

Руководство по установке

Avanpost CA



ОГЛАВЛЕНИЕ

АННОТАЦИЯ	3
ТЕРМИНЫ И СОКРАЩЕНИЯ	4
ОБЩИЕ СВЕДЕНИЯ	6
УСТАНОВКА ИЗ ДИСТРИБУТИВА	7
Установка и настройка PostgreSQL	7
Установка и настройка Avapost CA.....	8
Установка и настройка Nginx Reverse Proxy	10
БЫСТРЫЙ СТАРТ В DOCKER	12
КОНТАКТЫ	14
СПИСОК РИСУНКОВ	15
СПИСОК ТАБЛИЦ	16

АННОТАЦИЯ

Avanpost CA — это центр сертификации, обеспечивающий полный набор функций для управления цифровыми сертификатами в соответствии со принципами PKI и стандартом X.509.

Настоящий документ содержит пошаговое руководство по установке системы Avanpost CA.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Таблица 1 – Термины

Термин	Определение
ACL (Access Control List)	Список управления доступом. Набор правил, определяющий, какие пользователи или системы имеют права на выполнение определенных операций с объектом (например, с шаблоном сертификата). Права могут включать: чтение (read), запрос (request), изменение (write), утверждение (approve), удаление (delete)
Avanpost CA (Avanpost Certification Authority)	Центр сертификации, разработанный компанией Avanpost
CA (Certification Authority)	Центр сертификации. Удостоверяющий центр, который выпускает, подписывает и отзывает сертификаты, являясь доверенной третьей стороной
CRL (Certificate Revocation List)	Список отозванных сертификатов. Список, содержащий серийные номера сертификатов, отозванных до истечения срока их действия. Используется для проверки валидности сертификата
Key usage	Основные операции, для которых может использоваться ключ, указанный в сертификате, например, DigitalSignature, KeyEncipherment, CertSign

OCSP (Online Certificate Status Protocol)	Протокол онлайн-проверки статуса сертификата
Nginx	Веб-сервер и обратный прокси-сервер
SCEP (Simple Certificate Enrollment Protocol)	Простой протокол регистрации сертификатов
Systemd	Система инициализации и управления службами в Linux
База данных (БД)	Совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных

ОБЩИЕ СВЕДЕНИЯ

Поддерживаемые операционные системы

Для установки и работы Avanpost CA поддерживаются следующие операционные системы:

- Astra Linux SE 1.7+ (ядро 6.1+)
- Альт Сервер 10+
- RedOS 8+
- CentOS Stream 8+
- RHEL 8+
- Ubuntu 22.04+

Системы управления базами данных

Для хранения данных Avanpost CA поддерживает следующие СУБД:

- PostgreSQL 15+
- Postgres Pro
- Tantor
- Другие PostgreSQL-подобные СУБД

Веб-сервер

Для публикации веб-интерфейса системы рекомендуется использовать:

- Nginx

УСТАНОВКА ИЗ ДИСТРИБУТИВА

УСТАНОВКА И НАСТРОЙКА PostgreSQL

Установка выполняется на примере РЕД ОС 8.

1. Установите пакет PostgreSQL необходимой версии (пример установки 15 версии):

```
sudo dnf install postgresql15-server
```

2. Инициализируйте базу данных:

```
sudo postgresql-15-setup initdb
```

3. Добавьте сервис в автозагрузку и запустите:

```
sudo systemctl enable postgresql-15.service --now
```

```
sudo systemctl status postgresql-15.service
```

4. Настройте доступ к базе данных:

```
echo "host all all 127.0.0.1/0 md5" | sudo tee -a /var/lib/pgsql/15/data/pg_hba.conf
```

5. Включите прослушивание всех адресов:

```
sudo sed -i "s/#listen_addresses = 'localhost'/listen_addresses = '*'/"  
/var/lib/pgsql/15/data/postgresql.conf | grep listen_addresses
```

6. Зайдите под пользователем в psql:

```
sudo -u postgres psql
```

7. Добавьте пароль для пользователя postgres:

```
postgres=# ALTER USER postgres WITH ENCRYPTED PASSWORD 'P@ssw0rd';  
# ALTER ROLE  
\q
```

8. Перезагрузите сервис:

```
sudo systemctl restart postgresql-15.service
```

УСТАНОВКА И НАСТРОЙКА AVANPOST CA

1. Создайте системного пользователя:

```
sudo useradd avanpost -m -d /opt/avanpost
```

