SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Платформа Security Vision v.5

Руководство по установке

Версия: 1.1

Дата публикации: 12.05.2022

Содержание

1 Платформа

1.1 Установка и администрирование Платформы

Перед установкой подготавливаются серверы (физические или виртуальные) и установочные файлы ПО. Установка и последующая настройка компонентов Платформы выполняется в соответствии с требованиями и порядком, приведенными в настоящем документе. После установки проверяется работоспособность компонентов Платформы.

1.1.1 Установка на ОС Альт 8 СП

Мастер установки и сведения о лицензии (на бумажном носителе) поставляются Заказчику после приобретения Платформы.

Для установки компонентов Платформы на ОС семейства Linux используется тот же мастер установки, что и для установки на ОС семейства Windows. Для его запуска необходимы права администратора.

1.1.1.1 Установка и настройка дополнительных компонентов

Для подготовки ОС Альт 8 СП выполним следующие действия:

1 Войдем в систему под пользователем root, для чего введем в терминале:

```
su -
```

2 Обновим Альт Сервер 8 СП до актуальной версии:

a Выключим cdrom из списка доступных репозиториев:

```
apt-repo rm all cdroms
```

b Проверим, что cdrom отсутствует в списке:

```
apt-repo

Вывод команды

rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux CF/branch/x86_64 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux CF/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux CF/branch/noarch classic
```

c Обновим:

```
apt-get update
apt-get dist-upgrade
```

d После этого проверим:

```
rpm --eval %_priority_distbranch
```

Вывод команды

c9f2

```
apt-repo
```

Вывод команды

rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux CF2/branch/x86_64 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux CF2/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux CF2/branch/noarch classic

```
rpm -qa | grep apt-conf
```

Вывод команды

apt-conf-branch-9.0-alt5.c9f2.2.x86_64

e Снова обновим:

```
apt-get update
apt-get dist-upgrade
```

f Обновим ядро и введем команду для перезагрузки:

```
update-kernel
integalert fix
reboot
```

3 Введем команду для установки PostgreSQL:

```
apt-get install -y postgresql12 postgresq12-server
```

4 Введем команду для установки RabbitMQ:

```
apt-get install -y rabbitmq-server
```

5 Введем команды для установки пакета nginx-spnego (для последующей возможности настройки SSO):

```
apt-get install -y nginx nginx-spnego
ln -s /etc/nginx/modules-available.d/http_auth_spnego.conf /etc/nginx/modules-enabled.d/
```

6 Введем команду для установки Python:

```
apt-get install -y python3
```

7 Введем команду для установки Powershell:

```
apt-get install -y powershell
```

8 Введем команду для установки Node.js:

```
apt-get install -y nodejs
```

9 Введем команду для установки OpenJDK:

```
apt-get install -y java-11-openjdk
```

10 Распакуем архив с elasticsearch:

```
tar -xzf elasticsearch-7.0.0-linux-x86_64.tar.gz
```

11 Переместим распакованную папку в директорию opt/

```
cp -r elasticsearch-7.0.0 /opt/elasticsearch
```

12 Отредактируем конфигурационный файл elasticsearch

```
vim /opt/elasticsearch/config/elasticsearch.yml
```

a Уберем комментарии перед строками, указанными ниже, и заполним их следующим образом:

```
http.port: 9200
network.host: 127.0.0.1
cluster.name: localhost
```

13 Создадим пользователя и добавим ему права на elasticsearch:

```
useradd  -r elasticsearch
groupadd elasticsearch
chown -R elasticsearch:elasticsearch /opt/elasticsearch
```

14 Изменим параметры ядра (рекомендация с официального сайта ALT Linux):

```
echo "vm.max_map_count=262144" >> /etc/sysctl.conf
sysctl -w vm.max_map_count=262144
```

15 Создадим SystemD Unit-файл: /etc/systemd/system/elasticsearch.service

```
vim /etc/systemd/system/elasticsearch.service
```

a Заполним файл следующим образом:

```
[Unit]
Description=Elasticsearch Service
After=network.target

[Service]
WorkingDirectory=/opt/elasticsearch
ExecStart=/opt/elasticsearch/bin/elasticsearch
Restart=always
RestartSec=10
SyslogIdentifier=elasticsearch
User=elasticsearch
UMask=002
LimitNPROC=2048

[Install]
WantedBy=multi-user.target
```

