# 1. Технические требования

Для установки системы требуется 3 сервера:

1. Сервер БД;
2. SFTP-сервер;
3. Сервер приложения.

Требования к серверам

| | Процессор | Оперативная память | Жесткий диск | Операционная система |
|---|---|---|---|---|
| Сервер базы данных | 4 ядра | 8 GB | 100 GB | Ubuntu 20.04 (или другая, совместимая с PostgreSQL) |
| Сервер приложения (back+front) | 4 ядра | 8 GB | 50 GB | Ubuntu 20.04 |
| SFTP-сервер | 2 ядра | 4 GB | 100 GB | Ubuntu 20.04 |

# 2. Инструкция по установке

## 2.1. Настройка БД

1. На сервер БД установите PostgreSQL 13 согласно официальной документации https://www.postgresql.org/download/linux/ubuntu/
2. Создайте пользователя с правами на создание базы данных

## 2.2. Настройка SFTP

1. Разверните SFTP (если планируется большой объём данных – на отдельном сервере; иначе можно развернуть на сервере приложения или на сервере базы данных)
2. Создайте нового пользователя и задайте ему пароль
3. Создайте директорию, в которой будут храниться файлы
4. Предоставьте на нее права на чтение, запись и выполнение (chmod 755) созданному пользователю

## 2.3. Установка приложения

1. Установите Docker согласно официальной документации (https://docs.docker.com/engine/install/ubuntu/)

2. Установите Docker Compose согласно официальной документации (https://docs.docker.com/compose/install/)

3. Скопируйте дистрибутив soc-incidents-portal в локальную директорию на сервере.

4. Создайте файл docker-compose.yml и задайте там необходимые параметры и порты в соответствии с инфраструктурой (пример ниже в разделе 3.2)

5. Импортируйте образы

```
# sudo docker image load -i <путь_к_архиву.tar>
```

6. Запустите контейнеры

```
# sudo docker-compose up -d –build
```

7. В директории /home/<user>/soc-incidents-portal/configs/ создайте файл appsettings.json, в котором укажите строку подключения к БД, параметры SFTP-подключения, почтового клиента и т.д. Описание и структура файла в разделе 3.1.

8. В директории /home/<user>/soc-incidents-portal/configs/ создайте файл nlog.config, в котором укажите параметры логирования. Пример файла в разделе 3.3.

9. В директории /home/<user>/soc-incidents-portal/configs/ создайте файл nginx.conf с конфигурацией веб-сервера nginx. Пример файла в разделе 3.4.

10. Перезапустите контейнеры

11. Портал будет доступен по адресу http://<адрес_сервера_приложения>:8080

# 3. Описание конфигурационных файлов

## 3.1. Конфигурационный файл портала appsettings.json

### *3.1.1. Структура конфигурационного файла*

| **Параметр** | **Описание** |
|---|---|
| AllowedHosts | Список разрешённых хостов. Строка, адреса перечисляются через запятую |
| ConnectionStrings | Настройки подключения к БД |
| CORS | Настройки CORS |
| EmailOptions | Настройки почтовых уведомлений |
| SmsOptions | Настройки подключения к SMS-шлюзу |
| Auth | Настройки авторизации |
| CaptchaOptions | Настройки CAPTCHA |
| RequestsLogging | Настройки логирования входящих запросов |
| IncidentsReportingOptions | Настройки ежедневных отчётов |
| SftpOptions | Настройки подключения к SFTP-серверу |
| TelegramNotificationsOptions | Настройки уведомлений в Telegram |
| IssueFilesOptions | Настройки валидации прикрепляемых файлов |
| IssueStagesOptions | Настройки мониторинга стадий обработки инцидента |

**Настройки подключения к БД**

| **Параметр** | **Описание** |
|---|---|
| SOCIncidents | Строка подключения к базе данных портала |

**Настройки CORS**

| Параметр | Описание |
|---|---|
| AllowAll | Общие разрешения |
| Origins | Разрешённые источники |
| Methods | Разрешённые методы |
| Headers | Разрешённые заголовки |

