

# Инструкция по развёртыванию Security Capsule SIEM

## 1. Дистрибутивы и docker-контейнеры.

Установка производилась на образе ОС Альт Сервер 10

```
[root@alt-server-10 ~]# uname -a
Linux alt-server-10 5.10.82-std-def-alt1 #1 SMP Fri Dec 3 14:49:25 UTC 2021 x86_64
GNU/Linux
```

Дистрибутивы: SecurityCapsuleSIEMCorrelator-2.0.2-4alt10.x86\_64.rpm,  
SecurityCapsuleSIEMCollector-2.0.0-4alt10.x86\_64.rpm

Docker-контейнеры: siemwebapplicationcert.tar.gz, postgres.tar.gz

## 2. Установка

2.1. Обновим индекс пакетов:

```
[root@alt-server-10 ~]# apt-get update
```

2.2. Установим пакеты sudo, openssh-server:

```
[root@alt-server-10 ~]# apt-get install openssh-server sudo
```

2.3. Добавим пользователя sa в группу wheel:

```
[root@alt-server-10 ~]# usermod -aG wheel sa
```

2.4. Раскомментируем строку «#WHEEL\_USERS ALL=(ALL) NOPASSWD: ALL», отредактировав файл sudoers редактором visudo.

```
[root@alt-server-10 ~]# visudo
```

2.5. Установим DOCKER:

```
[root@alt-server-10 ~]# apt-get install docker-engine docker-compose
```

2.6. Включим автозагрузку сервиса mongod.service и запустим его:

```
[root@alt-server-10 ~]# systemctl enable docker.service
[root@alt-server-10 ~]# systemctl start docker.service
```

2.7. Разархивируем контейнер postgres.tar.gz:

```
[root@alt-server-10 ~]# tar fx postgres.tar.gz
[root@alt-server-10 ~]# cd postgres/
```

2.8. Зададим пароль пользователя postgres, отредактировав значение переменной «POSTGRES\_PASSWORD=» в файле «.env».

```
[root@alt-server-10 postgres]# vim .env
```

2.9. Развернём контейнер postgres:

```
[root@alt-server-10 postgres]# bash run.sh
```

2.10. Разархивируем контейнер siemwebapplicationcert.tar.gz:

```
[root@alt-server-10 ~]# tar fx siemwebapplicationcert.tar.gz
[root@alt-server-10 ~]# cd siemwebapplicationcert/
```

2.11. Подключим токен Guardant к usb порту, чтобы определить адрес порта:

```
[root@alt-server-10 siemwebapplicationcert]# lsusb
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 004: ID 0a89:0009 Aktiv Guardant Code
Bus 001 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 001 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

2.12. Значения Bus и Device, **001** и **004** соответственно, подставим в переменную «**GUARDANT\_USB=**» в файле «.env». Пример, **GUARDANT\_USB=/dev/bus/usb/001/004**

В значение переменной «**DOCKER\_HOST\_IP=**» укажем IP адрес Альт сервера.

Также может быть изменён номер порта в переменной «**SIEMWEBAPP\_PORT=**»

```
[root@alt-server-10 siemwebapplicationcert]# vim .env
```

В файле **siem/appsettings.json** отредактируем значение переменной «**Password=**», прописав туда пароль, который задавали на этапе развёртывания контейнера postgres.

2.13. Развернём контейнер siemwebapplicationcert:

```
[root@alt-server-10 siemwebapplicationcert]# bash run.sh
```

2.14. Проверим список запущенных контейнеров:

```
[root@alt-server-10 ~]# docker ps
```

```
[root@alt-server-10 ~]# docker ps
CONTAINER ID   IMAGE                                COMMAND                                CREATED        STATUS        PORTS
db339ef92f76   siemwebapplicationcert:latest       "dotnet SIEMWebAppli..."           40 seconds ago Up 39 seconds 443/tcp, 0.0
0.0:8000->80/tcp, :::8000->80/tcp   siemwebappcert-srv
ad580513ee4b   postgres:11-alpine                  "docker-entrypoint.s..."           14 minutes ago Up 14 minutes  5432/tcp
postgres-srv
```

2.15. Установим базу MongoDB:

```
[root@alt-server-10 ~]# apt-get install mongo mongo-server mongo-tools
```

2.16. Включим автозагрузку сервиса mongod.service и запустим его:

