

Защищённое развёртывание OpenClaw: руководство для нетехнических пользователей

Безопасное развёртывание OpenClaw с помощью Ansible и контейнеров Podman. Это руководство по усилению защиты охватывает сетевую изоляцию, лимиты бюджета API и фильтрацию исходящего трафика для ИИ-агентов.

Фернандо Люктемберг, 10 февраля 2026

Это дополнение к OpenClaw Security Guide: Step-by-Step Hardening by Tier. То руководство было написано для людей, знакомых с Linux, сетями и концепциями безопасности. Это — для всех остальных.

Если вы посмотрели видео на YouTube про OpenClaw, подумали «хочу такое», но ни разу не подключались к серверу по SSH и не слышали слова «Ansible» — это руководство для вас. Мы проведём вас от нуля до полностью защищённого развёртывания OpenClaw, шаг за шагом, с пояснениями к каждой команде.

Что вы получите в итоге: Безопасный, изолированный экземпляр OpenClaw, работающий на удалённом сервере (или запасном оборудовании), доступный с телефона или ноутбука по HTTPS, со всеми мерами усиления защиты из основного руководства, применёнными автоматически.

Что нужно для старта: Компьютер (Mac, Windows или Linux), банковская карта для сервера (если используете Hetzner или AWS) и примерно 90 минут сосредоточенной работы.

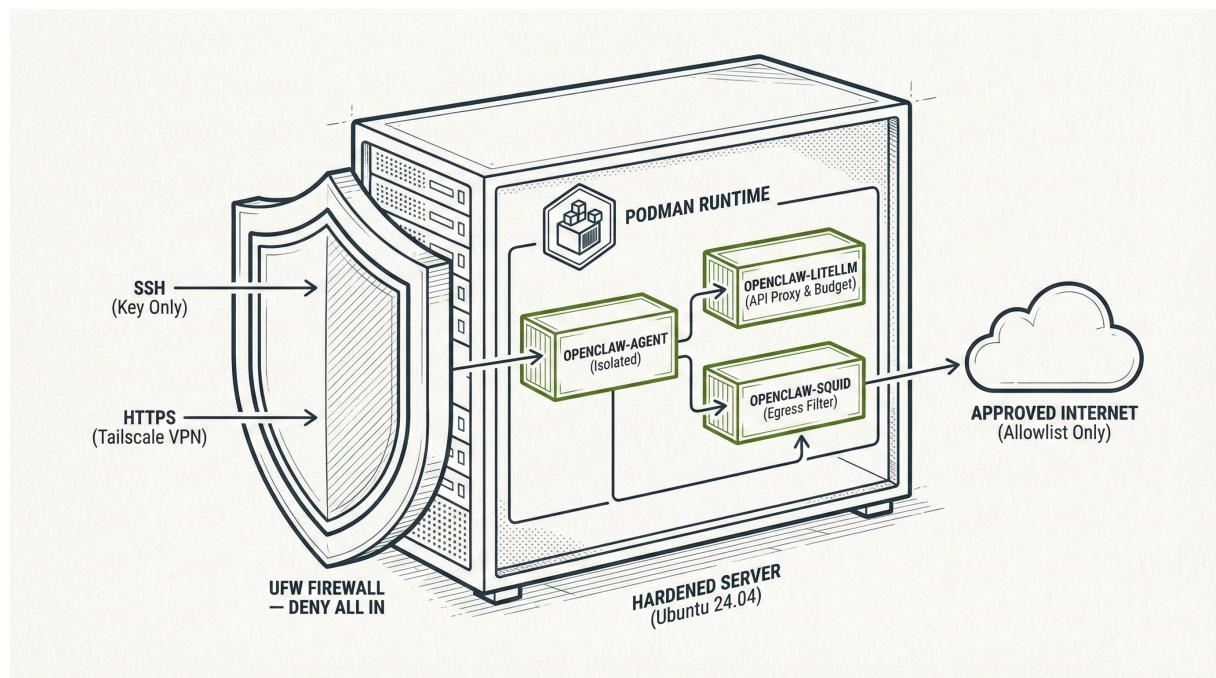


Figure 1: Рис. 1: Архитектура защищённого OpenClaw

Прежде чем начать: правила

Эти правила взяты из основного руководства по безопасности. Они действуют независимо от способа развёртывания.