**Настройки почтовых уведомлений**

| Параметр | Описание |
|---|---|
| Host | Хост |
| PortSmtp | Порт для работы по протоколу SMTP |
| PortImap | Порт для работы по протоколу IMAP |
| AuthenticateLogin | Логин для авторизации на сервере |
| AuthenticatePassword | Пароль для авторизации на сервере |
| FormTitle | Имя отправителя, которое будет указано в письмах |
| FromEmail | Адрес, который будет использован для отправки писем |
| CheckCertificateRevocation | Признак, который определяет необходимость проверки серверного сертификата |
| EmailReceiveInterval | Интервал получения электронной почты |
| EnabledEmailReceive | Признак того, что включено получение электронной почты. |
| EnabledAnalystGroupMailing | Признак того, что включена рассылка уведомлений для группы аналитиков. |
| AnalystGroupEmail | Электронная почта группы аналитиков. |

**Настройки подключения к SMS-шлюзу**

| Параметр | Описание |
|---|---|
| SmsServerUrl | URL-адрес SMS-сервера |
| Login | Логин для аутентификации на сервере |
| Password | Пароль для аутентификации на сервере |

| Параметр | Описание |
|---|---|
| Subject | Отправитель сообщения |
| CheckCertificateRevocation | Признак, который определяет необходимость проверки серверного сертификата |

**Настройки авторизации**

| Параметр | Описание |
|---|---|
| JwtSecretKey | Ключ для шифрования jwt токена |
| TokenExpireTime | Время жизни токена |
| PasswordAllowedEnteredAttemptsCount | Допустимое количество попыток для ввода пароля |
| Enabled2fa | Признак того, что включена двухфакторная аутентификация |
| OtpExpireTime | Время жизни одноразового пароля |
| OtpAllowedEnteredAttemptsCount | Допустимое количество попыток для ввода одноразового пароля |
| AuthenticationRequestsCleanerInterval | Интервал срабатывания сервиса для чистки неактуальных запросов на аутентификацию |
| AuthHeader | Заголовок, который необходимо указывать для авторизации. |
| OtpLength | Длина одноразового пароля. Минимальное значение: 5. Максимальное значение: 20. |

**Настройки CAPTCHA**

| Параметр | Описание |
|---|---|
| ExpireTime | Время жизни CAPTCHA |
| CaptchaRequestsCleanerInterval | Интервал срабатывания сервиса для чистки неактуальных запросов на получение CAPTCHA |

**Настройки логирования входящих запросов**

| Параметр | Описание |
|---|---|
| Enabled | Признак того, что логирование запросов включено |

**Настройки ежедневных отчётов**

| Параметр | Описание |
|---|---|
| EnabledReportingService | Включён ли сервис рассылки отчётов |
| ReportingServiceInterval | Как часто срабатывает сервис |
| UploadReportsToSftpServer | Сохранять ли файлы с отчётами на SFTP |
| ReportsFolderOnSftpServer | Наименование директории на SFTP |

**Настройки подключения к SFTP-серверу**

| Параметр | Описание |
|---|---|
| Host | Адрес SFTP-сервера |
| Port | Порт |
| Username | Имя пользователя SFTP |
| Password | Пароль пользователя SFTP |

**Настройки уведомлений в Telegram**

| Параметр | Описание |
|---|---|
| EnabledNotifications | Включены ли уведомления |
| BotApiUrl | Адрес бота |

**Настройки валидации прикрепляемых файлов**

| Параметр | Описание |
|---|---|
| MaxFileSize | Максимальный размер файла в Мегабайтах |
| AllowedExtensions | Список допустимых расширений |
| ValidateFileByContent | Валидировать ли файлы по контенту или проверять просто расширение |
| FilesFolderOnSftpServer | Наименование директории на SFTP |

**Настройки мониторинга стадий обработки инцидента**

| Параметр | Описание |
|---|---|
| ExpiredStagesMonitoringEnabled | Признак того, что включен сервис для мониторинга стадий |
| AwaitingWorkTimeStagesMonitoringEnabled | Признак того, что включен сервис для мониторинга рабочего времени организаций и запуска/остановки стадий в соответствии с ним |

| Параметр | Описание |
| --- | --- |
| StagesMonitoringInterval | Интервал срабатывания сервиса для мониторинга стадии |
| ProcessingResponseStageExpire Time | Время на обработку стадии "Обработка ответа" |

### *3.1.2. Пример конфигурационного файла*

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Trace",
      "System": "Warning",
      "Microsoft": "Warning",
      "Hangfire": "Warning"
    }
  },
  "AllowedHosts": "*",
  "ConnectionStrings": {
    "SOCIncidents":
"Host=localhost;Port=5432;Database=SOCIncidents;Username=postgres;Password=***"
  },