```
[root@alt-server-10 ~]# systemctl enable mongod.service
[root@alt-server-10 ~]# systemctl start mongod.service
```

2.17. Создадим пользователей MongoDB - userdb и root:

```
[root@alt-server-10 ~]# mongo admin --eval "db.createUser({ user:'userdb',
pwd:'cde34rfv1ieWS', roles: [{ role:'readWriteAnyDatabase', db:'admin'}]})"

[root@alt-server-10 ~]# mongo admin --eval "db.createUser({ user:'root',
pwd:'cde34rfv1ieWS', roles: [{ role:'root', db:'admin'}]})"
```

2.18. В конфигурационном файле /etc/mongo/mongod.conf раскомментируем строку «#auth = true» и присвоим переменной **bind\_ip** следующие значения «**bind\_ip = 127.0.0.1, 172.16.238.1**».

2.19. Выполним перезапуск сервиса mongod.service:

```
[root@alt-server-10 ~]# systemctl restart mongod.service
```

2.20. Выполним установку дистрибутивов коррелятора и сборщика

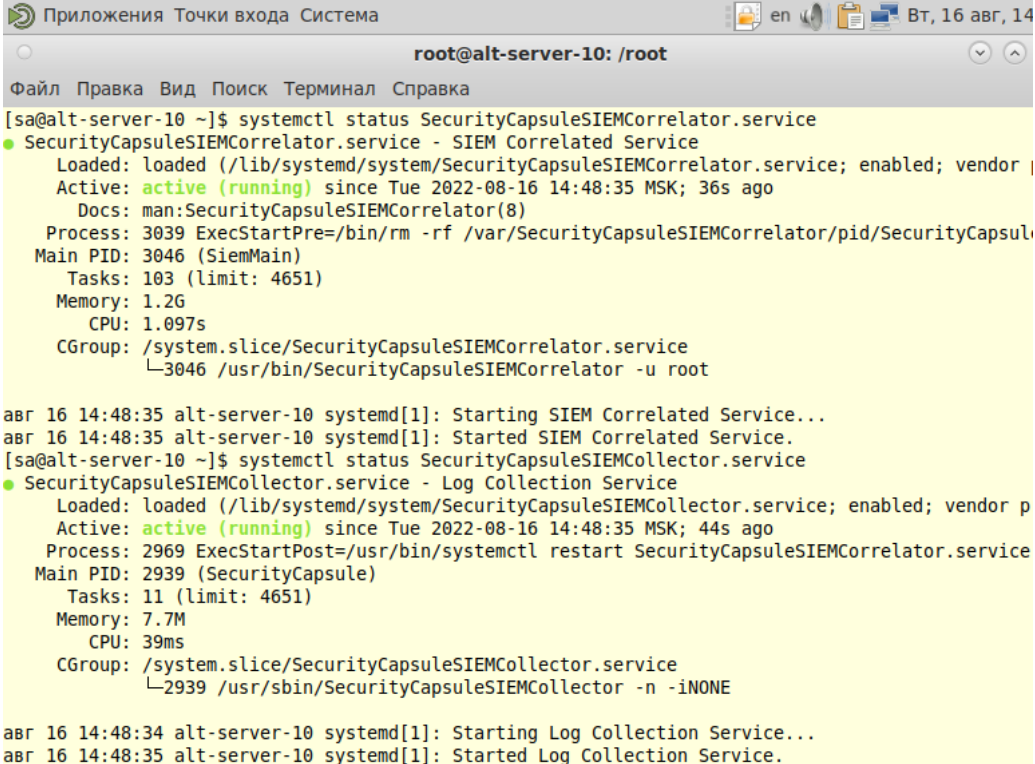
```
[root@alt-server-10 ~]# apt-get install ./SecurityCapsuleSIEMCorrelator-2.0.2-
4alt10.x86_64.rpm

