Cloudmaster - требования по ИБ

Рекомендуемые элементы конфигурации, связаны с реализацией функций информационной безопасности

Использование специализированного пользователя уровня операционной системы

В процессе установки Cloudmaster создаются и рекомендуются к использованию:

- пользователь ОС - cloudmaster-app
- группа пользователей ОС - cloudmaster-app

Ограничение прав доступа

Каталог с установленным Cloudmaster (/opt/cloudmaster) со всеми подкаталогами и файлами в них предоставить пользователю cloudmaster-app и группе cloudmaster-app

```
chown -R cloudmaster-app:cloudmaster-app /opt/cloudmaster
```

Как посмотреть список файлов, не принадлежащих пользователю cloudmaster-app и группе cloudmaster-app

```
find /opt/cloudmaster \( -not -user cloudmaster-app -o -not -group
cloudmaster-app -a -not -path '/opt/cloudmaster/www*' \) -exec stat -c '%U:%G
%n' {} \;
```

За исключением каталога /opt/cloudmaster/www - в котором расположены статичные файлы для SPA порталов. Этот каталог со всеми его подкаталогами и файлами необходимо предоставить группе nginx

```
chgrp -R nginx /opt/cloudmaster/www
```

Как посмотреть список файлов, не принадлежащих пользователю cloudmaster-app и группе nginx

```
find /opt/cloudmaster/www \( -not -user cloudmaster-app -o -not -group nginx
\) -exec stat -c '%U:%G %n' {} \;
```

Операции чтения конфигурационных и исполняемых файлов разрешить пользователю и группе.

А операцию изменения конфигурационных и исполняемых файлов разрешить только суперпользователю.

```
chmod 440 /opt/cloudmaster/services/auth/cm-idm.jar

chmod 440 /opt/cloudmaster/services/auth/application.properties

chmod 440 /opt/cloudmaster/services/broker/cm-broker.jar

chmod 440 /opt/cloudmaster/services/broker/application.properties

chmod 440 /opt/cloudmaster/nginx/*.conf

chmod 440  /opt/cloudmaster/temporal/temporal-server.yaml
```

Как посмотреть разрешения файлов

```
stat -c '%a %n' /opt/cloudmaster/services/auth/cm-idm.jar
/opt/cloudmaster/services/auth/application.properties
/opt/cloudmaster/services/broker/cm-broker.jar
/opt/cloudmaster/services/broker/application.properties
/opt/cloudmaster/nginx/*.conf /opt/cloudmaster/temporal/temporal-server.yaml
```

Ограничение входящего сетевого трафика

На уровне используемого файрволла ОС открыть только 443 и 22 TCP-порты для входящего HTTPS- и SSH-трафика

Как посмотреть список открытых портов

```
firewall-cmd --list-ports
```

Ограничение сетевой активности Temporal в рамках localhost

В конфигурационном файле /opt/cloudmaster/temporal/temporal-server.yaml установить секцию

```
worker:
    rpc:
      bindOnIP: '127.0.0.1'
      membershipPort: 6939
```

Как посмотреть секцию worker

```
grep -A4 'worker:' /opt/cloudmaster/temporal/temporal-server.yaml
```

Шифрование учётной записи базы данных

В конфигурационных файлах

- /opt/cloudmaster/services/auth/application.properties
- /opt/cloudmaster/services/broker/application.properties

учётная запись подключения к базе данных зашифрована и имеет формат

```
spring.datasource.username=ENC( {ШИФР} )
spring.datasource.password=ENC( {ШИФР} )
```

Как посмотреть логины и пароли подключения к БД

```
grep -E 'spring.datasource.username|spring.datasource.password'
/opt/cloudmaster/services/auth/application.properties
/opt/cloudmaster/services/broker/application.properties
```

Ограничение входящей HTTP-нагрузки

В конфигурационном файлах nginx */opt/cloudmaster/nginx/customer.conf* устанавливаем

```
limit_req zone=one burst=20;
```

В конфигурационном файлах nginx */opt/cloudmaster/nginx/00_common.conf* устанавливаем

```
limit_req_zone $binary_remote_addr zone=one:10m rate=10r/s;
```

Как посмотреть параметры ограничения входящей HTTP-нагрузки

```
grep 'limit_req' /opt/cloudmaster/nginx/*.conf
```

Ограничение используемых HTTP-методов

В конфигурационных файлах nginx */opt/cloudmaster/nginx/customer.conf и /opt/cloudmaster/nginx/customer.conf* для "**location**" устанавливаем ограничение

```
limit_except GET POST DELETE OPTIONS { deny all; }
```

Как посмотреть параметры ограничения используемых HTTP-методов

```
grep 'limit_except' /opt/cloudmaster/nginx/*.conf
```