s8.capital | Акционерное общество «С8 Капитал» | Волгоградский пр-т, д. 43, корп.3, Москва, 109316 | Тел.: +7 (495) 204-88-88 Факс: +7 (495) 204-88-87

Программное обеспечение «Двухфазная авторизация»

Руководство администратора

Оглавление

Акционерное общество
«С8 Капитал»
Волгоградский пр-т, д. 43, корп.3,
Москва, 109316
Тел.: +7 (495) 204-88-88
Факс: +7 (495) 204-88-87

Введение

Документ содержит описание возможностей и основных функциональных обязанностей администратора программного обеспечения «Двухфазная авторизация».

Термины, определения, сокращения

TFAUTH	Сервис двухфазной авторизации.
NGINX	Web-сервер.
GATE	Лотерейная система для учёта и процессинга транзакций.
AD - Active Directory	Служба каталогов компании.

1. TFAUTH

TFAUTH - приложение для двухфакторной аутентификации пользователя по реквизитам из ActiveDirectory и коду из SMS (или же из письма на email).

TFAUTH использует Web -интерфейс для получения реквизитов доступа пользователя и кода второго фактора аутентификации.

После успешной аутентификации у клиента сохраняется cookie с токеном, идентичный токен приложение сохраняет в файле в директории для хранения выпущенных токенов.

Обычно используется в связке в Web-сервером NGINX, который осуществляет проксирование на необходимый ресурс.

2. Механизм работы TFAUTH + NGINX

При получении запроса от пользователя nginx проверяет наличие cookie токена прохождения аутентификации, и, если токен существует, проверяет его наличие в списке токенов, выпущенных TFAUTH (TFAUTH и NGINX используют общую директорию для хранения файлов выпущенных токенов).

Если такой токен обнаружен и срок его действия не истёк, то аутентификация считается пройденной и NGINX проксирует запросы на целевой ресурс.

В остальных случаях (не найдена cookie с токеном; токен не обнаружен в списке выданных; срок действия токена истёк) NGINX осуществляет редирект на приложение TFAUTH для прохождения аутентификации и получения токена.

3. Конфигурация TFAUTH + NGINX

3.1. TFAUTH

Конфигурация TFAUTH осуществляется с помощью конфигурационного файла `tfauth.properties`, который необходимо разместить в каталоге ресурсов. Например, при запуске приложения в контейнере сервлетов jetty это будет `JETTY_BASE/resources`.

Пример конфигурационного файла:

tfauth.properties

```
spring.profiles.active = authLogSLF4J

# Блок настроек LDAP
ldap.domain = example.com
ldap.url = ldap://dc.example.com:389
ldap.group.admin = 2FA-ACCESS-GROUP
connection.time.out = 5

# Заголовок страницы аутентификации
app.title = Представьтесь, пожалуйста
```

```
# Максимальное время жизни токена аутентификации (в секундах)
app.token.max.age = 3600

# Возможность получения кода аутентификации на электронную почту
app.email.send.available = false

# Отключение второго фактора аутентификации
app.one.stage.auth = false

# Текст и отправитель сообщения
message.text = Код подтверждения пре-аутентификации: ${code}
message.originator = Stoloto

# Блок настроек отправки email
email.host = mail.example.com
email.port = 587
email.username = example
email.password = example
email.from = example@example.com
email.subject = Код подтверждения

# Блок настроек отправки СМС (предполагается использование fcgi из проекта sms)
gate.url = http://sms.example.com/smsurl
gate.login = gate_username
gate.password = gate_password
khd.sms.login = sms_username
khd.sms.password = sms_password

# Блок настроек директорий для хранения служебных данных, включая директорию для
хранения выпущенных токенов (слэш в конце пути обязателен)
directory.phone.sms = /tmp/smsdir/
directory.mail.message = /tmp/smsdir/
directory.token = /tmp/tokendir/
directory.csv.log = /tmp/

success.redirect.location = https://service.example.com
foreign.phone.check.enabled = false
```

Более подробную информацию о конфигурации TFAUTH можно получить в документации.

3.2. NGINX

Настройка NGINX осуществляется стандартно, например с помощью конфигурационного файла `tfauth.conf`, размещённого в `/etc/nginx/conf.d`.

Пример конфигурационного файла:

tfauth.conf

```
log_format custom '$remote_addr - $remote_user [$time_local] '
                                  '"$request" $status $body_bytes_sent '
                                  '"$http_referer" "$http_user_agent" '
                                  '"$http_x_forwarded_for" $request_id '
                                  '$flag $cookie__TOKEN';

server {
```

```
    server_name service.example.com;
    set $flag 0;
    # Директория для проверки наличия токена должна совпадать с директорией,
настроенной в приложении tfauth
    if (-f /tmp/tokendir/$cookie__TOKEN) {
        set $flag 1;
    }
    location / {
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        proxy_set_header Accept-Encoding "";
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        if ($flag = 1) {
            proxy_pass service.example.com;
        }
        # В данном случает предполагается, что tfauth и nginx развёрнуты на одном
узле и tfauth принимает соединения на порт 8080
        proxy_pass http://127.0.0.1:8080;
    }
    access_log /var/log/nginx/access.log custom;
}
```

3.3. Логирование в TFAUTH

Для настройки параметров логирования приложения TFAUTH необходимо в директории ресурсов разместить файл `logback.xml` с настройками логирования.

Пример конфигурационного файла, включающего вывод логов в STDOUT с уровнем логирования INFO:

logback.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <appender name="STDOUT" class="ch.qos.logback.core.ConsoleAppender">
        <encoder>
            <pattern>%d{HH:mm:ss.SSS} [%thread] %-5level %logger{36} -
%msg%n</pattern>
        </encoder>
    </appender>
    <logger name="ru.gamble" level="INFO"/>
    <root level="INFO">
        <appender-ref ref="STDOUT"/>
    </root>
</configuration>
```

4. Использование в Kubernetes

Для деплоя сервиса двухфакторной аутентификации в кластер Kubernetes разработан helm-чарт (репозиторий).

Общая конфигурация осуществляется через `values.yaml`. Например:

values.yaml

```
tfauth:
  env:
    # Отключение логов jetty
    - name: JAVA_OPTIONS
      value: "-Dorg.eclipse.jetty.LEVEL=OFF"
proxyTargets:
  - serverNames:
      - service.example.com
    # Куда проксировать при успешной проверке токена
    successTarget: https://service.example.com
    # Куда проксировать при неуспешной проверке токена
    failTarget: http://127.0.0.1:8080
# Настройки Ingress
ingress:
  hosts:
    - host: service.example.com
      paths:
        - path: /
          pathType: Prefix
  tls:
    - secretName: service-tls
      hosts:
        - service.example.com
```

Конфигурационные файлы приложения TFAUTH необходимо разместить внутри контейнера `app` по пути `/var/lib/jetty/resources` любым удобным способом (например, через инъекцию секретов hashicorp vault).

На текущий момент helm-чарт в пространстве имён `prod-atlassian` продуктового кластера Kubernetes.

Развёрнутое приложение используется для двухфакторной аутентификации для адресов jira.tccenter.ru и confluence.tccenter.ru при обращении с внешних адресов.

Тестовая версия приложения развёрнута в пространстве имён `stage-atlassian` stage-кластера Kubernetes и доступна по адресу https://stage-tfauth.stoloto.su/. Отправка SMS осуществляется через **tfi-fcgi-smsurl**, код доступа можно посмотреть в логах пода с fcgi.