[root@alt-server-10 ~]# apt-get install ./SecurityCapsuleSIEMCollector-2.0.0-
4alt10.x86_64.rpm
```

### 3. Проверка.

3.1. Проверим запуск служб коррелятора и сборщика:

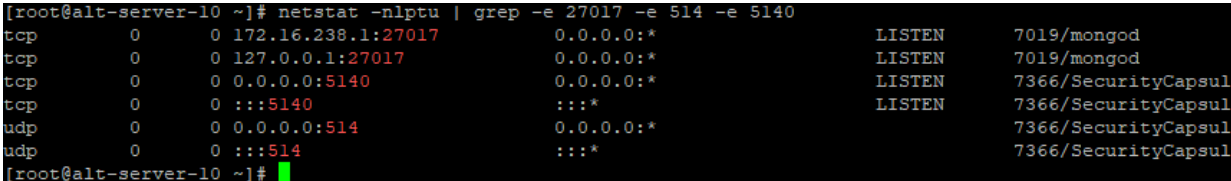
```
[root@alt-server-10 ~]# systemctl status SecurityCapsuleSIEMCollector.service  
[root@alt-server-10 ~]# systemctl status SecurityCapsuleSIEMCorrelator.service
```



```
Приложения Точки входа Система en Вт, 16 авг, 14  
root@alt-server-10: /root  
Файл Правка Вид Поиск Терминал Справка  
[sa@alt-server-10 ~]$ systemctl status SecurityCapsuleSIEMCorrelator.service  
● SecurityCapsuleSIEMCorrelator.service - SIEM Correlated Service  
   Loaded: loaded (/lib/systemd/system/SecurityCapsuleSIEMCorrelator.service; enabled; vendor p  
   Active: active (running) since Tue 2022-08-16 14:48:35 MSK; 36s ago  
     Docs: man:SecurityCapsuleSIEMCorrelator(8)  
   Process: 3039 ExecStartPre=/bin/rm -rf /var/SecurityCapsuleSIEMCorrelator/pid/SecurityCapsul  
   Main PID: 3046 (SiemMain)  
     Tasks: 103 (limit: 4651)  
    Memory: 1.2G  
       CPU: 1.097s  
   CGroup: /system.slice/SecurityCapsuleSIEMCorrelator.service  
           └─3046 /usr/bin/SecurityCapsuleSIEMCorrelator -u root  
  
авг 16 14:48:35 alt-server-10 systemd[1]: Starting SIEM Correlated Service...  
авг 16 14:48:35 alt-server-10 systemd[1]: Started SIEM Correlated Service.  
[sa@alt-server-10 ~]$ systemctl status SecurityCapsuleSIEMCollector.service  
● SecurityCapsuleSIEMCollector.service - Log Collection Service  
   Loaded: loaded (/lib/systemd/system/SecurityCapsuleSIEMCollector.service; enabled; vendor p  
   Active: active (running) since Tue 2022-08-16 14:48:35 MSK; 44s ago  
   Process: 2969 ExecStartPost=/usr/bin/systemctl restart SecurityCapsuleSIEMCorrelator.service  
   Main PID: 2939 (SecurityCapsule)  
     Tasks: 11 (limit: 4651)  
    Memory: 7.7M  
       CPU: 39ms  
   CGroup: /system.slice/SecurityCapsuleSIEMCollector.service  
           └─2939 /usr/sbin/SecurityCapsuleSIEMCollector -n -iNONE  
  
авг 16 14:48:34 alt-server-10 systemd[1]: Starting Log Collection Service...  
авг 16 14:48:35 alt-server-10 systemd[1]: Started Log Collection Service.
```

3.2. Проверим, что слушаются порты 8000/tcp, 27017/tcp, 5140/tcp, 514/udp

```
[root@alt-server-10 ~]# netstat -nlptu | grep -e 27017 -e 514 -e 5140
```



```
[root@alt-server-10 ~]# netstat -nlptu | grep -e 27017 -e 514 -e 5140  
tcp        0      0 172.16.238.1:27017  0.0.0.0:*           LISTEN      7019/mongod  
tcp        0      0 127.0.0.1:27017    0.0.0.0:*           LISTEN      7019/mongod  
tcp        0      0 0.0.0.0:5140      0.0.0.0:*           LISTEN      7366/SecurityCapsul  
tcp        0      0 :::5140           :::*                 LISTEN      7366/SecurityCapsul  
udp        0      0 0.0.0.0:514      0.0.0.0:*           7366/SecurityCapsul  
udp        0      0 :::514           :::*                 7366/SecurityCapsul  
[root@alt-server-10 ~]#
```

### 3.3. Проверим подключение к web-консоли через браузер:

