становятся все сложнее, динамичнее и теретрогеннее, используя как ресурсы уровня PaaS, так и IaaS. Передовые компании в области облачных вычислений предоставляют возможность разработки и управления облачными сервисами, развернутыми в нескольких облаках. В этом контексте сбор данных по состоянию и использованию облачных сервисов становится очень сложным при использовании традиционных мониторинговых инструментов, поскольку они были разработаны для локальных решений, предлагающих унифицированные API для мониторинга безопасности, и с учетом того, что со временем конфигурация программных приложений развивается медленно [2]. Поэтому следует считать целесообразной разработку как теоретических, так и прикладных аспектов создания и функционирования систем мониторинга безопасности сложных облачных сервисов. Эти происшествия и определяют актуальность темы исследования.

Анализ последних исследований и публикаций. Теоретические и прикладные вопросы мониторинга безопасности являются предметом научных исследований таких зарубежных и отечественных ученых. Проблемы и вопросы развития облачных технологий нашли свое отражение в трудах зарубежных и отечественных авторов и др. В частности, в своей работе исследователи Ф. Чоу, А. Муфту и Р. Шортер утверждают [3], что модель PaaS (Платформа как сервис) предлагает виртуальные среды выполнения облачных сервисов с общими инструментами и библиотеками для их разработки и внедрения в облако. PaaS использует модель IaaS (Инфраструктура как сервис) в качестве базы (серверы, память и сеть). При этом модель PaaS скрывает сложность управления IT-инфраструктурой. Исследование Д. Мрозека показало, что передача основных служб и прило-

жений в облако привела к появлению новых требований к разработке производительного программного обеспечения [4]. Конфигурация облачных сервисов стала более сложной, что требует пересмотра принципов построения систем мониторинга безопасности, иначе устранение возможных проблем потребует гораздо более значительных усилий и затрат. Таким образом, имея значительный практический интерес, проблема исследования построения и функционирования систем мониторинга безопасности сложных облачных сервисов заслуживает особого внимания.

Тенденции развития облачных вычислений свидетельствуют, что облачные сервисы становятся все более и более сложно разворачивающимися, создаваемыми и развивающимися системами на базе гибридных инфраструктур, состоящих из множества облаков, кибернетических систем и ресурсов Интернет. Контроль и мониторинг безопасности таких сервисов представляет собой сложную задачу. Целью работы является разработка теоретико-методологических подходов к определению сущности и особенностей построения систем мониторинга безопасности облачных сервисов, развернутых в облачной среде.

Развитие инфраструктуры облачных вычислений порождает новые объекты мониторинга безопасности — виртуальные машины, виртуальные серверы, облачные платформы. Контролировать подобную систему можно только при учете взаимосвязей между разными ее частями, только в этом случае можно гарантировать своевременное устранение и предотвращение неполадок [5]. В облачной среде система мониторинга безопасности должна не только получать информацию о работе отдельных компонентов инфраструктуры, но и проводить анализ с учетом работы всего облака. Чтобы решить проблему, связанную с несколькими облаками, нельзя полагаться на систему мониторинга безопасности, предоставленную конкретным вайдером облака. Необходимо создать модульную систему мониторинга безопасности с открытым кодом [6].

Основными элементами архитектуры такой системы являются анализаторы данных, которые получают данные и выполняют фильтрацию, агрегацию и статистический анализ. Данные описываются как кортежи в формате RDF (Resource Description Framework). Анализаторы получают данные из множества программных агентов — сборщиков данных, включающих существующие инструменты мониторинга безопасности провайдеров облаков, на базе которых развернут облачный сервис. Конфигурация выполняется с помощью мощного языка правил, позволяющего пользователю однократно указывать платформу, определяя модель программы [7]. По единому правилу пользователь сможет настроить то, что и как собирать данные, какие сборки должны выполняться, какое состояние нужно проверить и какие действия следует выполнить. Анализаторы данных рассчитывают исходные показатели и предоставляют их для специалистов по мониторингу или других анализаторов данных высшего уровня [8]. Визуализированные данные мониторинга безопасности используются для принятия решений в ответ на некоторые события. Облачные сервисы являются динамическими системами, поэтому система мониторинга безопасности нуждается в эластичности, необходимой для перенастройки и обновления внутренней модели мониторинга безопасности в соответствии с изменениями состояния сервиса. Такая эластичность получается путем предоставления сборщикам данных доступа к центральному серверу и регистрации на нем информации о контролируемых ими ресурсах. Собиратели данных должны периодически контактировать с сервером [9]. В случае, если за определенный период времени сборщик данных не предоставляет информацию, соответствующий контролируемый им ресурс удаляется из внутренней модели мониторинга безопасности и считается недоступным. Поскольку подключение всегда происходит от сборщиков данных к серверу, нет необходимости воплощать в себя стратегии маршрутизации и прослушивания портов на стороне клиента. Это позволит иметь меньше требований к провайдерам облаков, отвечающих за размещение систем мониторинга безопасности. Метрики мониторинга безопасности сами по себе не дают понимания, откуда поступают данные и как повысить их достоверность, система мониторинга безопасности должна придать семантическое значение всем компонентам облачного сервиса и отношениям между ними, создав модель мониторинга безопасности. К примеру, различные провайдеры облаков моделируются таким образом, чтобы можно было вычислить совокупность данных по всем облакам. Модель мониторинга безопасности синхронно поддерживается распределенными сборщиками данных, работающими в контролируемых облаках [10].

