«СА» – 20 лет: наши темы, наши авторы

ISSN 1813-5579 22012

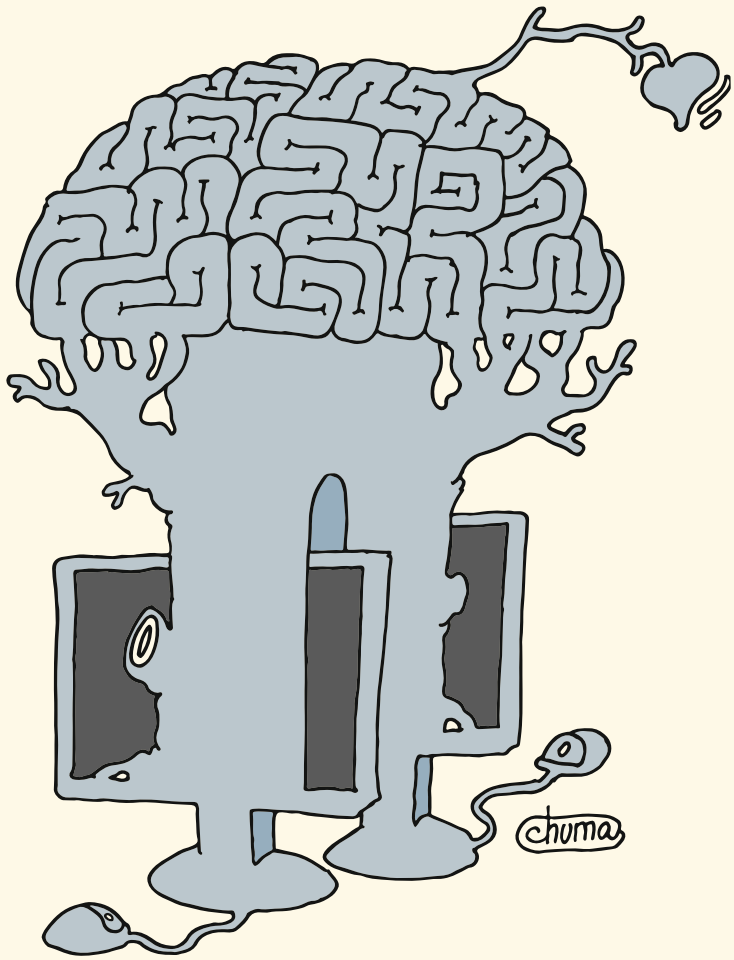
9 771813 557005

Системный администратор

ежемесячный журнал www.samag.ru

№12(241)
2022

В полку микропроцессоров прибыло



DevOps
Openshift и все вокруг него

ZABBIX:
настройка узлов и оповещение через telegram

Мобильная
электронная подпись в ЭДО

Рынок труда
Вакансия года

Дмитрий Гудзенко
«Вложение в себя, в образование – это то, что всегда с тобой»

Реально роботы!
Роботы промышленные, работающие и помогающие человеку

Наука и технологии

Наука и технологии

16+

Программы на языках Julia и Visual Basic .NET для аналитического моделирования многоканальной системы массового обслуживания с буферированием

Создание системы для измерения и оценки психофизиологического состояния водителя на основе аппаратных и программных средств Arduino

Визитка

СЕРГЕЙ ГОЛОВАШОВ,
руководитель центра компетенций DevOPS/ DevSecOPS, компания Bell Integrator

Визитка

НИКОЛАЙ СИТНИКОВ,
инженер DevOps, компания Bell Integrator

Openshift и все вокруг него,
часть 8: Безопасность

Поговорим про безопасность кластера, нейсмпейсов и под. Также будет рассмотрена частная модель угроз и предлагаемые ролевые модели, которые мы считаем правильными для Openshift сегодня.

Безопасность OpenShift – это комбинация двух компонентов, которая в основном обрабатывает ограничения безопасности.

> Ограничения контекста безопасности (SCC)
> Сервисный аккаунт

Ограничения контекста безопасности (SCC)

Он в основном используется для ограничения модуля, что означает, что он определяет ограничения для модуля, а также то, какие действия он может выполнять и какие вещи он может получить в кластере. OpenShift предоставляет набор предопределенных SCC, которые могут быть использованы, изменены и расширены администратором.

```
$ oc get scc
NAME               PRIV   CAPS   HOSTDIR   SELINUX    RUNASUSER          FSGROUP    SUPGROUP   PRIORITY
anyuid             false  []     false     MustRunAs  RunAsAny           RunAsAny   RunAsAny   10
hostaccess         false  []     true      MustRunAs  MustRunAsRange     RunAsAny   RunAsAny   <none>
hostmount-anyuid   false  []     true      MustRunAs  RunAsAny           RunAsAny   RunAsAny   <none>
nonroot            false  []     false     MustRunAs  MustRunAsNonRoot   RunAsAny   RunAsAny   <none>
privileged         true   []     true      RunAsAny   RunAsAny           RunAsAny   RunAsAny   <none>
restricted         false  []     false     MustRunAs  MustRunAsRange     RunAsAny   RunAsAny   <none>
```

Если кто-то хочет использовать какой-либо заранее заданный SCC, это можно сделать просто:

```
$ oadm policy add-user-to-scc <scc_name> <user_name>
$ oadm policy add-group-to-scc <scc_name> <group_name>
```

добавив пользователя или группу в scc-группу.

Сервисный аккаунт

Сервисные учетные записи в основном используются для управления доступом к главному API OpenShift, который вызывается при запуске команды или запроса с любого из главного или узлового компьютера.

Каждый раз, когда приложению или процессу требуется возможность, которая не предоставляется ограниченным SCC, вам нужно будет создать определенную учетную запись службы и добавить учетную запись в соответствующий SCC. Однако, если SCC не соответствует вашим требованиям, лучше создать новый SCC, соответствующий вашим требованиям, а не использовать тот, который лучше всего подходит. В конце установите его для конфигурации развертывания.

```
$ oc create serviceaccount Cadmin
$ oc adm policy add-scc-to-user vipin -z Cadmin
```

Контейнерная безопасность

В OpenShift безопасность контейнеров основана на том, насколько безопасна платформа контейнеров, и где работают контейнеры. Когда мы говорим о безопасности контейнеров и о том, что нужно позаботиться о них, возникает множество вещей.

Image Provenance – внедрена защищенная система маркировки, которая точно и неопровержимо определяет, откуда пришли контейнеры, работающие в производственной среде.

Сканирование безопасности – сканер изображений автоматически проверяет все изображения на наличие известных уязвимостей.

Аудит – производственная среда регулярно проверяется, чтобы убедиться, что все контейнеры основаны на современных контейнерах, а хосты и контейнеры настроены надежно.

Изоляция и минимальные привилегии – контейнеры работают с минимальными ресурсами и привилегиями, необходимыми для эффективного функционирования. Они не могут чрезмерно мешать хосту или другим контейнерам.

Обнаружение угроз во время выполнения – возможность обнаруживать активные угрозы для контейнерного приложения во время выполнения и автоматически реагировать на него.

Контроль доступа – модули безопасности Linux, такие как AppArmor или SELinux, используются для обеспечения контроля доступа.

Существует несколько ключевых методов архивирования безопасности контейнера.

> Управление доступом через oAuth
> Через веб-консоль самообслуживания
> По сертификатам платформы

Управление доступом через OAuth

В этом методе аутентификация для доступа к управлению API архивируется с получением защищенного токена для аутентификации через сервер OAuth, который встроен в главный компьютер OpenShift. Как администратор вы можете изменять конфигурацию сервера OAuth.

Подробнее о настройке сервера OAuth см. в главе 5 этого руководства.

Через веб-консоль самообслуживания

Эта функция безопасности веб-консоли встроена в веб-консоль OpenShift. Эта консоль гарантирует, что все команды, работающие вместе, не имеют доступа к другим средам без аутентификации. Мастер multi-telnet в OpenShift имеет следующие функции безопасности:

- Уровень TCL включен
- Использует сертификат x.509 для аутентификации
- Защищает конфигурацию etcd на главном компьютере

По сертификатам платформы

В этом методе сертификаты для каждого хоста настраиваются во время установки через Ansible. Поскольку он использует протокол связи HTTPS через Rest API, нам необходимо защищенное соединение TCL с различными компонентами и объектами. Это предопределенные сертификаты, однако для доступа можно даже установить собственный сертификат в кластере мастера. Во время первоначальной настройки мастера пользовательские сертификаты могут быть настроены путем переопределения существующих сертификатов с помощью параметра openshift_master_overwrite_named_certificates.

Пример:

```
openshift_master_named_certificates = [{"certfile": "/path/on/host/to/master.crt", "keyfile": "/path/on/host/to/master.key", "cafile": "/path/on/host/to/mastercert.crt"}]
```

Сетевая безопасность

В OpenShift для связи используется программно-определяемая сеть (SDN). Сетевое пространство имен используется для каждого модуля в кластере, причем каждый модуль получает свой собственный IP и диапазон портов для получения сетевого трафика на нем. С помощью этого метода можно изолировать модули, из-за которых они не могут взаимодействовать с модулями в другом проекте.

Изоляция проекта

Это может сделать администратор кластера с помощью следующей команды oadm из CLI.

```
$ oadm pod-network isolate-projects <project name 1> <project name 2>
```

Это означает, что определенные выше проекты не могут взаимодействовать с другими проектами в кластере.

Объем безопасности

Под защитой томов подразумевается защита PV и PVC проектов в кластере OpenShift. В основном в OpenShift есть четыре раздела для управления доступом к томам.

- Дополнительные группы
- fsGroup
- RunAsUser
- seLinuxOptions

Обратите внимание на наличие опций и инструкций SeLinux. Про него мы довольно подробно рассказывали в одной из наших статей про безопасность Linux http://samag.ru/archive/article/4631

Дополнительные группы

Дополнительные группы – это обычные группы Linux. Когда процесс выполняется в системе, он запускается с идентификатором пользователя и идентификатором группы. Эти группы используются для управления доступом к общему хранилищу.

```
# showmount -e <nfs-server-ip-or-hostname>
Export list for f21-nfs.vm:
/opt/nfs *
```

Проверьте монтирование NFS с помощью следующей команды.

```
# cat /etc/exports
/opt/nfs *(rw,sync,no_root_squash)
...
# ls -lZ /opt/nfs -d
drwxrws---. nfsnobody 2325 unconfined_u:object_r:usr_t:s0 /opt/nfs # id nfsnobody
uid = 65534(nfsnobody) gid = 454265(nfsnobody) groups = 454265(nfsnobody)
```

Проверьте сведения о NFS на сервере монтирования, используя следующую команду.

```
apiVersion: v1 kind: Pod
...
spec:
containers:
      name: ... volumeMounts:
- name: nfs
mountPath: /usr/share/... securityContext:
supplementalGroups: [2325] volumes:
      name: nfs nfs:
server: <nfs_server_ip_or_host> path: /opt/nfs
```

/ Opt / nfs / export доступен по UID 454265 и группе 2325.

fsGroup

fsGroup обозначает группу файловой системы, которая используется для добавления дополнительных групп контейнера. Идентификатор группы дополнений используется для

```
kind: Pod spec:
containers:
- name: ... securityContext:
fsGroup: 2325
```

общего хранилища, а fsGroup – для блочного хранилища.

