УДК 528.71

К. Е. Ефименко[1]*

Разработка программного модуля автоматизированной интеграции веб-сервисов

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: keefimenko@gmail.com

Аннотация. В статье исследуется процесс интеграции веб-сервисных решений в существующие проекты и построение инфраструктуры под задачи бизнеса. В работе содержится описание методологии создания и применения программного модуля для автоматизации процесса и интеграции нескольких программных приложений в единую систему. Рассматривается анализ существующих методов интеграции и преимущества автоматизированного подхода к данной проблеме. Разработан программный модуль, использующий технологии контейнеризации и оркестрирования. В процессе разработки программного модуля, реализованы функции обработки запросов на получение статического и динамического контента, балансировки и регистрации событий, а также настройки интеграции. Предлагается новый способ интегрирования и поддержки инфраструктуры веб-сервисов. Применяемые решения позволят значительно увеличить информационную безопасность организации путем повышения доступности и отказоустойчивости каждого компонента инфраструктуры вычислительной сети.

Ключевые слова: веб-сервис, виртуализация, TCP/IP, контейнер, оркестрирование контейнеров, Dev, Sec, SSH-ключ

K. E. Efimenko[1]*

Development of a software module for automated integration of web services

[1] National Research Nuclear University “MEPhI”, Moscow, Russian Federation
* e-mail: keefimenko@gmail.com

Abstract. The article investigates the process of integrating web-service solutions into existing projects and building infrastructure for business tasks. The paper describes the methodology of creating and using a software module to automate the process and integrate several software applications into a single system. The analysis of existing integration methods and advantages of automated approach to this problem are considered. The software module, which uses containerization and orchestration technologies, is developed. During the development of the software module, the functions of processing requests for static and dynamic content, balancing and event registration, as well as integration settings are implemented. A new way to integrate and support web services infrastructure is proposed. The applied solutions will significantly increase the information security of the organization by increasing the availability and fault tolerance of each component of the computing network infrastructure.

Keywords: web service, virtualization, TCP/IP, container, container orchestration, Dev, Sec, SSH key

Введение

Неправильный выбор стека технологий и компонентов, отсутствие изоляции модулей, отсутствие корректной интеграции компонентов может повлечь за собой крах всей критической инфраструктуры предприятия. Возрастает архитектурная потребность в использовании технологий контейнеризации и виртуализации с целью повышения коэффициента полезного действия от используемых вычислительных мощностей. Соответственно возрастает актуальность разработки подхода к автоматизированной интеграции веб-сервисов для обеспечения контроля над состоянием вычислительной сети.

Более подробно систематизация проблематики будет рассмотрена в следующем разделе.

Исследование предметной области

Автоматизированная интеграция в области разработки программного обеспечения была отображена в статье Parth Sane [1]. Данный процесс увеличивает пространство для атак, потому, в рамках исследования уязвимостей, эксплуатирующих веб-сервисные решения, использовалась открытая база данных публично раскрытых уязвимостей [2]. Для устранения потенциальных уязвимостей, основываясь на технической документации, был сконфигурирован высоконагруженный веб-сервер [3].

Не менее значительным аспектом исследования является выбор методов формирования децентрализованного реестра событий информационной инфраструктуры и интеллектуально-адаптивного управления информационной инфраструктурой предприятия. Соответствующей тематикой занимается Басыня Е. А. и Сафронов А. В. [4, 5].

В работе используется методология DevOps, основные положения которой были взяты из работы F. M. A. Erich, C. Amrit, M. Daneva [6].

Неотъемлемой частью любой обработки событий является их хранение. Для реализации необходимо выбрать способ хранения и класс системы управления базы данных. Один из классов систем управления базой данных описан в мануале [7]. Построение процесса непрерывного мониторинга с помощью одного из множества вариантов программ с открытым исходным кодом было предложено Ljubojevic M., Luka B., Bajic A. [8].

Применение программного модуля подразумевает внесение изменений в корпоративную вычислительную сеть. Проблемой организацией корпоративной вычислительной сети занимаются Джеймс Куроуз и Кит Росс [9].

Важным элементом обеспечения информационной безопасности является организация каналов связи по защищенному протоколу SSH. Научная публикация на тему защищенны протоколов управления была опубликована за авторством M. Başer, E. Y. Güven and M. A. Aydın [10].

Развертывание компонентов инфраструктуры организаций развивалось по мере увеличения требований к пропускной способности веб-сервиса и его функционалу. Первично процесс развертывания представлял собой запуск приложе-

ний на отдельных физических серверах. Это расходовало большое количество системных ресурсов, необходимых для содержания и администрирования кластера компонентов. Технологии виртуализации позволили значительно сократить ресурсные издержки, поскольку не было необходимости разносить программы и приложения на разные физические платформы, используя виртуальные машины.

На рис. 1 представлена хронология совершенствования технологий контейнеризации. Контейнеры стали популярны из-за таких возможностей как непрерывная разработка, разделение задач на Dev и Sec, повышение уровня абстракции от запуска ОС на виртуальном оборудовании до запуска приложения в ОС с использованием логических ресурсов.

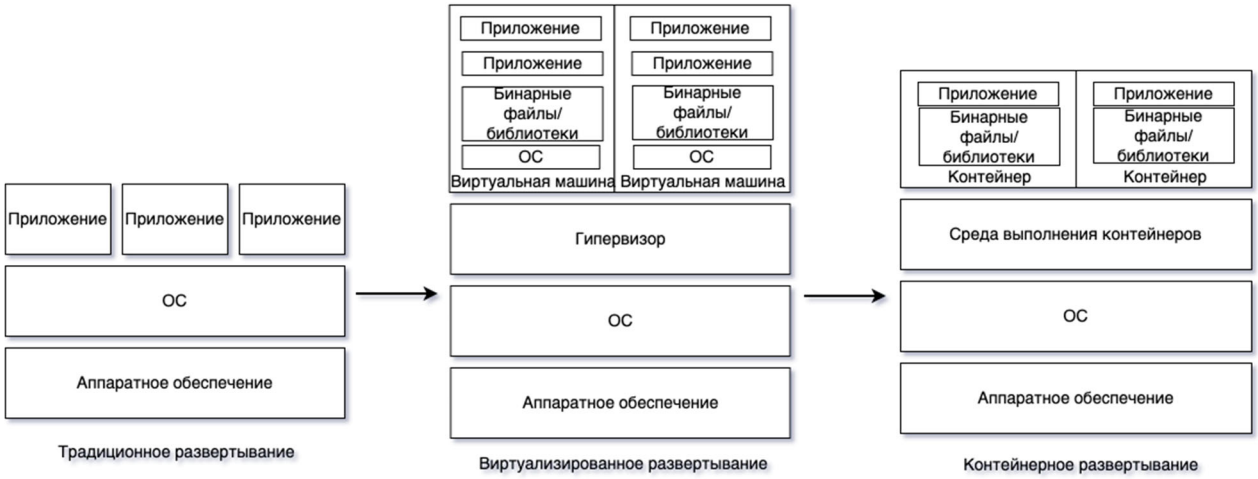

Рис. 1. Хронология совершенствования технологий виртуализации

В настоящее время процесс развертывания и интеграции осуществляется с помощью технологии контейнеризации. Образы контейнеров используют меньше вычислительных ресурсов в сравнении с образами виртуальных машин, что позволяет проводить более гибкую настройку.

Использование контейнеров как единиц объекта развертывания кроме гибкой настройки позволяет стандартизировать разворачиваемые кластеры компонентов. Необходимость профилирования инфраструктуры под конкретные нужды проекта усложняет контроль и поддержку уровня защищенности в организации. Невозможность применения универсальной политики безопасности способствует накоплению «компромиссных решений», что увеличивает количество потенциальных векторов атак.

Постановка задачи

Целью данной работы является обеспечение информационной безопасности веб-сервисов путем автоматизации процесса интеграции компонентов в информационную инфраструктуру предприятия.

В ходе решения данной проблемы выделены следующие задачи: исследование предметной области, моделирование предметной области, разработка модуля, а также тестирование и исследование предлагаемого решения.

Предлагаемое решение

Решение основано на использовании DevSecOps практик. В программном модуле применяются технологии управления инфраструктурой как кодом, а также средства контейнеризации и оркестрирования контейнеров.

Запуск программного модуля начинает процесс создания виртуальных машин веб-приложения. По заданным параметрам формируется количество серверов и их оснастка. Для всех виртуальных машин конфигурируется порт по умолчанию и доступ по SSH-ключу. После установки защищенного соединения последовательно в декларативном режиме на каждую виртуальную машину инсталлируется программное обеспечение и конфигурируются его функциональные возможности. Окончание работы программного модуля определяется состоянием завершения инсталлирования и конфигурирования.

Итогом развертывания является полностью функционирующая база для веб сервиса. Обработка запроса происходит с профилированием и активным управлением трафиком. После обработки запроса происходит обработка логов событий с дальнейшим попаданием в базу данных. На рис. 2 представлена UML-диаграмма последовательности действий по обработке запроса.