Никогда не запускайте OpenClaw на основном компьютере. Ни на ноутбуке. Ни на десктопе. Ни на Mac, за которым работаете. OpenClaw получает собственную машину — будь то арендованный сервер или старый ноутбук в шкафу.

Никогда не подключайте важные аккаунты. Ни основную почту. Ни банкинг. Ни рабочий Slack. Ни менеджеры паролей. Ни соцсети, которые вам дороги. Подключайте только одноразовые аккаунты, потерю которых вы переживёте безболезненно. Если сомневаетесь, подходит ли аккаунт — не подключайте.

Это не инструмент «настроил и забыл». Вам нужно будет проверять его раз в месяц. Если это кажется чрезмерным, используйте Claude.ai напрямую.

Перечитайте эти три правила. Если хотя бы одно из них — стоп-фактор, остановитесь здесь и используйте Claude.ai. Серьёзно. Для большинства это лучший продукт, и он не требует всего этого.

Ещё здесь? Поехали.

Где запускать OpenClaw

У вас три варианта. Выберите один.

Вариант А: Hetzner Cloud (рекомендуется)

Лучший выбор для большинства. Hetzner — европейская хостинг-компания с дешёвыми и надёжными серверами. Сервер, достаточный для OpenClaw, стоит около 3,50 евро/месяц (примерно \$4). Вы арендуете компьютер в data-центре. Не нужно беспокоиться об электричестве, аппаратных сбоях или физической безопасности.

Вариант В: AWS (Amazon Web Services)

Лучший выбор, если у вас уже есть аккаунт AWS или его оплачивает работодатель. AWS дороже (\$8–15/месяц за аналогичные характеристики) и сложнее в настройке. Интерфейс перегружен, если вы никогда им не пользовались. Но если вы уже в экосистеме AWS, работает нормально.

Вариант С: Локальное оборудование

Лучший выбор, если у вас есть запасной компьютер, который пылится без дела. Старый ноутбук, Mac Mini, вышедший на пенсию десктоп. Он должен работать под Linux (мы это разберём), оставаться включённым и быть подключённым к домашней сети. Стоимость — только электричество (\$5–10/месяц), но вы отвечаете за всё: перебои питания, аппаратные сбои, настройку сети.

Моя рекомендация: Если у вас пока нет чёткого мнения, выбирайте Hetzner. Это самый дешёвый, самый простой вариант, и его проще всего уничтожить и пересоздать, если что-то пойдёт не так.

Термины, которые вам встретятся

Прежде чем начать — вот термины, которые будут попадаться. Запоминать их не нужно. Просто знайте, что они существуют, чтобы не теряться при встрече с ними.

Server / VPS: Компьютер, который вы арендуете у компании вроде Hetzner или AWS. Он работает 24/7 в data-центре. VPS расшифровывается как Virtual Private Server (виртуальный выделенный сервер). Он «виртуальный», потому что одна физическая машина разделена на несколько изолированных серверов. Вы получаете свой кусок.

SSH: Secure Shell. Способ подключиться к удалённому компьютеру и вводить на нём команды. Представьте переписку с компьютером: вы пишете команду, он отвечает результатом.

Терминал: Приложение на вашем компьютере, где вы вводите команды. На Mac оно называется Terminal (находится в Applications ➔ Utilities). На Windows — PowerShell или Windows Terminal. На Linux зависит от дистрибутива, но вы, скорее всего, это знаете.

IP-адрес: Число, идентифицирующее компьютер в интернете, например 49.12.45.67. Когда вы создаёте сервер, он получает IP-адрес. По этому адресу вы к нему подключаетесь.