RunAsUser

RunAsUser использует идентификатор пользователя для связи. Это используется при определении изображения контейнера в определении модуля. Один идентификатор

пользователя может быть использован во всех контейнерах, если требуется.

При запуске контейнера указанный идентификатор сопоставляется с идентификатором владельца при экспорте. Если указанный идентификатор определен снаружи, он становится глобальным для всех контейнеров в модуле. Если это определено с определенным модулем, то это становится определенным для единственного контейнера.

Частная модель угроз для OpenShift

Так как в банке угроз отсутствуют угрозы, связанные с контейнерами и средой исполнения контейнеров, считаем, что для них справедливы те же угрозы, что и для виртуальных машин и гипервизоров. По требованиям ФСТЭК Кубернетес является гипервизором 2-го типа и должен защищаться соответствующими наложенными средствами информационной безопасности.

Сокращения и определения:

CSP – Container Security Platform
OPA – Open Policy Agent
SCC – Security Context Constraint
PSP – Pod Security Policy
PAM – Privileged Access Management
WAF – Web-application Firewall
TUF – The Update Framework

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 003	Угроза анализа криптографических алгоритмов и их реализации	Некорректная настройка криптографических алгоритмов в компонентах среды контейниризации (например, TLS)	Применение криптостойких алгоритмов и протоколов шифрования	Настройка спо	5,5
УБИ. 006	Угроза внедрения кода или данных	Отсутствие проверки образов контейнеров	Проверка и контроль целостности образов контейнеров	CSP	8
УБИ. 007	Угроза воздействия на программы с высокими привилегиями	Доступ к компонентам среды контейнеризации (доступ к ядру ОС вычислительного узла, управляющему контуру и т.д.)	Запрет на запуск контейнеров с повышенными привилегиями	CSP / OPA / SCC (PSP)	8,5
УБИ. 008	Угроза восстановления и/или повторного использования аутентификационной информации	Отсутствие или некорректная настройка системы контроля доступа к аутентификационным данным на уровне среды контейниризации	Ротация паролей УЗ администраторов платформы; Контроль доступа к ТУЗ с правами суперпользователя	PAM	7,4
УБИ. 010	Угроза выхода процесса за пределы виртуальной машины	Использование уязвимой версии ядра ОС или среды исполнения контейнеров в среде контейнеризации, запуск контейнеров с неполной изоляцией	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров	CSP / SCC (PSP)	7,8
УБИ. 012	Угроза деструктивного изменения конфигурации/среды окружения программ	Возможность у пользователя изменять переменные среды окружения на уровне среды контейнеризации	Использование ролевой модели; Контроль действий всех администраторов и привилегированных пользователей;	Ролевая модель / PAM	7,3
УБИ. 014	Угроза длительного удержания вычислительных ресурсов пользователями	Перегрузка среды запуска контейнеров одним контейнером	Мониторинг нагрузки на вычислительные узлы	CSP	5,8
УБИ. 015	Угроза доступа к защищаемым файлам с использованием обходного пути	Некорректная настройка разграничения доступа	Контроль доступа к защищаемым файлам; Мониторинг подозрительной активности	CSP / Настройка спо	7,3
УБИ. 016	Угроза доступа к локальным файлам сервера при помощи URL	Уязвимости в веб-клиенте среды контейниризации	Контроль уязвимостей СПО; Защита от эксплуатации веб-уязвимостей	CSP / WAF	7,5
УБИ. 017	Угроза доступа/перехвата/изменения HTTP cookies	Уязвимости в веб-клиенте среды контейниризации	Защита от эксплуатации веб-уязвимостей	WAF	6,6
УБИ. 018	Угроза загрузки нештатной операционной системы	Отсутствие проверки используемой в контейнере ОС + уязвимости в реестре образов	Проверка и контроль целостности базовых образов и образов компонентов платформы	CSP	7,8
УБИ. 020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Отсутствиепревентивных и рантайм проверок запускаемых пользователем приложением	Использование ролевой модели; Контроль действий администраторов проектов; Мониторинг подозрительной активности; Проверка образов контейнеров	CSP	

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 022	Угроза избыточного выделения оперативной памяти	Возможность перегрузить системные компоненты (по оперативной памяти) + отсутствие ограничения на потребление памяти контейнером	Установка ограничений на количество запрашиваемых ресурсов для контейнера	Настройка спо	6,6
УБИ. 023	Угроза изменения компонентов информационной (автоматизированной) системы	Отсутствие контроля доступа к компонентам платформы контейнеризации + уязвимости в компонентов платформы	Использование ролевой модели; Проверка на уязвимости и контроль целостности образов контейнеров и системных пакетов;	CSP / TUF	8,3
УБИ. 025	Угроза изменения системных и глобальных переменных	Возможность у пользователя изменять переменные среды окружения на уровне среды контейнеризации	Использование ролевой модели; Контроль действий всех привилегированных пользователей;	Ролевая модель / PAM	5,8
УБИ. 028	Угроза использования альтернативных путей доступа к ресурсам	Доступ к командной строке контейнера + наличие незащищенных каналов управления	Использование ролевой модели; Ограничение сетевого доступа; Защита от эксплуатации веб-уязвимостей; Защита от угроз сетевых атак	Ролевая модель / Firewall / WAF / CSP / K8S network policies	8,5
УБИ. 030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Использование учетных записей по умолчанию на уровне среды контейнеризации	Ротация credentials компонетов платформы; Контроль доступа к ТУЗ с правами суперпользователя	PAM / Настройка СПО	8,7
УБИ. 031	Угроза использования механизмов авторизации для повышения привилегий	Некорректные настройки системы разграничения доступа среды контейнеризации	Использование ролевой модели; Проверка на уязвимости и контроль целостности образов контейнеров;	CSP	8,5
УБИ. 033	Угроза использования слабостей кодирования входных данных	Уязвимости в API сервере среды контейниризации связаанные с некорректной обработкой входных данных	Проверка на уязвимости образов системных компонентов платформы	CSP	6
УБИ. 034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Использование слабых протоколов сетевого/локального обмена данными в среде контейнеризации	Проверка на уязвимости образов системных компонентов платформы; Проверка настроек платформы на соответствие стандартам	CSP	7,5
УБИ. 036	Угроза исследования механизмов работы программы	Использование дистрибутивов, реализующих среду контейниризации, с открытым исходным кодом	Проверка на уязвимости образов системных компонентов платформы; Использование ролевой модели; Защита от сетевых атак; Ограничение сетевого доступа	CSP / Firewall / Ролевая модель / K8S network policies	7,5
УБИ. 037	Угроза исследования приложения через отчёты об ошибках	Открытый доступ к логам среды контейниризации	Использование ролевой модели	Ролевая модель	7,3
УБИ. 041	Угроза межсайтового скриптинга	Уязвимости в веб-клиенте среды контейниризации	Проверка на уязвимости образов системных компонентов платформы	CSP	7,2
УБИ. 043	Угроза нарушения доступности облачного сервера	Отсутствие защиты от (D-)DoS атак на уровне среды контейниризации	Защита от (D-)DoS атак (на уровнях L2/L3/L7)	WAF / Anti-DDoS / Настройка СПО	
УБИ. 044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Использование уязвимой версии ядра ОС или среды исполнения контейнеров в среде контейнеризации	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров	CSP / SCC (PSP)	8,2
УБИ. 046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Наличие уязвимостей, а также некорректная настройка, протоколов взаимной идентификации и аутентификации среды контейнеризации	Проверка на уязвимости образов системных компонентов платформы; Мониторинг подозрительной активности; Корректные настройки протоколов информационного взаимодействия	CSP / Настройка спо	8,1

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Отсутствие проверки образов контейнеров	Проверка и контроль целостности образов контейнеров	CSP	8,5
УБИ. 052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Отсутствие синхронизации версий ядра хостовой ОС	Синхронизация версий ядра хостовых ОС	(организационная меры)	3,8
УБИ. 058	Угроза неконтролируемого роста числа виртуальных машин	Отсутствие или некорректная настройка системы контроля количества контейнеров (квотирования)	Установка ограничений на количество запускаемых контейнеров (использование механизма квотирования)	Настройка спо	5
УБИ. 059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Отсутствие или некорректная настройка системы контроля выделяемых ресурсов (квотирования)	Установка ограничений на количество запрашиваемых ресурсов для контейнера	Настройка спо	5
УБИ. 063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Неограниченный доступ к программному обеспечению среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности; Контроль действий привилегированных пользователей	Ролевая модель / PAM / CSP	6,5
УБИ. 065	Угроза неопределённости в распределении ответственности между ролями в облаке	Отсутствие фиксированного распределения ответственности между администраторами и пользователями среды контейниризации	Использование ролевой модели	Ролевая модель	
УБИ. 066	Угроза неопределённости ответственности за обеспечение безопасности облака	Отсутствие фиксированной ответственности за обеспечение безопасности среды контейниризации	Наличие в требованиях матрицы ответственности	(организационная меры)	
УБИ. 067	Угроза неправомерного ознакомления с защищаемой информацией	Отсутствие или некорректная настройка системы контроля доступа к данным среды контейниризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности; Контроль изоляции контейнеров	Ролевая модель / PAM / CSP / SCC (PSP)	5,6
УБИ. 068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Уязвимости в API сервере среды контейниризации связаанные с некорректной обработкой входных данных	Проверка на уязвимости образов системных компонентов платформы	CSP	9
УБИ. 069	Угроза неправомерных действий в каналах связи	Некорректная настройка протоколов передачи данных на уровне среды контейниризации	Проверка на уязвимости образов системных компонентов платформы; Применение криптостойких алгоритмов и протоколов шифрования; Ограничение сетевого доступа; Защита от эксплуатации веб-уязвимостей; Защита от угроз сетевых атак	Настройка СПО / Firewall / WAF / CSP / K8S network policies	7,6
УБИ. 070	Угроза непрерывной модернизации облачной инфраструктуры	Отсутствие непрерывной проверки среды контейнеризации на соответствие требованиям безопасности	Непрерываная проверка на уязвимости образов системных компонентов платформы; Мониторинг подозрительной активности	CSP	

