Мироненко А.В. Исследование проблем безопасности контейнеризованных сред при выполнении учебных практических работ в университете на примере Kubernetes: угрозы и меры защиты // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 56–62

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ КОНТЕЙНЕРИЗОВАННЫХ СРЕД ПРИ ВЫПОЛНЕНИИ УЧЕБНЫХ ПРАКТИЧЕСКИХ РАБОТ В УНИВЕРСИТЕТЕ НА ПРИМЕРЕ KUBERNETES: УГРОЗЫ И МЕРЫ ЗАЩИТЫ

Мироненко А.В.
ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993, Москва, Волоколамское ш., д. 4), e-mail: qwerty.mironenko@gmail.com

С увеличением популярности контейнерных технологий, возникают новые угрозы безопасности, особенно в образовательных учреждениях. В статье рассматриваются проблемы безопасности контейнеризованных сред, на примере Kubernetes в учебной среде, показываются различные потенциальные угрозы, а также предлагаются меры защиты для минимизации рисков и обеспечения безопасного использования контейнеров для учебных работ.

Ключевые слова: Информационные технологии, контейнеризация, развертывание, безопасность кластера, Kubernetes, обучение.

INVESTIGATION OF THE SECURITY PROBLEMS OF CONTAINERIZED ENVIRONMENTS WHEN PERFORMING EDUCATIONAL PRACTICAL WORK AT THE UNIVERSITY USING THE EXAMPLE OF KUBERNETES: THREATS AND PROTECTION MEASURES

Mironenko A.V.
MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: qwerty.mironenko@gmail.com

With the increasing popularity of container technologies, new security threats are emerging, especially in educational institutions. The article discusses the security problems of containerized environments, using Kubernetes as an example in an educational environment, shows various potential threats, and also suggests protective measures to minimize risks and ensure the safe use of containers for educational work.

Keywords: Information technology, containerization, deployment, cluster security, Kubernetes, training.

Введение

В современном мире информационных технологий контейнеризация стала неотъемлемой частью разработки и внедрения программных продуктов. Она обеспечивает удобство развертывания, масштабируемость и изоляцию приложений, что делает ее востребованной как в корпоративной, так и в академической среде. Однако вместе с ростом популярности контейнерных технологий возникают новые угрозы безопасности, особенно в образовательных учреждениях, где студенты используют контейнеры для выполнения учебных заданий. В данной статье рассматривается проблема безопасности

контейнеризованных сред на примере Kubernetes в университетской среде, выявляются потенциальные угрозы и предлагаются меры защиты для минимизации рисков и обеспечения безопасного использования контейнеров в учебных практических работах.

Краткая информация о Kubernetes

Kubernetes, первоначально разработанный Google и теперь поддерживаемый Cloud Native Computing Foundation, произвел революцию в способах развертывания, управления и масштабирования контейнерных приложений в организациях. По своей сути Kubernetes — это платформа с открытым исходным кодом, предназначенная для автоматизации развертывания, масштабирования и работы контейнеров приложений в кластерах хостов.

Его архитектура состоит из нескольких ключевых компонентов: главного узла (control plane, master node), который управляет кластером, рабочих узлов (worker nodes), на которых выполняются контейнерные приложения, etcd key-value базы данных для управления состоянием кластера и набора процессов вроде kubelet, который управляет узлами и взаимодействует с мастером, и kube-proxy, который управляет сетевым взаимодействием. Также для понимания терминологии необходимо пояснить что такое под.

Под — это наименьшая развертываемая вычислительная единица, которая может быть создана в Kubernetes. Под (от англ. pod (pea pod) - стручок гороха) — это группа из одного или нескольких контейнеров с общим хранилищем и сетевыми ресурсами, а также спецификацией запуска контейнеров. Содержимое пода всегда размещается и планируется совместно и запускается в общем контексте. Под моделирует «логический хост» для конкретного приложения: он содержит один или несколько контейнеров приложений, которые относительно тесно связаны. В необлачных контекстах приложения, выполняемые на одной и той же физической или виртуальной машине, аналогичны облачным приложениям, выполняемым на том же логическом хосте. [1]

Почему нужно защищать учебный кластер?