Для мониторинга безопасности работы современных облачных сервисов используется в качестве интегрального показателя эффективности метрика CMRR (Committed Monthly Recurring Revenue). Это совокупная стоимость всех текущих контрактов за месяц, учитывающая текущие контракты на использование сервиса, а также учет подписанных клиентами, но не исполненных контрактов. Важную роль также играет учет метрики «Churn», то есть вычисление прибыли, которая будет недополучена в результате выбытия клиентов сервиса. Для расчета данных показателей необходимо вести учет текущих операций, приобретение новых и убытие старых клиентов сервиса, то есть собирать данные по авторизации клиентов сервиса, вести учет вре-

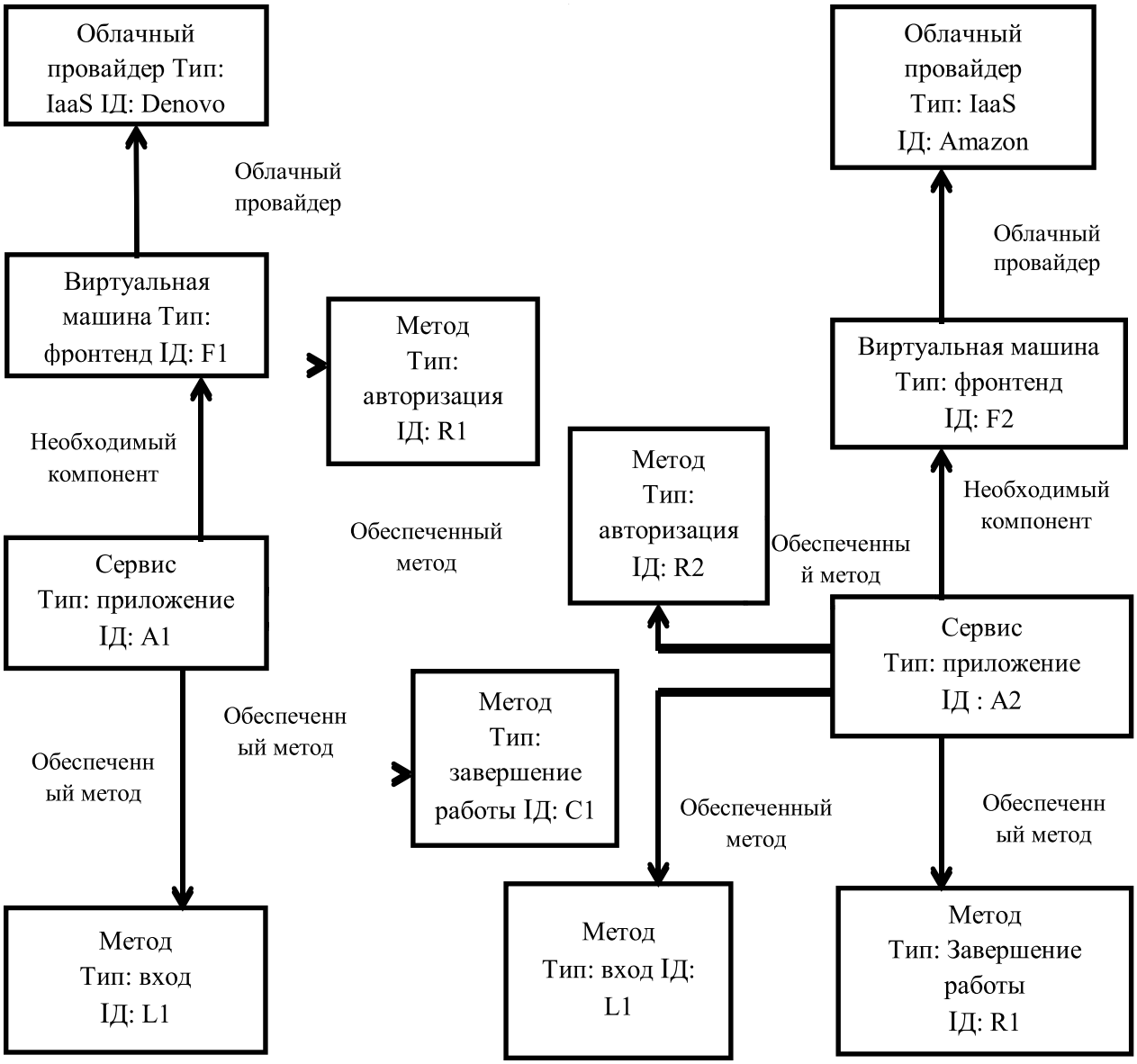

Рис. 1. Модель мониторинга безопасности многооблачного сервиса электронной торговли