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Уязвимости в программном обеспечении компонентов реализующих виртуальную сеть в среде контейниризации	Проверка на уязвимости образов системных компонентов платформы; Защита от сетевых атак	CSP / Firewall	7,2
УБИ. 074	Угроза несанкционированного доступа к аутентификационной информации	Отсутсвие или некорректная настройка системы контроля доступа к аутентификационным данным на уровне среды контейниризации	Ротация credentials компонетов платформы; Контроль доступа к ТУЗ с правами суперпользователя; Использование защищенного канала связи при интеграции со сторонними сервисами аутентификации	PAM / Настройка СПО	8
УБИ. 075	Угроза несанкционированного доступа к виртуальным каналам передачи	Уязвимости в программном обеспечении компонентов реализующих виртуальную сеть в среде контейниризации	Проверка на уязвимости образов системных компонентов платформы; Защита от сетевых атак	CSP / Firewall	7,2
УБИ. 076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Использование уязвимой версии ядра ОС или среды исполнения контейнеров в среде контейнеризации	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров	CSP / SCC (PSP)	7,8
УБИ. 077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Использование уязвимой версии ядра ОС или среды исполнения контейнеров в среде контейнеризации	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров	CSP / SCC (PSP)	5
УБИ. 078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Уязвимости в программном обеспечении компонентов реализующих виртуальную сеть в среде контейниризации	Проверка на уязвимости образов системных компонентов платформы; Защита от сетевых атак; Защита от эксплуатации веб-уязвимостей; Ограничение сетевого доступа	CSP / Firewall / WAF / K8S network policies	8,5
УБИ. 079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Использование уязвимой версии ядра ОС или среды исполнения контейнеров в среде контейнеризации	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров	CSP / SCC (PSP)	7,8
УБИ. 080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Некорректная настройка удаленного доступа к компонентам среды контейнеризации доступным удаленно	Использование ролевой модели; Контроль действий привилегированных пользователей; Защита от сетевых атак;	Ролевая модель / PAM / Firewall	8,5
УБИ. 086	Угроза несанкционированного изменения аутентификационной информации	Отсутсвие или некорректная настройка системы контроля доступа к аутентификационным данным на уровне среды контейниризации	Ротация credentials компонетов платформы; Контроль доступа к ТУЗ с правами суперпользователя; Использование защищенного канала связи при интеграции со сторонними сервисами аутентификации	PAM / Настройка СПО	8
УБИ. 088	Угроза несанкционированного копирования защищаемой информации	Отсутсвие или некорректная настройка системы контроля доступа к защищаемым данным на уровне среды контейниризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности; Контроль изоляции контейнеров	Ролевая модель / PAM / CSP / SCC (PSP)	6,2

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 090	Угроза несанкционированного создания учётной записи пользователя	Некорректная настройка системы контроля доступа в среде контейнеризации	Использование ролевой модели; Контроль доступа к ТУЗ с правами привилегированного пользователя	Ролевая модель / PAM	7,4
УБИ. 094	Угроза несанкционированного управления синхронизацией и состоянием	Отсутствие или некорректная настройка системы контроля доступа к компонентам управления синхронизации среды контейнеризации в том числе и внешним (например, служба синхронизации времени), а также к глобальным параметрам этих компонентов.	Использование ролевой модели; Контроль доступа к ТУЗ с правами привилегированного пользователя;	Ролевая модель / PAM	5,8
УБИ. 095	Угроза несанкционированного управления указателями	Отсутствие или некорректная настройка системы контроля доступа к памяти на уровне среды контейнеризации	Мониторинг подозрительной активности; Контроль изоляции контейнеров	CSP / SCC (PSP)	5
УБИ. 096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Отсутствие инструмента синхронизации политик безопасности облачной инфраструктуры на уровне среды контейнеризации	Автоматизация процессов внедрения и контроля политик безопасности (security governance)	OPA	
УБИ. 098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Использование ненужных сервисов на уровне компонентов среды контейнеризации, отсутствие контроля открытых портов компонентов среды контейнеризации ации	Использование ролевой модели; Ограничение сетевого доступа; Защита от угроз сетевых атак	Ролевая модель / Firewall / CSP / K8S network policies	5
УБИ. 099	Угроза обнаружения хостов	Отсутствие разграничения сетевого доступа на уровне среды контейнеризации	Ограничение сетевого доступа	K8S network policies	5
УБИ. 101	Угроза общедоступности облачной инфраструктуры	Некорректная настройка механизмов изоляции пользовательских ресурсов на уровне среды контейнеризации	Ограничение на запуск пользовательской нагрузки на инфраструктурных узлах с помощью корректной настройки планировщика; Защита от эксплуатации веб-уязвимостей; Защита от угроз сетевых атак	Настройка СПО / Firewall / WAF / K8S network policies	
УБИ. 102	Угроза опосредованного управления группой программ через совместно используемые данные	Отсутствие или некорректная настройка доступа к общим данным распределённых компонентов среды контейнеризации	Ограничение на запуск пользовательской нагрузки на инфраструктурных узлах с помощью корректной настройки планировщика; Защита от угроз сетевых атак	Настройка СПО / Firewall / K8S network policies	2,6
УБИ. 103	Угроза определения типов объектов защиты	Отсутствие или некорректная настройка механизмов контроля входных/выходных данных в компонентах среды контейнеризации	Проверка на уязвимости и контроль целостности образов контейнеров и системных пакетов; Корректная настройка сервисов метаданных; Ограничение сетевого доступа; Защита от сетевых угроз	CSP / TUF / Настройка СПО / Firewall / K8S network policies	3
УБИ. 108	Угроза ошибки обновления гипервизора	Отсутствие процесса проведение регулярных обновлений компонентов среды контейнеризации, а так же экстренного плана возвращения к работоспособному состоянию для данного процесса	Наличие процессов обновления и экстренного отката при обновлениях container host	(организационная меры)	5
УБИ. 109	Угроза перебора всех настроек и параметров приложения	Отсутствие или некорректная настройка механизмов контроля доступа к параметрам компонентов среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности	Ролевая модель / CSP	6,6
УБИ. 114	Угроза переполнения целочисленных переменных	Уязвимости в программных компонентах среды контейнеризации, приводящиец к переполнению целочисленных переменных	Проверка на уязвимости и контроль целостности образов контейнеров и системных пакетов; Мониторинг подозрительной активности	CSP / TUF	5,3

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 117	Угроза перехвата привилегированного потока	Отсутсвие или некорректная настройка механизмов контроля доступа к программным компонентам, имеющим повышенные привилегии в среде контейнеризации к распределённым программным компонентам	Пользование на уязвимости и контроль целостности образов контейнеров, запускаемых в привилегированном режиме (с нарушением изоляции); Мониторинг подозрительной активности	CSP / SCC (PSP)	6,4
УБИ. 118	Угроза перехвата привилегированного процесса	Отсутсвие или некорректная настройка механизмов контроля доступа к программным компонентам, имеющим повышенные привилегии в среде контейнеризации к распределённым программным компонентам	Пользование на уязвимости и контроль целостности образов контейнеров, запускаемых в привилегированном режиме (с нарушением изоляции); Мониторинг подозрительной активности	CSP / SCC (PSP)	7,2
УБИ. 119	Угроза перехвата управления гипервизором	Некорректная настройка механизма контроля доступа до программного интерфейса среды выполнения контейнеров	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров; Использование ролевой модели; Контроль доступа к ТУЗ с правами суперпользователя; Защита от сетевых угроз	CSP / SCC (PSP) / Ролевая модель / PAM / Firewall	8
УБИ. 120	Угроза перехвата управления средой виртуализации	Некорректная настройка механизма контроля доступа до программного интерфейса компонента, отвечающего за управление средой контейнеризации	Контроль уязвимостей Container Runtime и ядра хостовой ОС; Мониторинг подозрительной активности; Контроль изоляции контейнеров; Использование ролевой модели; Контроль доступа к ТУЗ с правами суперпользователя; Защита от сетевых угроз	CSP / SCC (PSP) / Ролевая модель / PAM / Firewall	8
УБИ. 122	Угроза повышения привилегий	Уязвимости в программных компонентах, отвечающих за разграничение доступа в среде контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности; Проверка на уязвимости образов системных компонентов платформы	Ролевая модель / CSP	8,5
УБИ. 124	Угроза подделки записей журнала регистрации событий	Отсутствие контроля доступа к записям журнала регистрации событий на уровне среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности; Контроль действий привилегированных пользователей; Проверка на уязвимости образов системных компонентов платформы	Ролевая модель / PAM / CSP	6,1
УБИ. 140	Угроза приведения системы в состояние «отказ в обслуживании»	Отсутствие защиты от DoS атак на уровне среды контейниризации	Защита от (D-)DoS атак (на уровнях L2/L3/L7)	WAF / Anti-DDoS / Настройка СПО	5
УБИ. 145	Угроза пропуска проверки целостности программного обеспечения	Установка программных компонентов среды контейнеризации без проверки их целостности	Проверка на уязвимости и контроль целостности образов контейнеров и системных пакетов;	CSP / TUF	8,8
УБИ. 149	Угроза сбоя обработки специальным образом изменённых файлов	Отсутствие механизма контроля доступа к файлам конфигурации среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности; Контроль действий привилегированных пользователей	Ролевая модель / PAM / CSP	6,8
УБИ. 152	Угроза удаления аутентификационной информации	Отсутсвие или некорректная настройка системы контроля доступа к аутентификационным данным на уровне среды контейниризации	Контроль доступа к ТУЗ с правами суперпользователя	PAM	6,6
УБИ. 153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Отсутствие защиты от DoS атак на уровне среды контейниризации	Защита от (D-)DoS атак (на уровнях L2/L3/L7)	WAF / Firewall / Anti-DDoS / Настройка спо	3,5