Можно подумать, что серьезно защищать кластер, использующийся студентами в учебных целях, не имеет смысла, поскольку он не содержит в себе чувствительных для бизнеса данных и критических приложений, которые требуют бесперебойного доступа.

Однако вот несколько ключевых причин, по которым следует серьезно относиться к его безопасности:

Обучение лучшим практикам: Учебные кластеры предоставляют студентам возможность изучать и применять best practice в сфере безопасности. Эти знания студенты могут перенести в будущую профессиональную деятельность.

Предотвращение злоупотреблений: Незащищенные кластеры могут быть использованы для незаконной деятельности, такой как распространение вредоносного ПО, атаки на другие сети или майнинг криптовалюты, что может привести как к повышенным расходам, так и к юридической ответственности.

Сохранение репутации учебного заведения: Инциденты безопасности могут негативно сказаться на репутации учебного заведения и подорвать доверие к его разработкам, выпускникам и программам обучения.

Создание безопасной учебной среды: Защита кластеров помогает создать безопасную и стабильную среду для обучения, где студенты могут сосредоточиться на учебе, не беспокоясь о потере работы из-за атак или сбоев.

Защита интеллектуальной собственности: Студенты могут работать над инновационными проектами, которые могут иметь коммерческую ценность. Незащищенные кластеры могут стать целью для кражи данных.

Угрозы безопасности

1. Небезопасные образы контейнеров

Одним из основных источников угроз безопасности в Kubernetes являются небезопасные образы контейнеров. Образы контейнеров, используемые в учебных целях, часто скачиваются из общедоступных источников и могут содержать уязвимости, которые могут быть использованы злоумышленниками для получения доступа к контейнеризованной среде.

2. Компрометация учетных данных

Еще одна распространенная угроза безопасности - это компрометация учетных данных. Злоумышленники могут использовать атаки фишинга или социальной инженерии для получения доступа к учетным данным администраторов Kubernetes. Как только злоумышленник получает доступ к учетным данным администратора, он может получить полный контроль над кластером Kubernetes, что позволяет ему развертывать вредоносные контейнеры, красть данные или нарушать работу приложений.

3. Внедрение вредоносного кода

Студенты могут случайно или намеренно внедрить вредоносный код в свои контейнеры. Это может привести к заражению всего Kubernetes-кластера, что может привести к серьезным последствиям, таким как кража данных, потеря работоспособности и финансовые убытки.

4. DoS-атаки

Kubernetes-кластеры могут быть подвержены атакам типа "отказ в обслуживании" (DoS). Эти атаки могут быть вызваны как неправильным использованием ресурсов студентами, так и целенаправленными атаками злоумышленников. DoS-атаки могут сделать кластер Kubernetes недоступным для пользователей, что может привести к перебоям в работе и финансовым потерям.

5. Несанкционированный доступ к API

API Kubernetes предоставляет мощный интерфейс для управления кластером. Однако уязвимости в API Kubernetes могут быть использованы злоумышленниками для получения несанкционированного доступа к кластеру. Это может позволить злоумышленникам развертывать вредоносные контейнеры, красть данные или нарушать работу приложений. [2]

Общие рекомендации по защите кластера.

Управление настройкой кластера. Защита control plane и worker nodes Kubernetes имеет основополагающее значение для защиты всего кластера. Крайне важно укрепить control plane, сердце Kubernetes, путем ограничения доступа, обеспечения связи по безопасным каналам, а также регулярного обновления и исправления его компонентов. Worker nodes, на которых фактически запускаются приложения, требуют не меньшего внимания. Их следует настроить по принципу наименьших привилегией и минимальных разрешений, необходимых для

работы. Сетевые политики имеют решающее значение для определения того, как модули взаимодействуют друг с другом и с внешним миром. Реализация жесткой сетевой политики помогает создать глубокую защиту, снижая риск перемещения вредоносной нагрузки по сети в случае взлома.

Аутентификация и авторизация. Надежное управление доступом пользователей является ключом к поддержанию целостности безопасности кластера Kubernetes. Внедрение контроля доступа на основе ролей (RBAC) имеет решающее значение для обеспечения того, чтобы пользователи (как студенты, так и преподаватели) и службы имели только тот доступ, который им необходим. Политики RBAC позволяют администраторам указывать, кто и к каким ресурсам имеет доступ в кластере. Интеграция с внешними поставщиками удостоверений через такие протоколы, как OpenID Connect, может централизовать управление пользователями и упростить процесс аутентификации. Регулярные проверки этих разрешений имеют жизненно важное значение для обеспечения того, чтобы они продолжали отражать необходимые уровни доступа.