мени их входа на сервис и завершение работы с ним. На рис. 1 показан пример модели мониторинга безопасности простого сервиса электронной торговли, развернутого на двух разных облаках (Denovo и Amazon), которая обеспечивает три разных метода мониторинга безопасности (авторизация, вход и завершение работы клиента) [11].

Конфигурация системы мониторинга безопасности облачного сервиса, развернутого в нескольких облаках, разрабатывается с помощью правил мониторинга безопасности, которые состоят из рекомендаций, разработанных инженером QoS (Quality of service, качество обслуживания) и описывают метрики мониторинга безопасности независимо от облака развертывания [12]. Правила мониторинга безопасности могут автоматически выводиться из требований, указанных в соглашении по качеству обслуживания, определенных при проектировании сервиса, а затем настроиться в соответствии с потребностями пользователей. Правила мониторинга безопасности состоят из 5 основных блоков [13]:

1. CM (цели мониторинга безопасности) — перечень ресурсов облачного сервиса, подлежащих мониторингу и определяемых классом, типом или идентификатором;
2. MM (метрики мониторинга безопасности) — данные, которые собираются согласно метрике мониторинга безопасности, вместе с идентификатором программного агента — сборщика данных;

Таблица 1. Пример правил мониторинга безопасности много облачного сервиса электронной торговли

Правила мониторинга	Основное правило (RT)	Детальное правило «детализация ОЗУ» (DR)
параметры	timeWindow: 60; timeStep: 60; включено: true	timeWindow: 10; timeStep: 10; включено: false
CM	тип: авторизация; тип: вход; тип: завершение работы	тип: фронтенд
MM	название метрики: время отклика; параметр: вероятность выборки: 1	название метрики: утилизация RAM; параметр: время выборки: 5
MA	вычислить 99-й процентиль	вычислить среднее значение; сгруппировать по виртуальным машинам
S	метрика > 10000	-
D	создать новую метрику: нарушение правила RT; запустить другое правило: DetailedRAM	Создать новую метрику «Средняя нагрузка ОЗУ» для каждой виртуальной машины

3. MA (совокупность метрик мониторинга безопасности) — где рассчитываются суммы, максимальные, минимальные и средние значения, проценты собранных данных, а также происходит группирование данных по определенному классу ресурсов (например, по облачному провайдеру или виртуальной машине);
4. S (состояние) — условие, подлежащее проверке, может быть выражено агрегированным показателем, выведенным на базе показателей более низкого уровня;
5. D (действие) — выполняемая функция при выполнении условия S (если есть).

В табл. 1 показаны примеры двух правил, определяющих конфигурацию системы мониторинга безопасности многооблачного сервиса электронной торговли [14].

Основное правило (RT) предписывает системе мониторинга безопасности собирать время отклика всех трех методов, вычислять 99-й процентиль каждые 60 секунд и проверять, ниже ли он 10 с.

В случае, если вычислительная метрика превышает 10 с, платформа выведет новую метрику «нарушения правила RT», которая будет доступна как вход для других правил и наблюдателей, которая позволит запустить другое правило, которое называется «Детализация ОЗУ» [15, 16]. Это второе правило подчеркивает, что система мониторинга безопасности должна собирать данные о средней загруженности оперативной памяти на всех виртуальных машинах фронтенда сервиса и создает новую метрику с именем «Средняя нагрузка ОЗУ» для каждой виртуальной машины [17]. Правило «Детализация ОЗУ» не является активным в исходной конфигурации системы мониторинга безопасности (его атрибут включения определен как false). Это означает, что данные, которые ему нужны, не собираются. Когда произойдет его активация основным правилом «RT» (т.е. если время отклика во время мониторинга безопасности медленное), сборщики данных получат инструкцию начать сбор и отправку необходимых показателей к анализатору данных, который может затем выполнить правило [18–20]. Благодаря внедрению данного механизма мониторинга можно увеличивать или уменьшать уровень мониторинга безопасности облачного сервиса и соответствующие затраты на выполнение всей системы мониторинга безопасности в зависимости от состояния сервиса.