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 155	Угроза утраты вычислительных ресурсов	Отсутствие или некорректная настройка системы контроля выделяемых ресурсов (квотирования)	Использование системы контроля выделяемых ресурсов	Настройка СПО	5
УБИ. 159	Угроза «форсированного веб-браузинга»	Уязвимости в программных компонентах реализующих веб-клиент для управления средой контейнеризации	Проверка на уязвимости образов системных компонентов платформы; Защита от эксплуатации веб-уязвимостей	CSP / WAF	8,7
УБИ. 162	Угроза эксплуатации цифровой подписи программного кода	Использование ненадежных алгоритмов при подписывание компонентов среды контейнеризации	Использование многоэтапного процесса подписи программного кода	TUF	6,7
УБИ. 164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Отсутствие защиты от DoS атак на уровне среды контейнеризации			
УБИ. 165	Угроза включения в проект не достоверно испытанных компонентов	Использование недостоверно испытанных компонентов защиты информации на уровне среды контейнеризации	Наличие процесса выбора СЗИ	(организационная меры)	7,6
УБИ. 169	Угроза наличия механизмов разработчика	Наличие активных механизмов разработчика на уровне среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности; Контроль действий привилегированных пользователей; Контроль изоляции контейнеров	Ролевая модель / PAM / CSP / SCC (PSP)	8,7
УБИ. 170	Угроза неправомерного шифрования информации	Отсутсвие проверки целостности дистрибутивов приложения; Отсутствие или некорректная настройка меахнизма разграничения доступа	Использование ролевой модели; Мониторинг подозрительной активности; Контроль изоляции контейнеров	Ролевая модель / CSP / SCC (PSP)	6
УБИ. 176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Некорректная настройка средств защиты информации на уровне среды контейнеризации	Наличие процесса выбора СЗИ	(организационная меры)	5,3
УБИ. 177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Отсутствие или некорректная настройка средств проверки вводимы данных для средств защиты на уровне среды контейнеризации	Процесс ввода данных оператором должен содержать этап проверки вводимых данных	(организационная меры)	4,3
УБИ. 178	Угроза несанкционированного использования системных и сетевых утилит	Отсутствие ограничения доступа к системным или сетевым утилитам на уровне среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности; Контроль изоляции контейнеров	Ролевая модель / CSP / SCC (PSP)	9,1
УБИ. 179	Угроза несанкционированной модификации защищаемой информации	Отсутствие или некорректная настройка механизма доступа приведшая к получению системных привилегий на уровне среды контейнеризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности; Контроль изоляции контейнеров	Ролевая модель / PAM / CSP / SCC (PSP)	7,7
УБИ. 181	Угроза перехвата одноразовых паролей в режиме реального времени	Отсутствие или некорректная настройка средств защиты информации используемых при передаче одноразовых паролей на уровне среды контейнеризации	Корректная настройка многофакторной аутентикации привилегированных учетных записей	PAM	7,6
УБИ. 183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Отсутствие или некорректная настройка механизма доступа к автоматизированной системе управления технологическими процессами на уровне среды контейнеризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности	Ролевая модель / PAM / CSP	7,6

Ссылка на угрозу	Название угрозы	Уровень среды контейнеризации	Меры митигации	Средство(-а) защиты	Оценка угрозы (CVSS)
УБИ. 187	Угроза несанкционированного воздействия на средство защиты информации	Отсутсвие или некорректная настройка механизма доступа к интерфейсам средств защиты информации на уровне среды контейнеризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности	Ролевая модель / PAM / CSP	5,1
УБИ. 191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Отсутствие проверки целостности дистрибутивов программных компонентов среды контейнеризации	Проверка на уязвимости и контроль целостности образов контейнеров и системных пакетов;	CSP / TUF	8,5
УБИ. 192	Угроза использования уязвимых версий программного обеспечения	Отсутствие процесса проведение регулярных обновлений программных компонентов среды контейнеризации	Проверка на уязвимости и контроль целостности образов контейнеров и системных пакетов;	CSP / TUF	9,9
УБИ. 198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Отсутсвие или некорректная настройка средств антивирусной защиты, а также отсутствие или некорректная настройка механизма контроля доступа на уровне среды контейнеризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности; Наличие процесса создания УЗ администратора	Ролевая модель / PAM / CSP / (организационная меры)	8
УБИ. 208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Отсутствие средств контроля запускаемого ПО для компонентов среды контейнеризации	Использование ролевой модели; Мониторинг подозрительной активности	Ролевая модель / CSP	5
УБИ. 210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Отсутствие процесса проведение регулярных обновлений компонентов среды контейнеризации, а так же экстренного плана возвращения к работоспособному состоянию для данного процесса	Наличие процесса проведение регулярных обновлений компонентов среды контейнеризации, а также экстренного плана возвращения к работоспособному состоянию для данного процесса	(организационная меры)	6,2
УБИ. 211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Отсутствие проверки конфигурационных файлов на уровне среды контейнеризации	Процесс ввода данных оператором должен содержать этап проверки вводимых данных	(организационная меры)	6,2
УБИ. 212	Угроза перехвата управления информационной системой	Отсутствие или некорректная настройка механизмов контроля доступа к панели управления среды контейнеризации	Использование ролевой модель; Контроль доступа к ТУЗ с правами привилегированного пользователя; Мониторинг подозрительной активности	Ролевая модель / PAM / CSP	8,2
УБИ. 214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Отсутствие интеграции системы аудита среды контейнеризации с SOC (Security Operations Center)	Отправка логов аудита в SOC	Настройка СПО	6,1
УБИ. 217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Отсутствие проверки цифровой подписи при загрузке дистрибутивов компонентов среды контейнеризации	Использование многоэтапного процесса подписи программного обеспечения	TUF	8,5

Ролевая модель и роли Openshift

Роль администратора ИС

admin-is.yaml

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
   name: admin-is
rules:
- apiGroups:
   - ''
   resources:
   - configmaps
   - endpoints
   - pods
   - replicationcontrollers
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - ''
   resources:
   - events
   - resourcequotas
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - ''
   resources:
   - namespaces
   - serviceaccounts
   verbs:
   - get
   - list
- apiGroups:
   - ''
   resources:
   - pods/log
   verbs:
   - get
- apiGroups:
   - ''
   resources:
   - services
   verbs:
   - create
   - delete
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - apps
   resources:
   - controllerrevisions
   - deployments
   - statefulsets
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - apps
   resources:
   - deployments/scale
   - statefulsets/scale
   verbs:
   - get
   - patch
   - update
- apiGroups:
   - apps
   resources:
   - replicasets
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - apps.openshift.io
   resources:
   - deploymentconfigs
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - apps.openshift.io
   resources:
   - deploymentconfigs/instantiate
   - deploymentconfigs/rollback
   verbs:
   - create
- apiGroups:
   - apps.openshift.io
   resources:
   - deploymentconfigs/log
   verbs:
   - get
- apiGroups:
   - apps.openshift.io
   resources:
   - deploymentconfigs/scale
   verbs:
   - get
   - patch
   - update
- apiGroups:
   - autoscaling
   resources:
   - horizontalpodautoscalers
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - batch
   resources:
   - jobs
   - cronjobs
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - config.openshift.io
   resources:
   - projects
   verbs:
   - get
   - list
- apiGroups:
   - discovery.k8s.io
   resources:
   - endpointslices
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - events.k8s.io
   resources:
   - events
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - extensions
   resources:
   - ingresses
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
```

