УДК 004.056

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ КОНТЕЙНЕРИЗАЦИИ КАК КОМПОНЕНТА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.А. Меньшов

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: kolyaman_only_steam@mail.ru

Основное внимание уделяется рассмотрению технологии контейнеризации и использованию её как компонента обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, контейнер, оркестратор.

THE USE OF CONTEINERIZATION TECHNOLOGY AS A COMPONENT OF INFORMATION SECURITY

N.A. Menshov

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarskii rabochii prospekt, Krasnoyarsk, 660037, Russian Federation
E-mail: kolyaman_only_steam@mail.ru

The focus is on consideration of containerization technology and its use as a component of information security.

Keywords: information security, containerization, orchestrator.

Введение. Согласно отчёту Flexera контейнеры используют 53% компаний (речь идет просто о Docker-контейнерах) [3]. В отчетё Red Hat The State of Enterprise Open Source 2021 (1250 респондентов), около 50% используют контейнеры в production. Еще 37% — только для dev-окружения [4]. Технология контейнеризации стремительно набирает популярность в IT сфере. Основной целью данной статьи является рассмотрение технологии контейнеризации и оценка предоставляемых ею механизмов для реализации мер по обеспечению информационной безопасности.

Технология контейнеризации. Контейнеризация – способ упаковки, совместного использования и развертывания приложения. Контейнер включает в себя все зависимости (пакеты, библиотеки, код приложения, файловая система, сетевой стек и т.д.), которые необходимы приложению для функционирования. При развертывании контейнера все его ресурсы помещаются в фактически изолированную среду, к которой другие контейнеры не могут получить доступ. Контейнеры реализованы на двух ключевых технологиях: пространстве имен Linux (namespace) и контрольных группах Linux (cgroups). Пространство имен создает практически изолированное пользовательское пространство и предоставляет приложению выделенные системные ресурсы. Cgroups обеспечивают ограничение аппаратных ресурсов, расстановку приоритетов, мониторинг и контроль приложения. Контейнеры – виртуализация на уровне операционной системы. В отличии от виртуальных машин контейнеры используют как оборудование, так и ядро операционной системы, что уменьшает затраты ресурсов (оперативной памяти, процессорного времени, дискового пространства), но обеспечивает меньший уровень изолированности системы [1].

Система оркестрации. При упаковке приложения в контейнер, создаётся образ контейнера. Образ создается из конфигурационного файла, в котором описаны все необходимые параметры конфигурации (переменные окружения, порты, пользователей, установку и обновление пакетов, копирование файлов и т.д.). Для того, чтобы выполнить централизованное хранение образов контейнеров, используются реестры. Реестр представляет собой дерево папок. Кроме самих образов в реестре хранятся и их более старые версии. Рано или поздно встаёт вопрос о том, как эффективно управлять образами. Микросервисные архитектуры, постоянное наращивание функционала, запуск новых продуктов – всё это ведёт к увеличению числа контейнеров, а значит, и к усложнению управления ими. Для преодоления трудностей масштабирования были созданы среды контейнерной оркестрации, которые еще называются оркестраторами [2].

Системы оркестрации обладают следующим функционалом: запуск контейнеризованных приложений в кластере; организация сетевого взаимодействия; поддержка актуального состояния приложения в соответствии с желаемой конфигурацией; отладка приложений; мониторинг ресурсов; мониторинг систем хранения данных; контроль потока данных между контейнерами и оркестратором; проверка работоспособности приложений; репликация узлов с приложениями; применение горизонтального автомасштабирования подов (под – группа контейнеров с общими разделами, запускаемых как единое целое); именование и обнаружение; распределение ресурсов и балансировка нагрузки между контейнерами; обкатка обновлений; доступ к журнальным файлам и их обработка; предоставление аутентификации и авторизации.

Преимущества и недостатки технологии. Контейнеры обладают следующими преимцществами: быстрое создание и развертывание приложений; непрерывные разработка, интеграция и развертывание; разграничение ответственности разработчиков и администраторов; однородность сред разработки, тестирования и промышленного использования; переносимость между разными облачными провайдерами и операционными системами; сосредоточение управления непосредственно на приложении; слабо связанные, распределенные, эластичные, независимые микросервисы; изоляция, утилизация ресурсов;

Недостатки: высокая сложность, рост количества контейнеров, работающих с приложением, влияет на сложность управления ими; разрастание, нередко в контейнеры упаковывается гораздо больше ресурсов, чем реально требуется, из-за этого образ разрастается, занимая больше места на диске; запуск контейнеров в Windows-среде не всегда удобен; недостаточная зрелость, технологии контейнеризации приложений появились на рынке сравнительно недавно, не всегда удаётся сразу решить возникшую проблемы.

Использование технологии контейнеризации как компонента обеспечения информационной безопасности. Изоляция контейнера усложняет возможность проведения атак из приложения внутри контейнера на ресурсы информационной системы. Система оркестрации предоставляет контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения внутри контейнеров и контроль целостности программного обеспечения. Обеспечивает возможность восстановления стабильной версии программного обеспечения при тестировании новой версии в процессе эксплуатации или при возникновении нештатных ситуаций. Предоставляет дополнительную идентификацию и аутентификацию пользователей. Предоставляет средство мониторинга ресурсов, систем хранения данных и потока данных между контейнерами. Предоставляет возможность масштабирования и распределения ресурсов, а также обеспечивает балансировку нагрузки между контейнерами, что обеспечивает доступность циркулирующей информации.

Однако у всего этого есть и обратная сторона. Контейнеры имеют достаточное количество уязвимостей. Например, CVE-2014-3519, CVE-2016-5195, CVE-2016-9962, CVE-2017-5123 и CVE-2019-5736, которые могут привести к получению злоумышленником доступа к данным

за пределами контейнера. Также необходимо обеспечить безопасность системы оркестрации. Практически все компоненты оркестратора, включая запущенные на нем приложения, могут быть использованы злоумышленником для начала/развития атаки. К примеру, Microsoft адаптировала структуру MITRE ATT&CK и создала матрицу атак на систему оркестрации Kubernetes «Threat Matrix for Kubernetes» с описанием 10 техник от Initial Access до Impact и 45 тактик, реализующих указанные техники. Кроме того, можно обратиться непосредственно к материалам MITRE, выпустившей собственную матрицу «Containers Matrix» несколько позже, чем это сделала Microsoft.

Выводы. Технология контейнеризации может быть использована как компонент обеспечения информационной безопасности. Она предоставляет инструменты для реализации мер обеспечения информационной безопасности, что при правильном менеджменте и использовании механизмов может повысить общий уровень безопасности информационной системы. Однако технология ещё довольно незрела и имеет большой уровень вхождения.

Библиографические ссылки

1. Как сделать контейнеры еще более изолированными: обзор контейнерных sandbox-технологий [Электронный ресурс]. URL: https://habr.com/ru/company/itsumma/blog/457760/

2. Осваиваем Kubernetes. Оркестрация контейнерных архитектур [Электронный ресурс]. URL: https://itsecforu.ru/wp-content/uploads/2019/11/Dzhidzhi_Saifan_Osvaivaem_Kubernetes._Orkestraci.pdf

3. Flexera. State of the Cloud Report. [Электронный ресурс] URL: https://info.flexera.com/CM-REPORT-State-of-the-Cloud

4. Red Hat. The State of Enterprise Open Source. [Электронный ресурс] URL: https://www.redhat.com/rhdc/managed-files/rh-enterprise-open-source-report-f27565-202101-en.pdf