16 Включим и запустим службу elasticsearch:

```
systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl start elasticsearch.service
```

17 Создадим системные базы данных postgresql:

```
/etc/init.d/postgresql initdb
```

18 Изменим шифрование в postgresql12:

```
echo "password_encryption = scram-sha-256" >> /var/lib/pgsql/data/postgresql.conf
```

19 Запустим postgresql:

```
systemctl start postgresql
systemctl enable postgresql
```

20 Войдем под пользователем postgres:

```
su - postgres -s /bin/bash
```

21 Войдем в postgresql12:

```
psql
```

22 Настроим пароль пользователю postgres:

```
alter user postgres password ‘1q2w#E$R’;
\q
```

23 Настроим доступ к базе данных:

```
echo "listen_addresses = 'localhost'" >> /var/lib/pgsql/data/postgresql.conf
```

24 Приведем файл **/var/lib/pgsql/data/pg_hba.conf** к виду:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             postgres                                scram-sha-256
local   all             all                                     peer
# IPv4 local connections:
host    all             postgres        0.0.0.0/0               scram-sha-256
host    all             all             127.0.0.1/32            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
                                                                85,1          Внизу
```

25 Перезапустим Postgresql:

```
systemctl restart postgresql
```

26 Запустим RabbitMQ:

```
systemctl start rabbitmq.service
systemctl enable rabbitmq.service
```

27 Проверим, что активны компоненты:

– Elasticsearch

```
systemctl status elasticsearch.service
```

– RabbitMQ

```
systemctl status rabbitmq.service
```

– PostgreSQL

```
systemctl status postgresql.service
```

1.1.1.2 Установка Платформы

Установка выполняется на ОС Альт 8 СП версии build 2021-12-21.

Для установки платформы Security Vision на ОС Альт 8 СП выполним следующие действия:

1 Создадим пользователя **sv** и группу **sv_users**, добавим пользователей **sv** и **nginx** в новую группу:

```
useradd -r sv   — создаем пользователя sv
passwd sv       — настраиваем пароль
groupadd sv_users     — создаем группу sv_users
gpasswd -a sv sv_users
gpasswd -a nginx sv_users
```

2 Перенесем папку с порталом, сервисами и конфигурационным файлом nginx.conf в каталог **/tmp**

3 Отредактируем файлы appsettings.json:

a В файлах appsettings.json, расположенных в папках внутри директорий **services** и **portal**, установим значение 127.0.0.1 в параметре Host в строке SecurityPortal;

b В файле appsettings.json, расположенном в папке **securityvision.api-5/**, установим значение 127.0.0.1 в строке PortalUrl. При этом не следует менять порт.

c В файле appsettings.json, расположенном в папке **securityvision.collector-5/**, установим значение 127.0.0.1 в строке PortalUrl в пункте ElasticsearchClientSettings. При этом не следует менять порт.

4 Отредактируем сервисы в папке serviceconfigs: укажем в поле User созданного пользователя sv (кроме securityvision.connectors.service, где пользователем будет root) и проверим путь до директории, в которой будет располагаться папка (по умолчанию путь: /usr/bin/).

5 Перенесем папку с порталом в каталог, указанный в securityvision.*.service (по умолчанию путь: /usr/bin/).

6 Перенесем содержимое папки serviceconfigs в каталог **/lib/systemd/system/**

7 Перейдем в папку **tools/securityvision.databaseupgradetool-5** в директории **securityvision** и отредактируем файл appsettings.json, в котором укажем значение 127.0.0.1 в параметре Host. Затем выполним команду:

```
SecurityVision.DatabaseUpgradeTool --linux
```

8 Выдадим права на папку пользователю **sv** и группе **sv_users**

```
chown -R sv:sv_users securityvision/
```

9 Изменим права для папки:

```
chmod -R 750 securityvision/
```

10 Создадим папку **/etc/nginx/certs/**

11 Выполним команды для создания сертификатов:

```
openssl genrsa -aes256 -out /etc/nginx/certs/server.key 2048
openssl req -new -key /etc/nginx/certs/server.key -out /etc/nginx/certs/server.csr
cp /etc/nginx/certs/server.key /etc/nginx/certs/server.key.sv
openssl rsa -in /etc/nginx/certs/server.key.sv -out /etc/nginx/certs/server.key
openssl x509 -req -days 365 -in /etc/nginx/certs/server.csr -signkey
/etc/nginx/certs/server.key -out /etc/nginx/certs/server.crt
```

12 Поместим файл конфигурации nginx.conf в каталог **/etc/nginx/sites-enabled.d**

13 Перезапустим NGINX:

```
systemctl restart nginx
```

14 Выполним start и enable всех сервисов Платформы:

```
systemctl enable securityvision.webapi.service
systemctl start securityvision.webapi.service
--------
```

15 Проверим, что все сервисы активны:

```
systemctl status securityvision.webapi.service
--------
```

1.1.2 Установка на ОС Альт Сервер 10

Мастер установки и сведения о лицензии (на бумажном носителе) поставляются Заказчику после приобретения Платформы.

Для установки компонентов Платформы на ОС семейства Linux используется тот же мастер установки, что и для установки на ОС семейства Windows. Для его запуска необходимы права администратора.

1.1.2.1 Установка и настройка дополнительных компонентов (2)

Для подготовки ОС Альт Сервер 10 выполним следующие действия:

1 Войдем в систему под пользователем root, для чего введем в терминале:

```
su -
```

2 Введите следующую команду:

```
apt-get update
```

3 Введем команду для установки PostgreSQL:

```
apt-get install -y postgresql14 postgresq14-server
```

4 Введем команду для установки RabbitMQ:

```
apt-get install -y rabbitmq-server
```

5 Введем команды для установки пакета nginx-spnego (для последующей возможности настройки SSO):

```
apt-get install -y nginx nginx-spnego
ln -s /etc/nginx/modules-available.d/http_auth_spnego.conf /etc/nginx/modules-enabled.d/
```

6 Введем команду для установки Python:

```
apt-get install -y python3
```

7 Введем команду для установки Powershell:

```
apt-get install -y powershell
```

8 Введем команду для установки Node.js:

```
apt-get install -y nodejs
```

9 Введем команду для установки OpenJDK:

```
apt-get install -y java-11-openjdk
```

10 Распакуем архив с elasticsearch:

```
tar -xzf elasticsearch-7.0.0-linux-x86_64.tar.gz
```

11 Переместим распакованную папку в директорию opt/

```
cp -r elasticsearch-7.0.0 /opt/elasticsearch
```

12 Отредактируем конфигурационный файл elasticsearch

```
vim /opt/elasticsearch/config/elasticsearch.yml
```

a Уберем комментарии перед строками, указанными ниже, и заполним их следующим образом:

```
http.port: 9200
network.host: 127.0.0.1
cluster.name: localhost
```

13 Создадим пользователя и добавим ему права на elasticsearch:

```
useradd  -r elasticsearch
groupadd elasticsearch
chown -R elasticsearch:elasticsearch /opt/elasticsearch
```

14 Изменим параметры ядра (рекомендация с официального сайта ALT Linux):

```
echo "vm.max_map_count=262144" >> /etc/sysctl.conf
sysctl -w vm.max_map_count=262144
```

15 Создадим SystemD Unit-файл: /etc/systemd/system/elasticsearch.service

```
vim /etc/systemd/system/elasticsearch.service
```

a Заполним файл следующим образом:

```
[Unit]
Description=Elasticsearch Service
After=network.target

[Service]
WorkingDirectory=/opt/elasticsearch
ExecStart=/opt/elasticsearch/bin/elasticsearch
Restart=always
RestartSec=10
SyslogIdentifier=elasticsearch
User=elasticsearch
UMask=002
LimitNPROC=2048
```

```
[Install]
WantedBy=multi-user.target
```

16 Включим и запустим службу elasticsearch:

```
systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl start elasticsearch.service
```

17 Создадим системные базы данных postgresql:

```
/etc/init.d/postgresql initdb
```

18 Запустим postgresql:

```
systemctl start postgresql
systemctl enable postgresql
```

19 Настроим пароль для пользователя postgres:

```
psql -U postgres
alter user postgres password ‘1q2w#E$R’;
\q
```

20 Настроим доступ к базе данных:

```
echo "listen_addresses = 'localhost'" >> /var/lib/pgsql/data/postgresql.conf
```

21 Приведем файл **/var/lib/pgsql/data/pg_hba.conf** к виду:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             postgres                                scram-sha-256
local   all             all                                     peer
# IPv4 local connections:
host    all             postgres        0.0.0.0/0               scram-sha-256
host    all             all             127.0.0.1/32            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
                                                                        85,1          Внизу
```

22 Перезапустим Postgresql:

```
service postgresql restart
```

23 Запустим RabbitMQ:

```
systemctl start rabbitmq.service
systemctl enable rabbitmq.service
```

24 Проверим, что активны компоненты:

- Elasticsearch

```
systemctl status elasticsearch.service
```

- RabbitMQ

```
systemctl status rabbitmq.service
```

- PostgreSQL

```
systemctl status postgresql.service
```

1.1.2.2 Установка Платформы

Установка выполняется на ОС Альт Сервер 10 версии, актуальной на дату 05.22.

Для установки платформы Security Vision на ОС Альт Сервер 10 выполним следующие действия:

1 Создадим пользователя **sv** и группу **sv_users**, добавим пользователей **sv** и **nginx** в новую группу:

```
useradd -r sv   — создаем пользователя sv
passwd sv      — настраиваем пароль
groupadd sv_users     — создаем группу sv_users
gpasswd -a sv sv_users
gpasswd -a nginx sv_users
```

2 Перенесем папку с порталом, сервисами и конфигурационным файлом nginx.conf в каталог **/tmp**

3 Отредактируем файлы appsettings.json:

a В файлах appsettings.json, расположенных в папках внутри директории **services**, установим значение 127.0.0.1 в параметре Host в строке SecurityPortal;

b В файле appsettings.json, расположенном в папке **securityvision.api-5/**, установим значение 127.0.0.1 в строке PortalUrl. При этом не следует менять порт.

c В файле appsettings.json, расположенном в папке **securityvision.collector-5/**, установим значение 127.0.0.1 в строке PortalUrl в пункте ElasticsearchClientSettings. При этом не следует менять порт.

4 Отредактируем сервисы в папке serviceconfigs: укажем в поле User созданного пользователя sv (кроме securityvision.connectors.service, где пользователем будет root) и проверим путь до директории, в которой будет располагаться папка (по умолчанию путь: /usr/bin/).

5 Перенесем папку с порталом в каталог, указанный в securityvision.*.service (по умолчанию путь: /usr/bin/).

6 Перенесем содержимое папки serviceconfigs в каталог **/lib/systemd/system/**

7 Перейдем в папку **tools/securityvision.databaseupgradetool-5** в директории **securityvision** и отредактируем файл appsettings.json, в котором укажем значение 127.0.0.1 в параметре Host. Затем выполним команду:

```
SecurityVision.DatabaseUpgradeTool --linux
```

8 Выдадим права на папку пользователю **sv** и группе **sv_users**

```
chown -R sv:sv_users securityvision/
```

9 Изменим права для папки:

```
chmod -R 750 securityvision/
```

10 Создадим папку **/etc/nginx/certs/**

11 Выполним команды для создания сертификатов:

```
openssl genrsa -aes256 -out /etc/nginx/certs/server.key 2048
openssl req -new -key /etc/nginx/certs/server.key -out /etc/nginx/certs/server.csr
cp /etc/nginx/certs/server.key /etc/nginx/certs/server.key.sv
openssl rsa -in /etc/nginx/certs/server.key.sv -out /etc/nginx/certs/server.key
openssl x509 -req -days 365 -in /etc/nginx/certs/server.csr -signkey
/etc/nginx/certs/server.key -out /etc/nginx/certs/server.crt
```

12 Поместим файл конфигурации nginx.conf в каталог **/etc/nginx/sites-enabled.d**

13 Перезапустим NGINX:

```
systemctl restart nginx
```

14 Выполним start и enable всех сервисов Платформы:

```
systemctl enable securityvision.webapi.service
systemctl start securityvision.webapi.service
--------
```

15 Проверим, что все сервисы активны:

```
systemctl status securityvision.webapi.service
--------
```