```
   - update
   - watch
- apiGroups:
   - image.openshift.io
   resources:
   - imagestreamimages
   - imagestreams/layers
   verbs:
   - get
- apiGroups:
   - image.openshift.io
   resources:
   - imagestreams
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - image.openshift.io
   resources:
   - imagestreamtags
   - imagetags
   verbs:
   - create
   - delete
   - get
   - list
   - patch
   - update
- apiGroups:
   - metrics.k8s.io
   resources:
   - pods
   verbs:
   - get
   - list
- apiGroups:
   - networking.k8s.io
   resources:
   - ingresses
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - policy
   resources:
   - poddisruptionbudgets
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - route.openshift.io
   resources:
   - routes
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - template.openshift.io
   resources:
   - templateinstances
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - template.openshift.io
   resources:
   - templates
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
```

Роль аудитора ИБ

auditor-ib.yaml

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
   name: auditor-ib
rules:
   - verbs:
      - create
      - patch
      - update
      apiGroups:
      - ''
      resources:
      - nodes/proxy
   - verbs:
      - get
      - list
      apiGroups:
      - ''
      resources:
      - nodes
   - verbs:
      - get
      - list
      - watch
 - verbs:
      - get
      - list
      - watch
      apiGroups:
      - operators.coreos.com
      resources:
      - clusterserviceversions
      - catalogsources
      - installplans
      - subscriptions
      - operatorgroups
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - packages.operators.coreos.com
      resources:
      - packagemanifests
      - packagemanifests/icon
   - verbs:
      - get
      apiGroups:
      - apiextensions.k8s.io
      resources:
      - customresourcedefinitions
      resourceNames:
      - clusterloggings.logging.
        openshift.io
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - logging.openshift.io
      resources:
      - clusterloggings
   - verbs:
      - get
      apiGroups:
      - apiextensions.k8s.io
      resources:
      - customresourcedefinitions
      resourceNames:
      - collectors.logging.openshift.io
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - logging.openshift.io
      resources:
      - collectors
   - verbs:
      - get
      apiGroups:
      - apiextensions.k8s.io
      resources:
      - customresourcedefinitions
      resourceNames:
      - lasticsearches.logging.openshift.io
```

```
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - logging.openshift.io
    resources:
    - elasticsearches
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - authentication.istio.io
    - config.istio.io
    - networking.istio.io
    - rbac.istio.io
    - security.istio.io
    - authentication.maistra.io
    - rbac.maistra.io
    resources:
    - '*'
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - jaegers.jaegertracing.io
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - jaegertracing.io
    resources:
    - jaegers
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - kialis.kiali.io
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - kiali.io
    resources:
    - kialis
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - kibanas.logging.openshift.io
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - logging.openshift.io
    resources:
    - kibanas
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - localvolumes.local.storage.
      openshift.io
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - local.storage.openshift.io
    resources:
    - localvolumes
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - logforwardings.logging.
      openshift.io
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - logging.openshift.io
    resources:
    - logforwardings
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - monitoringdashboards.
      monitoring.kiali.io
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - monitoring.kiali.io
    resources:
    - monitoringdashboards
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - packages.operators.coreos.com
    resources:
    - packagemanifests
- verbs:
    - get
    - list
    - watch
    apiGroups:
    - ''
    - image.openshift.io
    resources:
    - imagestreamimages
    - imagestreammappings
    - imagestreams
    - imagestreamtags
- verbs:
    - get
    apiGroups:
    - ''
    - image.openshift.io
    resources:
    - imagestreams/layers
- verbs:
    - get
    apiGroups:
    - ''
    resources:
    - namespaces
- verbs:
    - get
    apiGroups:
    - ''
    - project.openshift.io
    resources:
    - projects
- verbs:
    - get
    apiGroups:
    - ''
    resources:
    - imagetags
- verbs:
    - list
    apiGroups:
    - ''
    resources:
    - imagetags
- verbs:
    - watch
    apiGroups:
    - ''
    resources:
    - imagetags
- verbs:
    - get
    apiGroups:
    - image.openshift.io
    resources:
    - imagetags
- verbs:
    - list
    apiGroups:
    - image.openshift.io
    resources:
    - imagetags
- verbs:
    - watch
    apiGroups:
    - image.openshift.io
    resources:
    - imagetags
- verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
```

```
    resources:
    - customresourcedefinitions
    resourceNames:
    - servicemeshcontrolplanes.
      maistra.io
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - maistra.io
    resources:
    - servicemeshcontrolplanes
  - verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - servicemeshmemberrolls.maistra.io
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - maistra.io
    resources:
    - servicemeshmemberrolls
  - verbs:
    - get
    apiGroups:
    - apiextensions.k8s.io
    resources:
    - customresourcedefinitions
    resourceNames:
    - servicemeshmembers.maistra.io
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - maistra.io
    resources:
    - servicemeshmembers
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - ''
    resources:
    - configmaps
    - endpoints
    - persistentvolumeclaims
    - persistentvolumeclaims/status
    - pods
    - replicationcontrollers
    - replicationcontrollers/scale
    - serviceaccounts
    - services
    - services/status
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - ''
    resources:
    - bindings
    - events
    - limitranges
    - namespaces/status
    - pods/log
    - pods/status
    - replicationcontrollers/status
    - resourcequotas
    - resourcequotas/status
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - ''
    resources:
    - namespaces
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - apps
    resources:
    - controllerrevisions
    - daemonsets
    - daemonsets/status
    - deployments
    - deployments/scale
    - deployments/status
    - replicasets
    - replicasets/scale
    - replicasets/status
    - statefulsets
    - statefulsets/scale
    - statefulsets/status
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - autoscaling
    resources:
    - horizontalpodautoscalers
    - horizontalpodautoscalers/status
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - batch
    resources:
    - cronjobs
    - cronjobs/status
    - jobs
    - jobs/status
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - extensions
    resources:
    - daemonsets
    - daemonsets/status
    - deployments
    - deployments/scale
    - deployments/status
    - ingresses
    - ingresses/status
    - networkpolicies
    - replicasets
    - replicasets/scale
    - replicasets/status
    - replicationcontrollers/scale
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - policy
    resources:
    - poddisruptionbudgets
    - poddisruptionbudgets/status
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - networking.k8s.io
    resources:
    - ingresses
    - ingresses/status
    - networkpolicies
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - metrics.k8s.io
    resources:
    - pods
    - nodes
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - snapshot.storage.k8s.io
    resources:
    - volumesnapshots
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - ''
    - build.openshift.io
    resources:
    - buildconfigs
    - buildconfigs/webhooks
    - builds
  - verbs:
    - get
    - list
    - watch
    apiGroups:
    - ''
    - build.openshift.io
    resources:
    - builds/log
  - verbs:
```

```
      - view
      apiGroups:
      - build.openshift.io
      resources:
      - jenkins
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - apps.openshift.io
      resources:
      - deploymentconfigs
      - deploymentconfigs/scale
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - apps.openshift.io
      resources:
      - deploymentconfigs/log
      - deploymentconfigs/status
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - image.openshift.io
      resources:
      - imagestreams/status
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - quota.openshift.io
      resources:
      - appliedclusterresourcequotas
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - route.openshift.io
      resources:
      - routes
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - route.openshift.io
      resources:
      - routes/status
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - template.openshift.io
      resources:
      - processedtemplates
      - templateconfigs
      - templateinstances
      - templates
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      - build.openshift.io
      resources:
      - buildlogs
   - verbs:
      - get
      - list
      - watch
      apiGroups:
      - ''
      resources:
      - resourcequotausages
```

Роль разработчика

```
developer.yaml
apiVersion: rbac.authorization.k8s.io/
v1
kind: ClusterRole
metadata:
   name: developer
rules:
- apiGroups:
   - ''
   resources:
   - configmaps
   - endpoints
   - pods
   - replicationcontrollers
   - secrets
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - ''
   resources:
   - events
   - resourcequotas
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - ''
   resources:
   - namespaces
   - serviceaccounts
   verbs:
   - get
   - list
- apiGroups:
   - ''
   resources:
   - pods/attach
   - pods/exec
   - pods/portforward
   verbs:
   - create
   - get
- apiGroups:
   - ''
   resources:
   - pods/eviction
   verbs:
   - create
- apiGroups:
   - ''
   resources:
   - pods/log
   verbs:
   - get
- apiGroups:
   - ''
   resources:
   - pods/proxy
   - services/proxy
   verbs:
   - create
   - delete
   - get
   - patch
   - update
- apiGroups:
   - ''
   resources:
   - replicationcontrollers/scale
   verbs:
   - get
   - patch
   - update
- apiGroups:
   - ''
   resources:
   - services
   verbs:
   - create
   - delete
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - apps
   resources:
   - controllerrevisions
   - deployments
   - statefulsets
```

```
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - apps
    resources:
    - deployments/scale
    - statefulsets/scale
    verbs:
    - get
    - patch
    - update
- apiGroups:
    - apps
    resources:
    - replicasets
    verbs:
    - get
    - list
    - watch
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs/instantiate
    - deploymentconfigs/rollback
    verbs:
    - create
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs/log
    verbs:
    - get
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs/scale
    verbs:
    - get
    - patch
    - update
- apiGroups:
    - authorization.k8s.io
    resources:
    - localsubjectaccessreviews
    verbs:
    - create
- apiGroups:
    - authorization.openshift.io
    resources:
    - localresourceaccessreviews
    - localsubjectaccessreviews
    - selfsubjectrulesreviews
    - subjectrulesreviews
    verbs:
    - create
- apiGroups:
    - autoscaling
    resources:
    - horizontalpodautoscalers
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - batch
    resources:
    - jobs
    - cronjobs
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - build.openshift.io
    resources:
    - buildconfigs
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - build.openshift.io
    resources:
    - buildconfigs/instantiate
    - buildconfigs/instantiatebinary
    - buildconfigs/webhooks
    - builds
    - builds/clone
    - builds/log
    verbs:
    - create
- apiGroups:
    - config.openshift.io
    resources:
    - projects
    verbs:
    - get
    - list
- apiGroups:
    - discovery.k8s.io
    resources:
    - endpointslices
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - events.k8s.io
    resources:
    - events
    verbs:
    - get
    - list
    - watch
- apiGroups:
    - extensions
    resources:
    - ingresses
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreamimages
    - imagestreams/layers
    - imagestreams/secrets
    verbs:
    - get
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreamimports
    verbs:
    - create
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreams
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreamtags
    - imagetags
    verbs:
    - create
```

```
   - delete
   - get
   - list
   - patch
   - update
- apiGroups:
   - metrics.k8s.io
   resources:
   - pods
   verbs:
   - get
   - list
- apiGroups:
   - networking.k8s.io
   resources:
   - ingresses
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - policy
   resources:
   - poddisruptionbudgets
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - route.openshift.io
   resources:
   - routes
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - template.openshift.io
   resources:
   - processedtemplates
   verbs:
   - create
- apiGroups:
   - template.openshift.io
   resources:
   - templateinstances
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - template.openshift.io
   resources:
   - templates
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
```

Роль сервисного аккаунта

deployer.yaml

```
apiVersion: rbac.authorization.k8s.io/
v1
kind: ClusterRole
metadata:
   name: deployer
rules:
- apiGroups:
   - ''
   resources:
   - configmaps
   - endpoints
   - pods
   - replicationcontrollers
   - secrets
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - ''
   resources:
   - events
   - resourcequotas
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - ''
   resources:
   - namespaces
   - serviceaccounts
   verbs:
   - get
   - list
- apiGroups:
   - ''
   resources:
   - pods/log
   verbs:
   - get
- apiGroups:
   - ''
   resources:
   - replicationcontrollers/scale
   verbs:
   - get
   - patch
   - update
- apiGroups:
   - ''
   resources:
   - services
   verbs:
   - create
   - delete
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - apps
   resources:
   - controllerrevisions
   - deployments
   - statefulsets
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
   - watch
- apiGroups:
   - apps
   resources:
   - deployments/scale
   - statefulsets/scale
   verbs:
   - get
   - patch
   - update
- apiGroups:
   - apps
   resources:
   - replicasets
   verbs:
   - get
   - list
   - watch
- apiGroups:
   - apps.openshift.io
   resources:
   - deploymentconfigs
   verbs:
   - create
   - delete
   - deletecollection
   - get
   - list
   - patch
   - update
```

```
    - watch
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs/instantiate
    - deploymentconfigs/rollback
    verbs:
    - create
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs/log
    verbs:
    - get
- apiGroups:
    - apps.openshift.io
    resources:
    - deploymentconfigs/scale
    verbs:
    - get
    - patch
    - update
- apiGroups:
    - autoscaling
    resources:
    - horizontalpodautoscalers
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - batch
    resources:
    - jobs
    - cronjobs
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - config.openshift.io
    resources:
    - projects
    verbs:
    - get
    - list
- apiGroups:
    - discovery.k8s.io
    resources:
    - endpointslices
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - events.k8s.io
    resources:
    - events
    verbs:
    - get
    - list
    - watch
- apiGroups:
    - extensions
    resources:
    - ingresses
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreamimages
    - imagestreams/layers
    verbs:
    - get
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreams
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - image.openshift.io
    resources:
    - imagestreamtags
    - imagetags
    verbs:
    - create
    - delete
    - get
    - list
    - patch
    - update
- apiGroups:
    - metrics.k8s.io
    resources:
    - pods
    verbs:
    - get
    - list
- apiGroups:
    - networking.k8s.io
    resources:
    - ingresses
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - policy
    resources:
    - poddisruptionbudgets
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - route.openshift.io
    resources:
    - routes
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
- apiGroups:
    - template.openshift.io
    resources:
    - processedtemplates
    verbs:
    - create
- apiGroups:
    - template.openshift.io
    resources:
    - templateinstances
    verbs:
    - get
    - list
    - watch
- apiGroups:
    - template.openshift.io
    resources:
    - templates
    verbs:
    - create
    - delete
    - deletecollection
    - get
    - list
    - patch
    - update
    - watch
```

Ключевые слова: безопасность в openshift и kubernetes.