Безопасность сети. Безопасность сети Kubernetes заключается в контроле потока входящего и исходящего трафика кластера. Сетевые политики и сегментация имеют основополагающее значение для изоляции и защиты конфиденциальных рабочих нагрузок. Сетевые политики позволяют администраторам контролировать поток трафика между модулями и между модулями и внешними сетями, тем самым определяя, как группы модулей могут взаимодействовать друг с другом и с другими конечными точками сети. При отсутствии сетевых политик модули в кластере Kubernetes могут иметь неограниченный доступ к сети, что потенциально позволяет беспрепятственному распространению вредоносного трафика или нарушений. Реализация сегментации сети в кластере Kubernetes может предотвратить несанкционированный доступ и ограничить радиус атаки в случае компрометации. Кроме того, шифрование трафика как внутри кластера (внутрикластерная связь), так и при выходе из кластера или входе в него (например, входящий и исходящий) имеет важное значение для защиты данных от перехвата и подделки. Рассмотрите возможность использования Kubernetes — собственных или сторонних инструментов, которые улучшают управление и визуализацию сетевых политик. Такие инструменты, как Calico, Cilium или Weave Net, могут предоставлять расширенные возможности сетевой политики, упрощая управление сложными сетевыми конфигурациями и визуализируя взаимодействие между различными сетевыми политиками. [3]

Безопасность подов. Pod Security Admission имеют решающее значение для определения условий безопасности, которым должны соответствовать поды для работы в кластере. Они помогают применять лучшие практики, такие как предотвращение привилегированного доступа, ограничение доступа к ресурсам хоста и контроль использования томов и файловых систем. Включает в себя также определение лимитов ресурсов для подов как по памяти, так и по использованию процессора. Это предотвращает перегрузку узлов кластера и обеспечивает бесперебойную работу других приложений. Использование запросов ресурсов (requests) для определения минимального количества ресурсов, необходимых для работы пода гарантирует, что под будет запланирован на узел с достаточными ресурсами и не прекратит работу в связи с их исчерпанием. Помимо этого, регулярное сканирование образов контейнеров и сред

выполнения на уязвимости помогает выявлять и устранять потенциальные проблемы безопасности до того, как их можно будет использовать.

Безопасность данных. Защита данных, как при хранении, так и при передаче, является важнейшим аспектом безопасности Kubernetes даже для тестового студенческого кластера. Применение всех доступных средств защиты данных позволит студентам разрабатывать любые приложения. Шифрование хранящихся данных, использование серверов хранения, поддерживающих шифрование, и безопасное управление ключами шифрования являются фундаментальными практиками. Что касается передаваемых данных, использование Transport Layer Security (TLS) для всех внутренних и внешних коммуникаций гарантирует, что данные шифруются во время передачи, защищая их от утечки и атак типа «man-in-the-middle».

Ведение журнала и мониторинг. Эффективное ведение журнала и мониторинг необходимы для поддержания безопасности кластера Kubernetes. Это предполагает сбор и анализ журналов различных компонентов кластера Kubernetes для обнаружения, оповещения и реагирования на аномальные действия, которые могут указывать на нарушение безопасности. Такие инструменты, как Prometheus для мониторинга и Elasticsearch, Fluentd и Kibana (стек EFK) для ведения журналов, могут показаться избыточными, но стать полезными в учебных целях. Обнаружение аномалий можно дополнительно улучшить за счет интеграции передовых инструментов безопасности, которые используют машинное обучение для обнаружения необычных закономерностей в работе системы. [4]