Резюмируя рассмотрение концептуальных основ построения и функционирования системы мониторинга безопасности сложных облачных сервисов, можно выделить, что предложенный модульный подход к построению системы мониторинга безопасности поможет специалистам сосредоточиться на абстрактных, не закрепленных за конкретным облачным провайдером, концепциях при настройке системы контроля в нескольких облаках. При формировании структуры системы мониторинга безопасности облачного сервиса предложенные методы позволят формировать и контролировать одновременно соглашение об уровне сервиса (SLA) вместе с системой метрик и показателей эффективности работы облачных сервисов.

Исследование мониторинга безопасности облачных сервисов важно не только потому, что они представляют собой мощный ресурс повышения эффективности работы отдельно взятых предприятий и компаний, а также и по причинам, что их развитие является важным индикатором состояния информационного общества.

ЛИТЕРАТУРА

1. Esposito C., De Santis A., Tortora G., Chang H., Choo K-KR. Blockchain: A panacea for healthcare cloud-based data security and privacy? // IEEE Cloud Computing. № 5(1). 2018. Pp. 31–7.
2. Whaiduzzaman M., Gani A., Anuar N.B., Shiraz M., Haque M.N., Haque I.T. Cloud service selection using multicriteria decision analysis // The Scientific World Journal. № 2014. 2014. Pp. 459375.
3. Chow F., Muftu A., Shorter R. Virtualization and cloud computing in dentistry // Journal of the Massachusetts Dental Society. № 63(1). 2014. Pp. 14–7.
4. Mrozek D.A review of Cloud computing technologies for comprehensive microRNA analyses // Computational biology and chemistry. № 88. 2020. Pp. 107365.
5. Sajid A., Abbas H. Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges // Journal of medical systems. № 40(6). 2016. Pp. 155.
6. Moura J., Hutchison D. Review and analysis of networking challenges in cloud computing // Journal of Network and Computer Applications. № 60. 2016. Pp. 113–29.
7. Tabrizchi H., Rafsanjani M.K. A survey on security challenges in cloud computing: issues, threats, and solutions // The Journal of Supercomputing. № 1. 2020. Pp. 40.
8. Mehraeen E., Ghazisaeedi M., Farzi J., Mirshekari S. Security challenges in healthcare cloud computing // Systematic review. № 9(3). 2016. Pp. 157.
9. Dashti W., Qureshi A., Jahangeer A., Zafar A. Security challenges over cloud environment from service provider prospective // Cloud Computing and Data Science. № 12. 2020. Pp. 20.
10. Ogiela L., Ogiela M.R., Ko H. Intelligent Data Management and Security in Cloud Computing // Sensors. № 20. 2020. Pp. 12.
11. Tariq M.I., Ahmed S., Memon N.A., Tayyaba S., Ashraf M.W., Nazir M., et al. Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks // Sensors. № 20. 2020. Pp. 5.
12. Wu B., Wang C., Yao H. Security analysis and secure channel-free certificateless searchable public key authenticated encryption for a cloud-based Internet of things // PloS one. № 15(4). 2020. Pp. e0230722.
13. Shakil K.A., Zareen F.J., Alam M., Jabin S. A biometric authentication and data management system for healthcare data in cloud // Journal of King Saud University-Computer and Information Sciences. № 32(1). 2020. Pp. 57–64.
14. Giri S., Shakya S. Cloud Computing and Data Security Challenges: A Nepal Case // International Journal of Engineering Trends and Technology. 67(3). 2019. Pp. 146–150.
15. Bazm M.M., Lacoste M., Südholt M., Menaud J.M. Isolation in cloud computing infrastructures: new security challenges // Annals of Telecommunications. № 74(3). 2019. Pp. 197–209.
16. Singh A., Chatterjee K. Cloud security issues and challenges // J Netw Comput Appl. № 79(C). 2017. Pp. 88–115.
17. Kumar P.R., Raj P.H., Jelciana P. Exploring data security issues and solutions in cloud computing // Procedia Computer Science. № 125. 2018. Pp. 691–7.
18. Subramanian N., Jeyaraj A. Recent security challenges in cloud computing // Computers & Electrical Engineering. № 71. 2018. Pp. 28–42.
19. Stergiou C., Psannis K., Gupta B., Ishibashi Y. Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT // Sustain Comput Informatics Syst. № 19. 2018. Pp. 174–84.
20. Abrar H., Hussain S.J., Chaudhry J., Saleem K., Orgun M.A., Al-Muhtadi J., et al. Risk analysis of cloud sourcing in healthcare and public health industry // IEEE Access. № 6. 2018. Pp. 19140–50.

Журнал «Современная наука: актуальные проблемы теории и практики»