Визитка

СЕРГЕЙ ГОЛОВАШОВ,
руководитель центра компетенций DevOPS/ DevSecOPS, компания Bell Integrator

Визитка

НИКОЛАЙ СИТНИКОВ,
инженер DevOps, компания Bell Integrator

Openshift и все вокруг него, часть 9: ISTIO

В данной статье мы завершаем цикл про Openshift и разговариваем про безопасность кластера, нейсмпейсов и под, рассматриваем работу Istio.

Для начала разберемся, что такое Service Mesh, и кому он нужен.

Service Mesh (с англ. «сервисная сетка») – слой архитектуры, отвечающий за надежную доставку запросов через сложную сеть микросервисов.

Когда ваше приложение выросло из монолита в микросервисную архитектуру, то с каждым днем становится все сложнее ею управлять и мониторить. В таком случае вам необходимо переходить на решения, которые решают часть проблем, связанных с микросервисами:

- балансировка нагрузки внутри микросервисной сетки;
- обнаружение сервисов (Service discovery);
- восстановление после сбоев (Failure recovery);
- метрики;
- мониторинг.

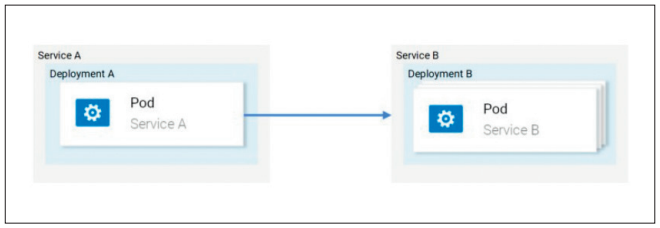
Также решают более сложные задачи:

- A/B тестирование;
- канареечные выкатки (Canary rollouts);
- контроль доступа (Access control);
- сквозная аутентификация (end-to-end authentication).

Тут на помощь приходит Istio, созданный компаниями Google, IBM и Lyft.

Идея Istio

В мире без Istio один сервис делает прямые запросы к другому, а в случае сбоя сервис должен сам обработать его: предпринять новую попытку, предусмотреть таймаут, открыть circuit breaker и т.п.



Istio же предлагает специализированное решение, полностью отделённое от сервисов и функционирующее путём вмешательства в сетевое взаимодействие. И таким образом оно реализует:

- **Отказоустойчивость**: опираясь на код статуса в ответе, оно понимает, произошёл ли сбой в запросе, и выполняет его повторно.
- **Канареечные выкаты**: перенаправляет на новую версию сервиса лишь фиксированное процентом число запросов.
- **Мониторинг и метрики**: за какое время сервис ответил?
- **Трассировка и наблюдаемость**: добавляет специальные заголовки в каждый запрос и выполняет их трассировку в кластере.
- **Безопасность**: извлекает JWT-токен, аутентифицирует и авторизует пользователей.

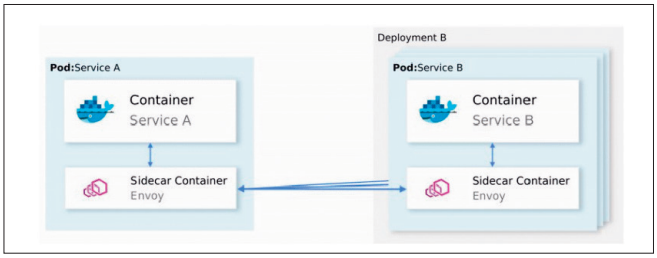
Это лишь некоторые из возможностей, чтобы заинтриговать вас. А теперь давайте погрузимся в технические подробности.

Архитектура Istio

Istio перехватывает весь сетевой трафик и применяет к нему набор правил, вставляя в каждый pod умный прокси в виде sidecar-контейнера. Прокси, которые активируют все возможности, образуют собой Data Plane, и они могут динамически настраиваться с помощью Control Plane.

Data Plane

Вставляемые в pod'ы прокси позволяют Istio с лёгкостью добиться соответствия нужным нам требованиям. Например, проверим функции повторных попыток и circuit breaker.



Подытожим:

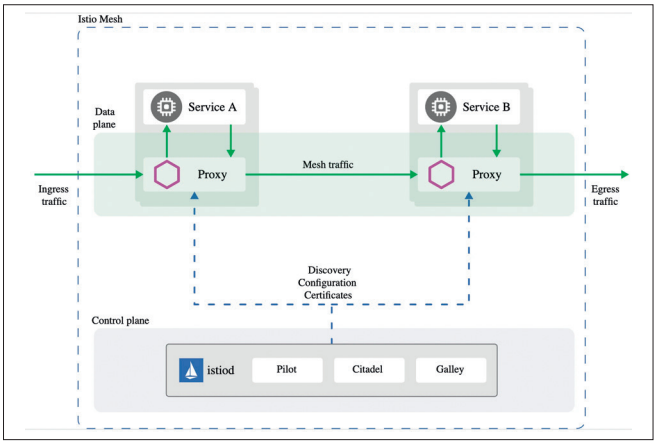
- Envoy (речь про прокси, находящийся в sidecar-контейнере, который распространяется и как отдельный продукт – прим. перев.) отправляет запрос первому экземпляру сервиса B и происходит сбой.
- Envoy Sidecar предпринимает повторную попытку (retry). (1)
- Запрос со сбоем возвращается вызвавшему его прокси.
- Так открывается Circuit Breaker и происходит вызов следующего сервиса для последующих запросов. (2)

Это означает, что вам не придётся использовать очередную библиотеку Retry, не придётся делать свою реализацию Circuit Breaking и Service Discovery на языке программирования X, Y или Z. Всё это и многое другое доступно из коробки в Istio и не требует никаких изменений в коде.

Отлично! Теперь вы можете захотеть отправиться в вояж с Istio, но всё ещё есть какие-то сомнения, открытые вопросы. Если это универсальное решение на все случаи в жизни, то у вас возникает закономерное подозрение: ведь все такие решения в действительности оказываются не подходящими ни для какого случая. И вот наконец вы спросите: «Оно настраивается?» Теперь вы готовы к морскому путешествию – и давайте же познакомимся с Control Plane.

Control Plane

Он состоит из трёх компонентов: Pilot, Mixer и Citadel, – которые совместными усилиями настраивают Envoy'и для маршрутизации трафика, применяют политики и собирают телеметрические данные. Схематично всё это выглядит так:



Envoy'и (т.е. data plane) сконфигурированы с помощью Kubernetes CRD (Custom Resource Definitions) определёнными Istio и специально предназначенными для этой цели. Для вас это означает, что они представляются очередным ресурсом в Kubernetes со знакомым синтаксисом. После создания этот ресурс будет подобран control plane'ом и применён к Envoy'ям.

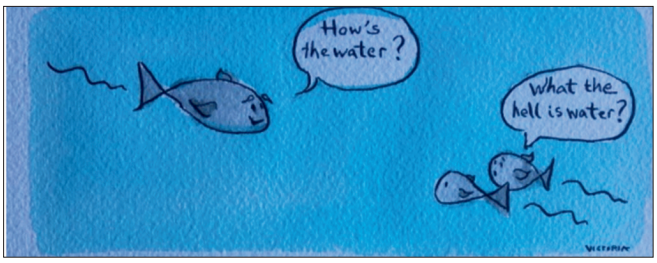
Отношение сервисов к Istio

Мы описали отношение Istio к сервисам, но не обратное: как же сервисы относятся к Istio?

Честно говоря, о присутствии Istio сервисам известно так же хорошо, как рыбам – о воде, когда они спрашивают себя: «Что вообще такое вода?».

Таким образом, вы можете взять рабочий кластер и после деплоя компонентов Istio сервисы, находящиеся в нём, продолжат работать, а после устранения этих компонентов – снова всё будет хорошо. Понятное дело, что при этом вы потеряете возможности, предоставляемые Istio.

Иллюстрация Victoria Dimitrakopoulos: – Как вам вода? – Что вообще такое вода?



Достаточно теории – давайте перенесём это знание в практику!

Установка и настройка istio

Будем запускать Istio.

Загрузите и установите ISTIO CLI.

Прежде, чем мы сможем начать настройку Istio, нам нужно сначала установить инструменты командной строки, с которыми вы будете взаимодействовать.

Для этого запустите следующую команду:

```
curl -L https://git.io/getLatestIstio | sh -
// version can be different as istio gets upgraded
cd istio-*
sudo mv -v bin/istioctl /usr/local/bin/
```

Пример вывода:

```
# curl -L https://git.io/getLatestIstio | sh -    % Total
% Received % Xferd  Average Speed   Time    Time     Time
Current                                 Dload  Upload
Total   Spent    Left  Speed   0     0    0     0    0     0
0      0 --:--:-- --:--:-- --:--:--     0 100  1631  100
1631    0     0   1849      0 --:--:-- --:--:-- --:--:--
1849 Downloading istio-1.1.2 from https://github.com/istio/
istio/releases/download/1.1.2/istio-1.1.2-linux.tar.gz ...
% Total    % Received % Xferd  Average Speed   Time    Time
Time  Current                                 Dload  Upload
Total   Spent    Left  Speed 100   614    0   614    0     0
1485      0 --:--:-- --:--:-- --:--:--  1483 100 15.0M  100
15.0M    0     0  8379k      0  0:00:01  0:00:01 --:--:-
- 21.5M Downloaded into istio-1.1.2: bin  install  istio-
telemetry.yaml  istio.VERSION  LICENSE  README.md  samples
tools Add /root/istio-1.1.2/bin to your path; e.g copy paste
in your shell and/or ~/.profile: export PATH="$PATH:/root/
istio-1.1.2/bin" root@kube-master:~# cd istio-*  root@kube-
master:~/istio-1.1.2# sudo mv -v bin/istioctl /usr/local/bin/
'bin/istioctl' -> '/usr/local/bin/istioctl'
```

Установка ISTIO

Определим учетную запись для Tiller

Сначала создайте сервисную учетную запись для Tiller:

```
kubectl apply -f install/kubernetes/helm/helm-service-
account.yaml
```