Применение политики с помощью Open Policy Agent (OPA). Open Policy Agent (OPA) — это механизм политики общего назначения с открытым исходным кодом, который унифицирует применение политики во всем стеке. В Kubernetes OPA можно использовать для применения пользовательских политик в кластерах, помимо того, что предлагается политиками безопасности подов. OPA интегрируется с процессом контроля доступа Kubernetes, позволяя администраторам определять детальные, контекстно-зависимые политики, контролирующие, какие ресурсы можно создавать и изменять. Используя OPA, организации могут применять широкий спектр политик, включая лучшие практики безопасности, требования соответствия и даже сложные организационные политики. Этот уровень контроля имеет решающее значение для поддержания целостности и безопасности кластеров Kubernetes, особенно в средах со строгими нормативными требованиями и требованиями соответствия. [5]

Сканирование образов в Kubernetes. Сканирование образов включает в себя анализ образов контейнеров на наличие известных уязвимостей, таких как устаревшие пакеты программного обеспечения, небезопасные конфигурации или открытые секреты. Этот процесс имеет решающее значение, поскольку образы контейнеров составляют основу рабочих нагрузок приложений, работающих в кластерах Kubernetes. Инструменты автоматического сканирования могут выявлять уязвимости на самой ранней стадии, позволяя студентам решать проблемы безопасности до того, как они достигнут производственной среды. Для сканирования образов контейнеров доступно несколько инструментов и платформ. Эти инструменты обычно поддерживают базы данных известных уязвимостей, которые они используют для оценки уровня риска образа контейнера. Некоторые популярные варианты: Twistlock и grype. Эти инструменты могут сканировать изображения на наличие широкого

спектра уязвимостей, в том числе перечисленных в базе данных Common Vulnerabilities and Exposures (CVE), и предоставлять подробные отчеты о результатах.

Обучение и осведомленность. Создание кластера со всеми мерами безопасности малополезно без обучения студентов основам безопасности контейнеров и Kubernetes. Кроме того, важной частью является предоставление студентам ресурсов для изучения лучших практик безопасности и создание культуры безопасности, в которой студенты могут без опасений сообщать о проблемах безопасности, которые возникли или были ими обнаружены.

Заключение.

В заключение хочется отметить, что безопасность сред Kubernetes — это постоянный путь, а не пункт назначения. Лучшие практики, изложенные в этой статье, могут служить основой, но их необходимо постоянно пересматривать и совершенствовать в ответ на новые идеи, технологии и угрозы. Поскольку Kubernetes укрепляет свою роль краеугольного камня облачных вычислений, приверженность безопасности как со стороны сообщества, так и отдельных пользователей будет играть решающую роль в долгосрочном успехе и надежности платформы.

Список литературы

1. Kubernetes Documentation: Securing a Cluster [Электронный ресурс] URL: https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/ (дата обращения: 05.04.2024)
2. Containers’ Security: Issues, Challenges, and Road Ahead [Электронный ресурс] URL: https://www.researchgate.net/publication/332482728_Containers'_Security_Issues_Challenges_and_Road_Ahead (дата обращения: 05.04.2024)
3. Ida, Or. Kubernetes Pentest Methodology [Электронный ресурс] URL: https://www.cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-3 (дата обращения: 05.04.2024)
4. Shamim M. S. I., Bhuiyan F. A., Rahman A. Xi commandments of kubernetes security: A systematization of knowledge related to kubernetes security practices //2020 IEEE Secure Development (SecDev). – 2020. – С. 58-64.
5. Open Policy Agent Documentation [Электронный ресурс] URL: https://www.openpolicyagent.org/docs/latest/ (дата обращения: 05.04.2024)

References

1. Kybernetes Documentation: Securing a Cluster [Electronic resource] URL: https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster / (date of request: 04/05/2024)
2. Containers’ Security: Issues, Challenges, and Road Ahead [Electronic resource] URL: https://www.researchgate.net/publication/332482728_Containers'_Security_Issues_Challenges_and_Road_Ahead (accessed 05.04.2024)
3. Ida Or. Kybernetes Pentest Methodology [Electronic resource] URL: https://www.cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-3 (date of application: 04/05/2024)

4. Shami m M. S. I., Bhuiyan F. A., Rahman A. Xi commands of kubernetes security: A systematization of knowledge related to kubernetes security practices //2020 IEEE Secure Development (SecDev). – 2020. – pp. 58-64.
5. Open Policy Agent Documentation [Electronic resource] URL: https://www.openpolicyagent.org/docs/latest / (date of application: 04/05/2024)