  "CORS": {
    "AllowAll": {
      "Origins": true,
      "Headers": true,
      "Methods": true
    },
    "Origins": [
    ],
    "Headers": [
    ],
    "Methods": [
    ]
  },

  "EmailOptions": {
    "Host": "mail.ru",
    "PortSmtp": 587,
    "PortImap": 143,
    "FormTitle": "Портал SPACEVIEW",
    "FromEmail": "spaceview@mail.ru",
    "CheckCertificateRevocation": false,
    "AuthenticateLogin": "soc",
    "AuthenticatePassword": "***",
    "EnabledEmailReceive": true,
    "EmailReceiveInterval": "0:0:30",
    "PortalUrl": "https://0.0.0.0:8443",
    "AnalystGroupMailingLocale": "ru-RU",
    "EnabledAnalystGroupMailing": true,
    "AnalystGroupEmail": "all_soc@mail.ru",
    "EnabledEnabledEmailHandleFromClients": false,
    "EnabledEnabledEmailReceiveFromExternalSystem": true
  },
  "SmsOptions": {
    "SmsServerUrl": "https://... ",
```

```
    "Login": "***",
    "Password": "***",
    "Subject": "subject",
    "CheckCertificateRevocation": false
  },
  "Auth": {
    "JwtSecretKey": "******************",
    "TokenExpireTime": "0.3:0:0",
    "PasswordAllowedEnteredAttemptsCount": "5",
    "BruteForceLoginBlockingTime": "00:05:00",
    "Enabled2fa": false,
    "OtpLength": "5",
    "OtpExpireTime": "0:1:0",
    "OtpAllowedEnteredAttemptsCount": "3",
    "AuthenticationRequestsCleanerInterval": "1:0:0",
    "AuthHeader": "custom-auth-header"
  },
  "CaptchaOptions": {
    "ExpireTime": "0:2:0",
    "CaptchaRequestsCleanerInterval": "1:0:0"
  },
  "RequestsLogging": {
    "Enabled": true
  },
  "IpSafeList": "127.0.0.1;::1;172.*",
  "IncidentsReportingOptions": {
    "EnabledReportingService": true,
    "ReportingServiceInterval": "0:01:00",
    "UploadReportsToSftpServer": true,
    "ReportsFolderOnSftpServer": "reports"
  },
  "SftpOptions": {
    "Host": "0.0.0.0",
    "Port": 2222,
    "Username": "socSftpUser",
    "Password": "***"
  },
  "TelegramNotificationsOptions": {
    "EnabledNotifications": false,
    "BotApiUrl": "https://tgbot.azurewebsites.net/api/tdbot?chid=-***"
  },
    "IncidentsAutoClosingOptions": {
    "EnabledAutoClosing": true,
    "AutoClosingPeriod": "10.0:00:00",
    "AutoClosingServiceInterval": "0:1:00",
    "AutoClosingSolutionValue": "Информация не предоставлена."
  },
  "IssueFilesOptions": {
    "MaxFileSize": 50,
    "AllowedExtensions": [ "xls", "xlsx", "doc", "docx", "csv", "rar", "zip", "7z",
"txt", "log", "evtx" ],
    "ValidateFileByContent": true,
    "FilesFolderOnSftpServer": "SocAttachedFiles"
  },
  "IssueStagesOptions": {
    "ExpiredStagesMonitoringEnabled": true,
    "AwaitingWorkTimeStagesMonitoringEnabled": true,
    "StagesMonitoringInterval": "0:00:30",
    "ProcessingResponseStageExpireTime": "0:30:00"
  }
}
```

## 3.2. Конфигурационный файл портала docker-compose.yml

```
version: "3.5"

networks:
  soc-net:

services:
  soc-api:
    image: build-soc-incidents_soc-api
    restart: always
    networks:
      soc-net:
    volumes:
      - /home/user/soc-incidents-
portal/configs/appsettings.json:/app/appsettings.json
      - /home/user/soc-incidents-portal/configs/nlog.config:/app/nlog.config
      - /var/log/soc-incidents-portal:/app/Log
    environment:
      - http_proxy=
      - https_proxy=
    ports:
      - 80:80

  soc-web:
    image: build-soc-incidents_soc-web
    restart: always
    depends_on:
      - soc-api
    networks:
      soc-net:
    volumes:
      - /home/user/soc-incidents-portal/configs/nginx:/etc/nginx/conf.d
      - /home/user/soc-incidents-portal/configs/ssl:/etc/nginx/ssl
    ports:
      - 8443:443
      - 8080:80
```

## **3.3.** Конфигурационный файл портала nlog.config