Вывод:

```
serviceaccount/tiller unchanged
clusterrolebinding.rbac.authorization.k8s.io/tiller unchanged
```

Установите Istio CRD

```
# helm install install/kubernetes/helm/istio-init --name
istio-init --namespace istio-system
```

Проверим установку:

```
# kubectl get crds | grep 'istio.io'
adapters.config.istio.io              2019-04-08T12:39:02Z
apikeys.config.istio.io               2019-04-08T12:39:02Z
attributemanifests.config.istio.io    2019-04-08T12:39:01Z
authorizations.config.istio.io        2019-04-08T12:39:02Z
bypasses.config.istio.io              2019-04-08T12:39:02Z
checknothings.config.istio.io         2019-04-08T12:39:02Z
circonuses.config.istio.io            2019-04-08T12:39:02Z
cloudwatches.config.istio.io          2019-04-08T12:39:00Z
clusterrbacconfigs.rbac.istio.io      2019-04-08T12:39:01Z
deniers.config.istio.io               2019-04-08T12:39:02Z
destinationrules.networking.istio.io 2019-04-08T12:39:01Z
dogstatsds.config.istio.io            2019-04-08T12:39:00Z
edges.config.istio.io                 2019-04-08T12:39:02Z
envoyfilters.networking.istio.io      2019-04-08T12:39:01Z
fluentds.config.istio.io              2019-04-08T12:39:02Z
gateways.networking.istio.io          2019-04-08T12:39:01Z
.....
....
```

Наконец, установите основные компоненты Istio:

```
# helm install install/kubernetes/helm/istio --name istio
--namespace istio-system --set global.configValidation=false
--set sidecarInjectorWebhook.enabled=false --set grafana.
enabled=true --set servicegraph.enabled=true
```

Проверьте установленные службы:

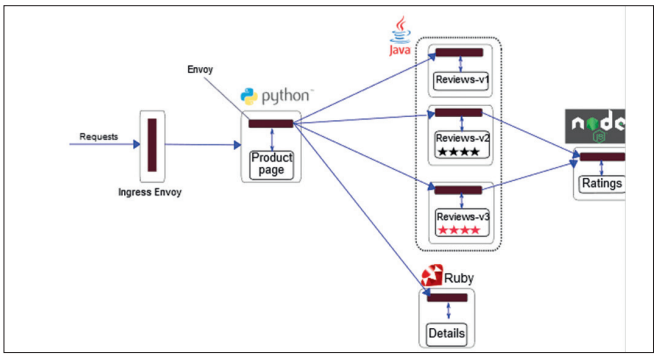
```
# kubectl get svc -n istio-system
NAME        TYPE     CLUSTER-IP     EXTERNAL-IP    PORT(S)  AGE
grafana  ClusterIP  10.96.171.173  <none>  3000/TCP  2m40s
istio-citadel  ClusterIP  10.96.65.75  <none>  8060/TCP,15014/
TCP  2m40s
istio-galley  ClusterIP  10.106.97.125  <none>  443/TCP,15014/
TCP,9901/TCP  2m40s
istio-ingressgateway  LoadBalancer  10.102.204.117
172.20.240.112   80:31380/TCP,443:31390/TCP,31400:31400/
TCP,15029:30709/TCP,15030:30672/TCP,15031:31789/
TCP,15032:32654/TCP,15443:30390/TCP,15020:31778/TCP  2m40s
istio-pilot  ClusterIP  10.109.0.98  <none>  15010/TCP,15011/
TCP,8080/TCP,15014/TCP  2m40s
istio-policy  ClusterIP  10.106.140.39  <none>  9091/
TCP,15004/TCP,15014/TCP  2m40s
istio-telemetry  ClusterIP  10.98.74.109  <none>  9091/
TCP,15004/TCP,15014/TCP,42422/TCP  2m40s
prometheus  ClusterIP  10.98.183.129  <none>  9090/TCP  2m40s
servicegraph  ClusterIP  10.100.212.98  <none>  8088/TCP
```

Убедитесь, что поды находятся в рабочем состоянии.

```
# kubectl get pods -n istio-system
NAME                                READY STATUS RESTARTS AGE
grafana-57586c685b-5nsb9              1/1   Running  0 3m25s
istio-citadel-7579f8fbb9-frnqz        1/1   Running  0 3m25s
istio-galley-79d4c5d9f7-llpvk         1/1   Running  0 3m25s
istio-ingressgateway-5fbcf4488f-vzt98 1/1   Running  0  3m25s
istio-init-crd-10-cwn8j               0/1   Completed 0  6m28s
istio-init-crd-11-k4lx4               0/1   Completed 0  6m28s
istio-pilot-df78f86cb-sfzjt           2/2   Running  0  3m25s
istio-policy-5f4747447c-rvt72         2/2   Running  2  3m25s
istio-telemetry-84697c64d7-btbbm      2/2   Running  2  3m25s
prometheus-66c9f5694-lp2wq            1/1   Running  0  3m25s
servicegraph-57d6f5b58c-4m92m         1/1   Running  1  3m24s
```

Развернем образец приложения.

Теперь, когда у нас есть все ресурсы, установленные для Istio, мы будем использовать пример приложения под названием BookInfo для проверки ключевых возможностей service mesh, таких как интеллектуальная маршрутизация, просмотр данных телеметрии с помощью Prometheus & Grafana.



Приложение Bookinfo разбито на четыре отдельных микросервиса:

- productpage. Микросервис productpage вызывает детали и просматривает микросервисы для заполнения страницы.
- details. Микросервис details содержит информацию о книках.
- reviews. Микросервис reviews содержит рецензии на книги.
- ratings. Микросервис ratings содержит информацию о рейтинге книг, которая сопровождает рецензирование книг.

Существует три версии микросервиса reviews:

- Версия v1 не вызывает службу ratings.
- Версия v2 вызывает сервис ratings и отображает каждый рейтинг в виде от 1 до 5 черных звездочек.
- Версия v3 вызывает сервис ratings и отображает каждый рейтинг в виде от 1 до 5 красных звездочек.

Развертывание примера приложения

Разверните примеры приложений вручную, добавив istio proxy и подтвердив, что службы работают правильно

```
# kubectl apply -f <(istioctl kube-inject -f samples/
bookinfo/platform/kube/bookinfo.yaml)
```

Пример вывода:

```
service/details created
deployment.extensions/details-v1 created
service/ratings created
deployment.extensions/ratings-v1 created
service/reviews created
deployment.extensions/reviews-v1 created
deployment.extensions/reviews-v2 created
deployment.extensions/reviews-v3 created
service/productpage created
deployment.extensions/productpage-v1 created
```

Убедитесь, что поды и службы запущены:

```
# kubectl get pod,svc
```

```
NAME                                READY STATUS RESTARTS AGE
pod/details-v1-54c6f46b4b-q5b45       2/2   Running  0  58s
pod/my-nginx-6cc48cd8db-n6scm         1/1   Running  4  27d
pod/productpage-v1-5c4f6df4dd-7lcws  2/2   Running  0  58s
pod/ratings-v1-6ccbd9c4f4-2cjbd       2/2   Running  0  58s
pod/reviews-v1-bfc99c79-jhqr6         2/2   Running  0  58s
pod/reviews-v2-6ffb5f6b44-zf9tt       2/2   Running  0  58s
pod/reviews-v3-7c67bd445-bc5ms        2/2   Running  0  58s

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
service/details ClusterIP 10.99.96.161 <none> 9080/TCP 58s
```

```
service/kubernetes ClusterIP 10.96.0.1 <none> 443/TCP 27d
service/productpage ClusterIP 10.106.134.93 <none> 9080/TCP 58s
service/ratings ClusterIP 10.106.213.22 <none> 9080/TCP 58s
service/reviews ClusterIP 10.100.60.83 <none> 9080/TCP 58s
```

Определите виртуальный сервис и ingress:

```
# kubectl apply -f samples/bookinfo/networking/
bookinfo-gateway.yaml
```

Вывод:

```
gateway.networking.istio.io/bookinfo-gateway created
virtualservice.networking.istio.io/bookinfo created
```

Настройка маршрутизации запросов

Service versions (a.k.a. subsets).

В сценарии непрерывного развертывания предоставляемый сервис может иметь разные подмножества и может запускать разные версии одного и того же приложения.

Распространенные сценарии, в которых это происходит, включают A/B-тестирование, развертывание канареек и т. д.

Выбор конкретной версии может быть решен на основе различных критериев (заголовки, URL-адрес и т. д.). И/или объемов, присвоенных каждой версии.

Каждый сервис имеет версию по умолчанию, состоящую из всех его экземпляров.

Чтобы продемонстрировать это поведение применим правило назначения

```
# kubectl apply -f samples/bookinfo/networking/destination-
rule-all.yaml
```

Вывод:

```
destinationrule.networking.istio.io/productpage created
destinationrule.networking.istio.io/reviews created
destinationrule.networking.istio.io/ratings created
destinationrule.networking.istio.io/details created
```

Посмотреть правило назначения для bookinfo

```
kubectl get destinationrules -o yaml
```

Вывод:

```
...
...
spec:
   host: details
   subsets:
   - labels:
      version: v1
     name: v1
   - labels:
      version: v2
     name: v2

spec:
   host: productpage
   subsets:
   - labels:
      version: v1
     name: v1

spec:
   host: ratings
   subsets:
   - labels:
      version: v1
     name: v1
   - labels:
      version: v2
     name: v2
   - labels:
      version: v2-mysql
     name: v2-mysql
   - labels:
      version: v2-mysql-vm
     name: v2-mysql-vm

spec:
   host: reviews
   subsets:
   - labels:
      version: v1
     name: v1
   - labels:
      version: v2
     name: v2
   - labels:
      version: v3
     name: v3
```

Для маршрутизации только к одной версии вы применяете виртуальные службы, которые устанавливают версию по умолчанию для микросервисов.