2. Задайте пароль:

```
sudo passwd avanpost
```

3. Переключитесь на пользователя avanpost и разархивируйте дистрибутив:

```
su - avanpost  
sudo unzip Avanpost.CA.v0.1+b30d0c8.zip -d /opt/avanpost/
```

4. Создайте каталог для конфигурационных файлов:

```
mkdir /opt/avanpost/ca/config
```

5. Создайте файл с переменными окружения:

```
nano /opt/avanpost/ca/config/env
```

Добавьте в файл следующее:

```
POSTGRES_USER=postgres  
POSTGRES_PASSWORD=P@ssw0rd  
POSTGRES_DB=postgres  
POSTGRES_HOSTNAME=127.0.0.1  
CA_DATABASE_URL=postgres://$POSTGRES_USER:$POSTGRES_PASSWORD@$POSTGRES_HOST  
NAME:5432/postgres?sslmode=disable
```

6. Добавьте переменные окружения в файл .bashrc пользователя avanpost:

```
nano /opt/avanpost/.bashrc
```

Добавьте следующее:

```
export POSTGRES_USER=postgres
export POSTGRES_PASSWORD=P@ssw0rd
export POSTGRES_DB=postgres
export POSTGRES_HOSTNAME=127.0.0.1
export
CA_DATABASE_URL=postgres://postgres:P@ssw0rd@127.0.0.1:5432/postgres?sslmode=disabl
e
export CA_KEY_PATH=/opt/avanpost/tools/migratetool/ca-key.pem
```

7. Примените изменения и проверьте работоспособность:

```
source /opt/avanpost/.bashrc
echo $CA_KEY_PATH
```

8. Создайте systemd-сервис:

```
sudo vi /etc/systemd/system/ca.service
```

Добавьте следующее:

```
[Unit]
Description=Avanpost CA

[Service]
WorkingDirectory=/opt/avanpost/ca
ExecStart=bash -c 'cd /opt/avanpost/ca/tools/migratetool && ./migratetool && cd
/opt/avanpost/ca/ca && ./ca'
Restart=always
RestartSec=10
User=avanpost
EnvironmentFile=/opt/avanpost/ca/config/env
SyslogIdentifier=ca

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

9. Перезагрузите systemd, включите автозагрузку и запустите сервис:

```
sudo systemctl daemon-reload
```

```
sudo systemctl enable --now ca.service
```

УСТАНОВКА И НАСТРОЙКА NGINX REVERSE PROXY

1. Установите пакет Nginx:

```
sudo dnf install nginx
```

2. Создайте файл конфигурации:

```
sudo nano /etc/nginx/conf.d/avanpost-ca.conf
```

Добавьте следующее:

```
server {  
    listen    80;  
    server_name ca01.avanpost.local;  
  
    location /api/ {  
        proxy_pass      http://127.0.0.1:9999/api/;  
        proxy_http_version 1.1;  
        proxy_redirect  off;  
        proxy_set_header X-Real-IP    $remote_addr;  
        proxy_set_header Host        $host;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
    }  
  
    location /swagger/ {  
        proxy_pass      http://127.0.0.1:9999/swagger/;  
    }  
  
    location /scep/ {  
        proxy_pass      http://127.0.0.1:9999/scep/;  
    }  
  
    location /ocsp/ {  
        proxy_pass      http://127.0.0.1:9999/ocsp/;  
    }  
}
```

```
}  
  
location / {  
    proxy_pass      http://127.0.0.1:8080;  
    proxy_http_version 1.1;  
    proxy_redirect  off;  
    proxy_set_header X-Real-IP      $remote_addr;  
    proxy_set_header Host          $host;  
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
}  
}
```

3. Отключение SELinux:

```
sudo sed -i 's/SELINUX=enforcing/SELINUX=permissive/' /etc/selinux/config
```

4. Перезагрузите систему:

```
sudo init 6
```

БЫСТРЫЙ СТАРТ В DOCKER

Avanpost CA может быть развернут в виде набора Docker-контейнеров в среде контейнерной виртуализации. Данный развёртывания является простым и быстрым, что позволяет применять его в рамках демонстрации, тестирования и пилотных проектов.

Для работы этого способа на целевом сервере должен быть установлен Docker и Docker Compose

1. Разместите файл-архив (Avanpost.CA.v*.zip) с продуктом на сервере. Разархивируйте и перейдите в созданный каталог. Структура внутри будет выглядеть следующим образом:

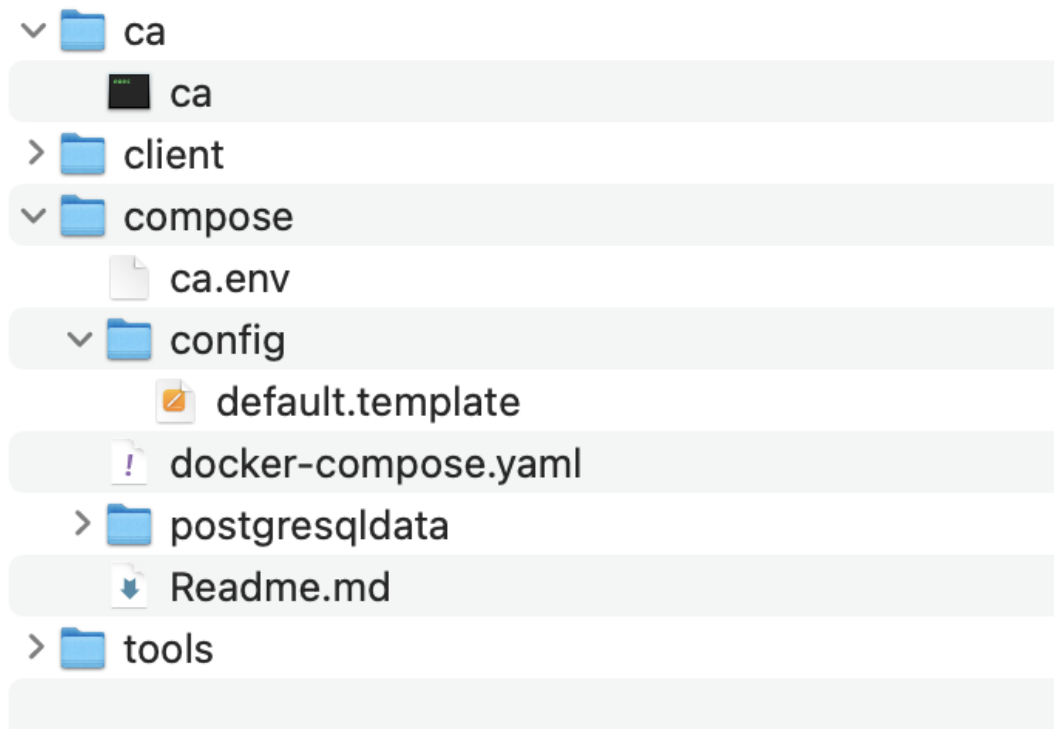


Рисунок 1 — Структура разархивированного файла

2. Перейдите в папку compose и отредактируйте файл ca.env. Укажите необходимые параметры:

```

# Адрес API CA (только hostname, без http://)
API_URL=ca.local

# Имя пользователя в БД Postgres
    
```

```
POSTGRES_USER=admin
```

```
# Пароль пользователя в БД Postgres
```

```
POSTGRES_PASSWORD=P@ssw0rd
```

```
# Имя БД Postgres
```

```
POSTGRES_DB=ca
```

```
# Строка подключения к БД Postgres
```

```
CA_DATABASE_URL=postgres://$POSTGRES_USER:$POSTGRES_PASSWORD@postgres:5432/$P
```

```
OSTGRES_DB?sslmode=disable
```

3. Выполните запуск проекта:

```
docker compose -p "avanpost-ca" up -d
```

После успешного запуска контейнеров административный интерфейс Avanpost CA будет доступен по следующим адресам:

- При локальной установке Docker: <http://localhost>
- При установке на удаленном сервере: http://IP-АДРЕС_СЕРВЕРА

КОНТАКТЫ

Avanpost СА разработан и поддерживается ООО «Аванпост».

Адрес: 129085, г. Москва, ул. Годовикова, д. 9, стр. 17

Телефон: +7 (495) 877 30 77

Е-mail: info@avanpost.ru (общий), partners@avanpost.ru (партнерство), support@avanpost.ru (поддержка)

Сайт: <https://www.avanpost.ru/>

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

СПИСОК РИСУНКОВ

Рисунок 1 — Структура разархивированного файла12

СПИСОК ТАБЛИЦ

Таблица 1 – Термины..... 4