Информационная система технико-экономических показателей теплоэлектростанций 2.0 (ИС ТЭП ТЭС 2.0)

ИНСТРУКЦИЯ АДМИНИСТРАТОРА (ДЛЯ УСТАНОВКИ ПО)

Санкт-Петербург
2023

Оглавление

Принятые термины и сокращения 2
1. Общие положения 2
2. Описание архитектуры системы “ИС ТЭП ТЭС 2.0” и взаимосвязи её компонентов 2
3. Установка и настройка системы 3
4. Диагностика неисправностей системы 7

Принятые термины и сокращения

Термин	Определение
ИС ТЭП ТЭС 2.0/ Система	Информационная система технико-экономических показателей теплоэлектростанций 2.0
ПО	Программное обеспечение
СУБД	Система управления базами данных

1. Общие положения

Настоящая Инструкция системного администратора разработана с целью:

- описания архитектуры системы и взаимосвязи её компонентов;
- описания процесса установки и настройки системы;
- определения порядка диагностирования проблем функционирования системы;
- упорядочения работы должностных лиц, связанной с диагностированием проблем функционирования системы.

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- установка и настройка системы;
- диагностирование проблем функционирования системы.

2. Описание архитектуры системы “ИС ТЭП ТЭС 2.0” и взаимосвязи её компонентов

“**ИС ТЭП ТЭС 2.0**” представляет собой программно-аппаратный комплекс, состоящий из сервера приложений, сервера базы данных и установленного на них ПО.

“**ИС ТЭП ТЭС 2.0**” включает в себя следующие серверы:

- Основной сервер приложения “ИС ТЭП ТЭС 2.0”
- Сервер баз данных;

На всех серверах операционной системой является РЕД ОС версии 7.2 Муром.

Сервер приложений (также установлен на всех серверах) Node.JS версии 16.18.

На сервере базы данных установлена СУБД Postgres Pro Standard 14.6.

3. Установка и настройка системы

3.1 Сервисы под управлением Node.JS
3.1.1 Установка и настройка Node.JS
Установка Node.JS на сервер приложения и на сервер базы данных

3.1.1.1 Проверить доступность модуля Node.JS соответствующей версии в репозитории и включить нужный поток в случае необходимости:
sudo dnf module list nodejs
sudo dnf module enable nodejs:16

3.1.1.2 Установить модуль Node.JS версии 16 из репозитория:
sudo dnf module install nodejs:16

3.1.1.3 Проверить установленную версию Node.JS и npm:
node -v
npm –v

3.1.1.4 Открыть необходимые порты для подключения к приложениям на firewall-e (в данном случае приложение на порту 20017/tcp):

- добавляем порт
  sudo firewall-cmd --permanent --zone=public --add-port= 20017/tcp
- перезапускаем firewall
  sudo firewall-cmd --reload
- проверяем включение правила
  sudo firewall-cmd --list-all

3.1.1.5 Создать и задать пароль пользователю webuser, от имени которого будут выполняться web-приложения:
useradd webuser
passwd webuser

3.1.1.6 В случае, если доступ сервера в интернет осуществляется через прокси-сервер, установить параметры доступа для npm через него:
npm config set https-proxy http://x.x.x.x:xxxx
npm config set proxy http:// x.x.x.x:xxxx

3.1.1.7 Установить менеджер процессов pm2
sudo npm install -g pm2

3.1.1.8 В случае, если доступ сервера в интернет осуществляется через прокси-сервер, установить параметры доступа для npm от имени пользователя webuser через него:
sudo su - webuser
npm config set https-proxy http://x.x.x.x:xxxx
npm config set proxy http:// x.x.x.x:xxxx

3.1.2 Запуск и мониторинг сервисов

Для поддержания непрерывной работы сервисов под управлением Node.JS создается файл ecosystem.config.js в каталоге проекта, например:

```
'use strict';
module.exports = {
  apps: [{
    name: 'tec',
    script: 'server/index.js',
    watch: true,
    exp_backoff_restart_delay: 100,
    env: {
      'TEC_PORT': 80,
      'TEC_SSL_PORT': 443,
      'NODE_ENV': 'tec-dev',
      'TEC_LOG_DIR': '/home/tec/logs/capcon',
      'TEC_FILE_ROOT': '/home/tec/data/files',
      'TEC_ESTIMATES_ROOT': '/home/tec/data/estimate',
      'TEC_SSL_CERTIFICATE': '/home/tec/ssl/aisks.pem',
      'TEC_PRIVATE_KEY': '/home/tec/ssl/aisks.key'
    },
    env_production: {
      'TEC_PORT': 80,
      'TEC_SSL_PORT': 443,
      'NODE_ENV': 'production',
      'TEC_LOG_DIR': '/home/webuser/logs/tec',
      'TEC_FILE_ROOT': '/home/webuser/data/files',
      'TEC_SSL_CERTIFICATE': '/home/webuser/ssl/aisks.pem',
      'TEC_PRIVATE_KEY': '/home/webuser/ssl/aisks.key'
    }
  }]
};
```

Для запуска и мониторинга приложений используется менеджер процессов pm2.

pm2 start ecosystem.config.js --only aisks --env production # создает приложение tec, используя переменные среды из окружения production на основе файла ecosystem.config.js

pm2 restart tec # перезапускает приложение tec

pm2 stop tec # останавливает приложение tec

pm2 logs 2 --lines 200 # отображает последние 200 строк лога приложения с id=2

3.2 Установка и настройка Postgres Pro
Установка СУБД Postgres Pro производится на сервере баз данных.
3.2.1 Проверить доступность модуля Postgres Pro соответствующей версии в репозитории и включить необходимый поток в случае необходимости:
sudo dnf module list Postgres Pro
sudo dnf module enable Postgres Pro:14

3.2.2 Установить Postgres Pro версии 14 из репозитория:
sudo dnf install Postgres Pro-server Postgres Pro-contrib

3.2.3 Открыть порт для подключения к Postgres Pro на firewall-е (по-умолчанию это порт 5432/tcp):

- добавляем порт
  sudo firewall-cmd --permanent --zone=public --add-port=5432/tcp
- перезапускаем firewall
  sudo firewall-cmd --reload
- Проверяем включение правила
  sudo firewall-cmd --list-all

3.2.4 Инициализировать базу данных
sudo Postgres Pro-setup initdb

3.2.5 Запустить и включить в автозапуск службу
sudo systemctl enable --now Postgres Pro

3.2.6 Проверить доступность и установленную версию СУБД:
sudo -u postgres psql -c "SELECT version();"

3.2.7 Задать пароль пользователю postgres, от имени которого запускается СУБД:
sudo passwd postgres

3.2.8 Задать пароль суперпользователю СУБД postgres:
sudo -u postgres psql
\password postgres
\q

3.2.9 Настроить парольную аутентификацию в файле конфигурации pg_hba.conf (расположение по-умолчанию $HOME/data/pg_hba.conf в каталоге пользователя postgres):

```
# "local" is for Unix domain socket connections only
local   all             all                                     md5
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# LAN connections
host    all             all             0.0.0.0/0               md5
```

В разделе LAN connections можно ограничить доступ только определенными сетями, указав соответствующую маску

3.2.10 Настроить следующие параметры в файле конфигурации Postgres Pro.conf (расположение по-умолчанию $HOME/data/Postgres Pro.conf в каталоге пользователя postgres):

#Включаем прослушивание на внешних интерфейсах системы
listen_addresses = ''*
#Устанавливаем количество соединений
max_connections = 100
#Включаем уровень записи в WAL, необходимый для восстанвления из резервной копии
wal_level = replica
#Включаем режим архивации
archive_mode = on
#Устанавливаем команду архивации, вместо /opt/Postgres Pro/wal_backup/ должен быть каталог, в котором будут размещаться резервные копии WAL
archive_command = 'test ! -f /opt/Postgres Pro/wal_backup/%f.gz && /usr/bin/gzip -c %p > /opt/Postgres Pro/wal_backup/%f.gz'
#Настраиваем полтику удержания WAL
wal_keep_segments = 60
#Параметры локализации
lc_messages = 'en_US.UTF-8'
lc_monetary = 'ru_RU.UTF-8'
lc_numeric = 'ru_RU.UTF-8'
lc_time = 'ru_RU.UTF-8'
#Параметры отображения даты
datestyle = 'iso, mdy'