В этом случае виртуальные сервисы направят весь трафик на reviews:v1.

```
# kubectl apply -f samples/bookinfo/networking/virtual-
service-all-v1.yaml
```

Вывод

```
virtualservice.networking.istio.io/productpage created
virtualservice.networking.istio.io/reviews created
virtualservice.networking.istio.io/ratings created
virtualservice.networking.istio.io/details created
```

```
# kubectl get virtualservices reviews -o yaml
```

Вывод

```
.......
.......
spec:
  hosts:
  - reviews
  http:
  - route:
   - destination:
      host: reviews
      subset: v1
```

Маршрут, основанный на идентификации пользователя

Пользовательская маршрутизация. В этом случае весь трафик от пользователя с именем Jason будет перенаправлен на обзоры сервиса: v2.

```
# kubectl apply -f samples/bookinfo/networking/virtual-
service-reviews-test-v2.yaml
```

Вывод

```
virtualservice.networking.istio.io/reviews configured
```

Если заголовок пользователя соответствует jason, он будет перенаправлен на reviews: v2.

```
kubectl get virtualservices reviews -o yaml
```

```
...........
...........
spec:
  hosts:
  - reviews
  http:
  - match:
   - headers:
      end-user:
        exact: jason
   route:
   - destination:
      host: reviews
      subset: v2
  - route:
   - destination:
      host: reviews
      subset: v1
```

Маршрут на основе трафика

Далее мы покажем, как постепенно переносить трафик с одной версии микросервиса на другую.

В нашем примере мы отправим 50% трафика на reviews: v1 и 50% на reviews: v3.

```
kubectl apply -f samples/bookinfo/networking/virtual-service-
all-v1.yaml
kubectl apply -f samples/bookinfo/networking/virtual-service-
reviews-50-v3.yaml
kubectl get virtualservice reviews -o yaml
```

Subset установлен для 50% трафика на v1 и 50% трафика на v3 для всех запросов reviews

```
root@kube-master:~/istio-1.1.2# kubectl get virtualservice
reviews -o yaml
.............
.............
spec:
  hosts:
  - reviews
  http:
  - route:
   - destination:
      host: reviews
      subset: v1
     weight: 50
   - destination:
      host: reviews
      subset: v3
     weight: 50
```

Мониторинг и визуализация IIstio

Сначала соберите новые данные телеметрии и загрузите файл YAML для хранения конфигурации для новой метрики и потока журналов, которые Istio будет генерировать и собирать автоматически.

```
# curl -LO https://eksworkshop.com/servicemesh/deploy.files/
istio-telemetry.yaml
# kubectl apply -f istio-telemetry.yaml
```

Вывод:

```
% Total  % Received % Xferd  Average Speed   Time   Time
Time  Current  0    0     0 --:--:-- --:--:-- --:--:--
0 100  2254  100  2254 0    0   3994     0 --:--:-- --:--:--
--:--:--  3996
metric.config.istio.io/doublerequestcount created
prometheus.config.istio.io/doublehandler created
rule.config.istio.io/doubleprom created
logentry.config.istio.io/newlog created
stdio.config.istio.io/newhandler created
rule.config.istio.io/newlogstdio created
```

Убедитесь в наличии служб prometheus и grafana

```
# kubectl -n istio-system get svc prometheus
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
prometheus ClusterIP 10.98.183.129 <none> 9090/TCP 75m
```

```
# kubectl -n istio-system get svc grafana
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
grafana ClusterIP 10.96.171.173 <none> 3000/TCP 75m
```

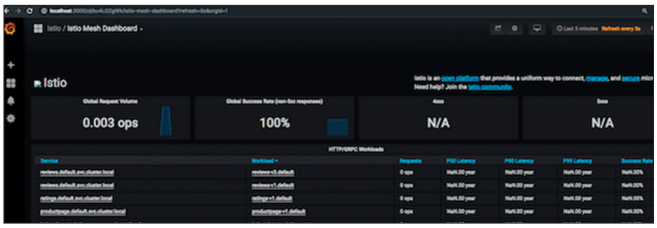
Настройте переадресацию портов для grafana.

```
kubectl -n istio-system port-forward $(kubectl -n istio-
system get pod -l app=grafana -o jsonpath='{.items[0].
metadata.name}') 8080:3000
```

Вывод:

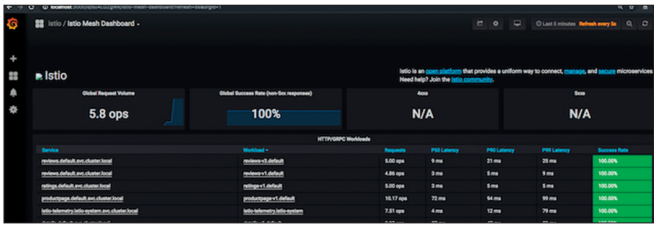
```
items [0]. metadata.name}') 8080:3000
Forwarding from 127.0.0.1:8080 -> 3000
```

Откройте GUI grafana.



Откройте новый терминал и отправьте трафик на mesh

```
# while true; do curl -o /dev/null -s "172.20.240.112/
productpage"; done
```



Зеркалирование трафика

Иногда нужно проверить новую версию на большем количестве пользователей, но выкатывать в прод нельзя. Для этого в Istio есть функционал зеркалирование трафика, мы запускаем параллельно новую версию сервиса и направляем туда трафик, не задевая при этом рабочую версию сервиса.

Для этого создаем файл istio-mirroring.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ratings
spec:
  hosts:
   - ratings
   http:
   - route:
    - destination:
       host: ratings
       subset: v1
       weight: 100
   mirror:
     host:
      ratings
      subset: v2
```

Применяем

```
kubectl -n mesh apply -f istio-mirroring.yaml
```

Проверяем

```
while true;do curl http://<load_balancer_ip>/gateway/books;
sleep 2;done
```

Вывод:

```
[
{
"id": 1,
"name": "War and Piece", "rating": 455.45, "presentation": ":-)",
"description": null
},
{
"id": 2,
"name": "Anna Karenina", "rating": 666.4, "presentation": "
:-)", "description": null
},
...
]
```

В логах контейнера ratings второй версии видим, что трафик зеркалируется и на него

```
2019-09-18 11:19:04.574
INFO 1 --- [nio-8080-exec-8] c.m.r.controller.BooksRatingsController
: [1, 2, 3, 4, 5, 6]
2019-09-18 11:19:06.686   INFO 1 --- [nio-8080-exec-9]
c.m.r.controller.BooksRatingsController : [1, 2, 3, 4, 5, 6]
2019-09-18 11:19:08.801   INFO 1 --- [io-8080-exec-10]
c.m.r.controller.BooksRatingsController : [1, 2, 3, 4, 5, 6]
2019-09-18 11:19:10.918   INFO 1 --- [nio-8080-exec-1]
c.m.r.controller.BooksRatingsController : [1, 2, 3, 4, 5, 6]
2019-09-18 11:19:13.065   INFO 1 --- [nio-8080-exec-2]
c.m.r.controller.BooksRatingsController : [1, 2, 3, 4, 5, 6]
2019-09-18 11:19:04.574   INFO 1 --- [nio-8080-exec-8]
c.m.r.controller.BooksRatingsController : [1, 2, 3, 4, 5, 6]
2019-09-18 11:19:06.686   INFO 1 --- [nio-8080-exec-9]
c.m.r.controller.BooksRatingsController : [1, 2, 3, 4, 5, 6]
```

Circuit Breaker

Очень важно, чтобы наши запросы гарантировано доходили до адресата. В istio реализован механизм Circuit Breaking. Прокси внутри кластера опрашивают сервисы и в случае поломки или медленного ответа выключают инстанс (под) сервиса из сети и направляют нагрузку на другие реплики сервиса.

Для сервиса books применим следующие правила:

```
apiVersion: networking.istio.io/v1alpha3 kind: DestinationRule
metadata:
name: books spec:
host: books trafficPolicy:
connectionPool:
tcp:
maxConnections: 1 http:
http1MaxPendingRequests: 1
maxRequestsPerConnection: 1 outlierDetection:
consecutiveErrors: 1 interval: 1s baseEjectionTime: 3m
maxEjectionPercent: 100
tls:
mode: ISTIO_MUTUAL
subsets:
   name: v1 labels:
version: v1
   name: v2 labels:
version: v2
```

Для сервиса books применим следующие правила:

- maxConnections – Максимальное количество подключений к сервису. Любое избыточное соединение будет в очереди.
- http1MaxPendingRequests – максимальное количество ожидающих запросов к сервису. Любые лишние ожидающие запросы будут отклонены.
- maxRequestsPerConnection – максимальное количество запросов в кластере.
- BaseEjectionTime – максимальная продолжительность извлечения для пода. Под будет извлечен на 20 секунд.
- ConsecutiveErrors – количество ошибок до того, как под будет удален из пула. Например, если у вас есть три последовательные ошибки при взаимодействии со службой, Istio помечает под как нездоровый.
- Interval – интервал времени для анализа выброса. Например, сервис проверяются каждые 10 секунд.
- MaxEjectionPercent – максимальный процент подов, которые могут быть извлечены из пула балансировки нагрузки. Например, установка этого поля в 100 подразумевает, что любые нездоровые поды, выдающие последовательные ошибки, могут быть извлечены, и запрос будет перенаправлен на исправные поды.

Заключение

С OpenShift Service Mesh вы можете лучше понять, как устроена ваша mesh-сеть, сделать ее более просматриваемой, что, в свою очередь, помогает поднять общий уровень сложности микросервисной архитектуры. Бонусом идет возможность реализовать больше функций и возможностей на уровне самой платформы OpenShift, а не кодировать их на уровне отдельных приложений, что облегчает жизнь разработчикам.

Еще один плюс – реализация вещей, которые раньше казались неподъемными, например, канареечное развертывание, A/B-тестирование и т.п.

Кроме того, вы получаете целостный подход к управлению микросервисными приложениями на всех своих кластерах OpenShift, что хорошо с точки зрения преемственности людей и непрерывности процессов. В конечном итоге это поможет перейти от монолитных приложений к распределенной микросервисной архитектуре и работать в большей степени на уровне конфигураций, чем кода.

Но если честно, то взяв отдельно взятую, защищенную наложенными средствами защиту, инфраструктуру какого-нибудь Банка: Истио является средством, которое потребует больший бюджет на реализацию (по нашим расчетом это +70% бюджета только на CPU). При этом нам не предлагается шифрование ГОСТ, как того требуют регуляторы, а избыточность дает лишнюю точку для отказа и при этом, если задуматься, то отказ сервис меша вызовет отказ работы всей сети, что нам уже удавалось увидеть в нескольких финансовых организациях. Получается, как в поговорке про мышей и кактус.

• • •

Ну вот мы и закончили цикл статей про Openshift, его безопасность, ролевую модель, уязвимости и средства их защиты. Данный цикл уже положил начало целому ряду статей про безопасность, в том числе внутри контейнеров, и мы обязательно продолжим освещать эту тематику. EOF

Ключевые слова: безопасность в openshift и kubernetes с использованием istio.