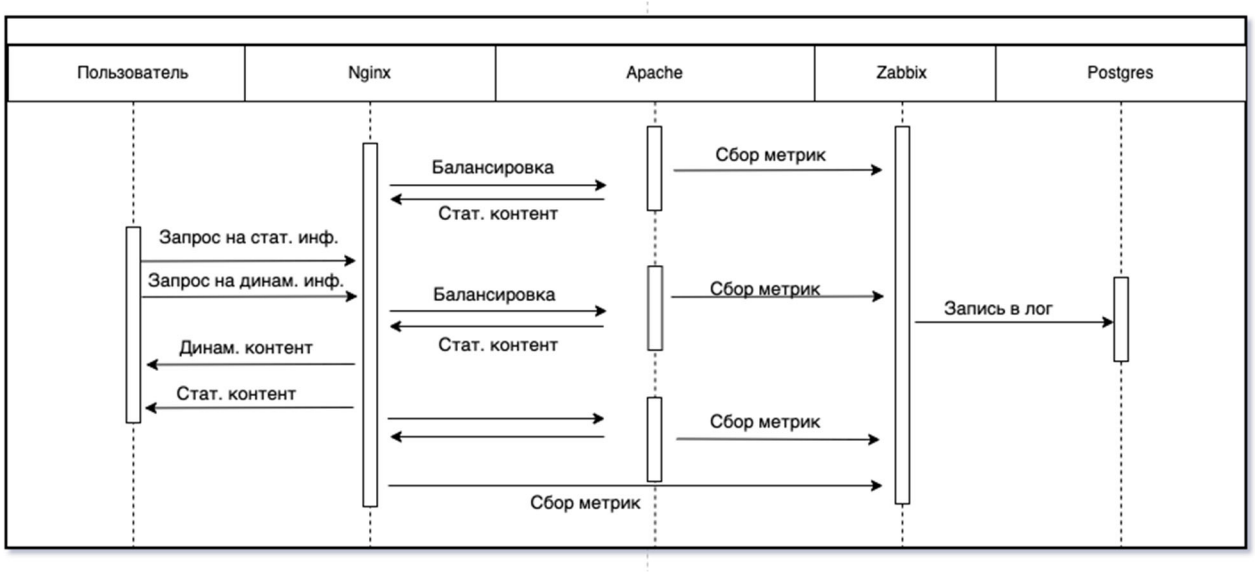

Рис. 2. UML-диаграмма последовательности действий по обработке запроса

Использование разворачиваемой инфраструктуры и способ ее развертывания позволяют в несколько нажатий сформировать информационную базу проекта на неограниченное число виртуальных машин. Безопасность применяемых решений гарантированно применяется на все установленные объекты сети.

Заключение

В рамках данной работы был спроектирован и разработан программный модуль для автоматизированной интеграции веб-сервисов. Благодаря качественному анализу уязвимостей удалось создать безопасную конфигурацию всех взаимодействующих узлов в рамках интегрируемого веб-сервиса. Все информационные потоки между виртуальными машинами безопасно организованы путем шифрования трафика. Топология и конфигурация виртуальных машин обеспечивает доступность и отказоустойчивость веб-сервиса.

Практическая значимость работы состоит в возможности применения разработанного программного модуля автоматизированной интеграции веб-сервисов с целью решения задач бизнеса. Программный модуль расширяем и может быть скорректирован в зависимости от специфики организации и ее целей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Parth Sane. A Brief Survey of Current Software Engineering Practices in Continuous Integration and Automated Accessibility Testing // 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking. Chennai, India, March 2021. P. 130-134.

2. База данных публично раскрытых уязвимостей кибербезопасности // https://cve.mitre.org/cve/search_cve_list.html

3. Техническая документация к веб серверу nginx// https://nginx.org/ru/docs

4. Басыня Е. А., Сафронов А. В. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия // Вестник УрФО. Безопасность в информационной сфере. - 2019. - No 4 (34). - С. 35-44.

5. Басыня Е. А. /Метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия // Информационные технологии. – 2020. - No 3 (26). – С. 185-191.

6. F. M. A. Erich, C. Amrit, M. Daneva / A qualitative study of DevOps usage in practice, 2017

7. Knowledge Base of Relational and NoSQL Database Management Systems // DB-ENGINES. 2019. URL: https://db-engines.com/en/ (дата обращения: 01.11.2022).

8. Ljubojevic M., Luka B., Bajic A. Centraылized monitoring of computer networks using Zenoss open source platform // InProceedings of the 17th International Symposium INFOTEH-JAHORINA (INFOTEH). East Sarajevo, Bosnia-Herzegovina, 21-23 March 2018. P. 1-5.

9. Компьютерные сети. Нисходящий подход /Джеймс Куроуз и Кит Росс, 2022. - No 1. - С. 65-100.

10. M. Başer, E. Y. Güven and M. A. Aydın, "SSH and Telnet Protocols Attack Analysis Using Honeypot Technique: Analysis of SSH AND TELNET Honeypot," 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021, pp. 806-811, doi: 10.1109/UBMK52708.2021.9558948.