3.2.11 Перезапустить сервис Postgres Pro для применения новых параметров:
sudo systemctl restart postgresql

3.2.12 Настройка резервного копирования
Создать скрипт резервного копирования. В данном примере каталог запуска Postgres Pro - /opt/postgresql, на сервере хранятся 2 последних базовых резервных копии (в каталоге db_backup) и WAL за последние 2-е суток (в каталоге wal_backup):

```
#!/bin/bash

PG_HOME=/opt/ postgresql
export PG_HOME
mkdir $PG_HOME/pg_backup
/usr/bin/pg_basebackup -U postgres -D $PG_HOME/pg_backup -Ft -z -Xf

INDEX=$(date +"%u")

test -e $PG_HOME/db_backup/base.${INDEX}.tar.gz && rm $PG_HOME/db_backup/base.${INDEX}.tar.gz
cp $PG_HOME/pg_backup/base.tar.gz $PG_HOME/db_backup/base.${INDEX}.tar.gz

test -e $PG_HOME/db_backup/base.last.tar.gz && rm $PG_HOME/db_backup/base.last.tar.gz
ln $PG_HOME/db_backup/base.${INDEX}.tar.gz $PG_HOME/db_backup/base.last.tar.gz

rm -r $PG_HOME/pg_backup
test -e $PG_HOME/db_backup/base.${INDEX}.tar.gz && test -e $PG_HOME/db_backup/base.$(date --date="-1 day" +"%u").tar.gz && find $PG_HOME/db_backup -type f -mtime +1 -exec rm {} \;
find $PG_HOME/wal_backup -type f -mtime +2 -exec rm {} \;
```

3.4 Обеспечение доступа к серверам “ИС ТЭП ТЭС 2.0” по протоколу HTTPS
3.4.1 Установка и обновление SSL-сертификатов для внутренних серверов “ИС ТЭП ТЭС 2.0”

Для генерации SSL-сертификата в удостоверяющий центр Заказчика направляется соответствующий CSR-запрос. Файл запроса с расширением .csr генерируется на соответствующем сервере (на который необходимо установить сертификат) при помощи следующей команды:

openssl req -out aisks.csr -newkey rsa:2048 -nodes -keyout aisks.key -config /path/to/san.conf

где /path/to/san.conf - путь до файла конфигурации san.conf со следующим содержимым:

```
[ req ]
default_bits      = 2048
distinguished_name = req_distinguished_name
req_extensions     = req_ext
[ req_distinguished_name ]
countryName                = Country Name (2 letter code)
stateOrProvinceName        = State or Province Name (full name)
localityName               = Locality Name (eg, city)
organizationName           = Organization Name (eg, company)
tecName                    = Tec Name (e.g. server FQDN or YOUR name)
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1   = tec.infoenergo.loc
DNS.2   = app-tec-17.infoenergo.loc
IP.1   = 10.3.78.4
```

Параметры *DNS.<n>*, *IP.<n>* указываются в соответствии с настройками сервера, для которого генерируется сертификат. В данном примере указаны настройки внутреннего сервера приложений “ИС ТЭП ТЭС 2.0” app-tec-17 (10.3.78.4).

В результате выполнения команды будут сформированы файлы закрытого ключа tec.key и файл запроса aisks.csr, который необходим для генерации SSL-сертификата. Сгенерированный файл сертификата необходимо разместить на соответствующем сервере “ИС ТЭП ТЭС 2.0”.

Файлы сертификатов и закрытых ключей располагаются в директориях /home/webuser/ssl основного сервера “ИС ТЭП ТЭС 2.0”

По истечении срока действия сертификатов, новые запросы могут быть сгенерированы той же командой. Они должны быть переданы сотрудникам информационной безопасности для генерации новых SSL-сертификатов в удостоверяющем центре Заказчика.

4. Диагностика неисправностей системы

4.1. Диагностика сервисов под управлением Node.JS

4.1.1. Для запуска монитора состояния сервисов под управлением Node.JS можно выполнить команду:

pm2 monit

4.1.2. Для просмотра логов выполняется команда:

pm2 logs <название или id сервиса> --lines <количество последних строк лога>

4.2. Диагностика состояния СУБД

Логи базы данных хранятся в течение 7 дней и располагаются в директории /opt/Postgresql/data/log на сервере БД.