```
<?xml version="1.0" encoding="utf-8" ?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:sl="http://www.nlog-project.org/schemas/NLog.Targets.Syslog.xsd"
      autoReload="true"
      internalLogLevel="trace"
```

```
      internalLogFile="Log/internal-nlog.log">

  <extensions>
    <add assembly="NLog.Targets.Syslog" />
  </extensions>

  <variable name="logFolder" value="${basedir}/Log" />

  <variable name="appName" value="SOC.Portal.WebApi" />

  <variable name="greylogServer" value="1.2.1.2" />
  <variable name="greylogPort" value="2514" />
  <variable name="syslogFacility" value="Local4" />

  <!-- the targets to write to -->
  <targets>
    <!-- write logs to file  -->
    <target xsi:type="File" name="allfile"
                    fileName="${logFolder}/nlog-all.log"
                    archiveFileName="${logFolder}/archives/nlog-all-{#}.log"
                    archiveEvery="Day"
                    archiveNumbering="Date"
                    archiveDateFormat="yyyy-MM-dd"
            maxArchiveFiles="7"
                    archiveOldFileOnStartup="true"
            layout="${longdate}
|${uppercase:${level}}
|${aspnet-traceidentifier}
|${callsite:className=true:includeNamespace=true:fileName=false:includeSourcePath=fals
e:methodName=true:cleanNamesOfAnonymousDelegates=true:cleanNamesOfAsyncContinuations=t
rue}
|${message} ${exception:format=ToString}" />

    <target xsi:type="Syslog" name="greyLog">
      <sl:layout xsi:type="SimpleLayout" text="@cee: { &quot;longdate&quot;:
&quot;${longdate}&quot;, &quot;level&quot;: &quot;${uppercase:${level}}&quot;,
&quot;traceidentifier&quot;: &quot;${aspnet-traceidentifier}&quot;,
&quot;callsite&quot;:
&quot;${callsite:className=true:includeNamespace=true:fileName=false:includeSourcePath
=false:methodName=true:cleanNamesOfAnonymousDelegates=true:cleanNamesOfAsyncContinuati
ons=true}&quot;, &quot;message&quot;: &quot;${message}&quot;, &quot;exception&quot;:
&quot;${exception:format=ToString}&quot;}" />
      <sl:messageSend>
        <sl:protocol>udp</sl:protocol>
        <sl:udp>
          <sl:server>${greylogServer}</sl:server>
          <sl:port>${greylogPort}</sl:port>
        </sl:udp>
      </sl:messageSend>
      <sl:messageCreation>
        <sl:facility>${syslogFacility}</sl:facility>
        <sl:rfc>Rfc5424</sl:rfc>
        <sl:rfc5424>
          <sl:hostname xsi:type="SimpleLayout" text="${machinename}" />
          <sl:appName xsi:type="SimpleLayout" text="${appName}" />
          <sl:procId xsi:type="SimpleLayout" text="${processid}" />
          <sl:msgId xsi:type="SimpleLayout" text="${threadid}" />
          <sl:disableBom>true</sl:disableBom>
        </sl:rfc5424>
      </sl:messageCreation>
    </target>
  </targets>
```

```
  <!-- rules to map from logger name to target -->
  <rules>
    <logger name="*" minlevel="Trace" writeTo="allfile" />
    <logger name="*" minlevel="Trace" writeTo="greyLog" />
  </rules>
</nlog>
```

## 3.4. Конфигурационный файл портала nginx.conf

```
user  nginx;
worker_processes  1;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;


events {
    worker_connections  1024;
}


http {
        client_max_body_size 51M;

    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request"
'
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';
    log_format full '$time_local [$status][$upstream_status] $remote_addr
$remote_user "$host"->$proxy_host->$upstream_addr "$request"
$body_bytes_sent [$request_time][$upstream_response_time] "$http_referer"
agent:"$http_user_agent" "$http_x_forwarded_for"';
    log_format graylog2_format '$remote_addr - $remote_user [$time_local]
"$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"
"$http_x_forwarded_for
"<msec=$msec|connection=$connection|connection_requests=$connection_request
s|millis=$request_time>';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    #gzip  on;

    underscores_in_headers on;

    include /etc/nginx/conf.d/*.conf;
}
```