SSH-ключ: Пара файлов (открытый и закрытый), используемая вместо пароля для входа на серверы. Открытый ключ размещается на сервере. Закрытый ключ остаётся на вашем компьютере. Это как замок и ключ: на сервере замок, у вас ключ, и больше ни у кого доступа нет.

Ansible: Инструмент для автоматизации настройки серверов. Вместо ручного ввода 200 команд вы запускаете один «плейбук» Ansible, и он делает всё за вас. Думайте о нём как об инструкции, которая выполняет сама себя.

Tailscale: Инструмент, создающий приватную зашифрованную сеть между вашими устройствами. После установки телефон, ноутбук и сервер могут безопасно общаться друг с другом, не выставляя ничего в публичный интернет.

Контейнер: Лёгкая изолированная «коробка», в которой работает программа. Представьте квартиру в многоэтажке: каждая квартира (контейнер) отделена, со своими замками и стенами, хотя все они в одном здании (сервере). OpenClaw работает внутри контейнеров, и если что-то пойдёт не так, ущерб останется внутри «коробки».

HTTPS: Зашифрованный веб-трафик. Когда вы видите значок замка в браузере — это HTTPS. Плейбук настраивает HTTPS для панели управления OpenClaw с помощью самоподписанного сертификата.

Часть 1: Подготовка компьютера

Прежде чем прикасаться к серверу, на вашем компьютере нужно установить несколько инструментов.

Шаг 1: Откройте терминал

Mac: Нажмите Cmd + Space, введите «Terminal», нажмите Enter. Появится окно с текстовым приглашением. Здесь вы будете вводить команды на протяжении всего руководства.

Windows: Вам нужна подсистема Windows для Linux (WSL). Откройте PowerShell от имени администратора (правый клик на меню «Пуск» ➔ «Windows PowerShell (Admin)») и выполните:

```
wsl --install
```

Перезагрузите компьютер по запросу. После перезагрузки откройте меню «Пуск» и найдите «Ubuntu». Это ваш терминал. Далее в руководстве предполагается, что вы вводите команды в терминале Ubuntu, а не в PowerShell.

Linux: Откройте терминал. Вы знаете как.

Шаг 2: Установите Ansible

Ansible — инструмент, который автоматически настроит ваш сервер. Установите его на свой компьютер (не на сервер).

Mac:

```
# Install Homebrew first (if you don't have it)
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

# Install Ansible
brew install ansible

# Verify it worked
ansible --version
```

Если команда `ansible --version` выводит номер версии (2.10 или выше), всё в порядке.

Windows (внутри WSL/Ubuntu):

```
sudo apt update
sudo apt install ansible -y

# Verify it worked
ansible --version
```

Linux (Debian/Ubuntu):

```
sudo apt update
sudo apt install ansible -y

# Verify it worked
ansible --version
```

Linux (Arch):

```
sudo pacman -S ansible

# Verify it worked
ansible --version
```

Если вместо номера версии видите ошибку — не продолжайте. Самое распространённое решение: сначала выполнить `sudo apt update`, а затем повторить установку.

Шаг 3: Установите Tailscale на компьютер

Tailscale — это способ безопасного доступа к OpenClaw с ваших устройств.

Перейдите на <https://tailscale.com> и создайте бесплатный аккаунт. Затем установите Tailscale на компьютер, за которым сейчас сидите:

Mac: Скачайте с <https://tailscale.com/download/mac> или установите через Homebrew:

```
brew install tailscale
```

Windows: Скачайте с <https://tailscale.com/download/windows> и запустите установщик.

Linux:

```
curl -fsSL https://tailscale.com/install.sh | sh  
sudo tailscale up
```

После установки войдите в Tailscale. Ваш компьютер появится в списке на панели администрирования по адресу <https://login.tailscale.com/admin/machines>.

Также установите Tailscale на телефон, если хотите получать доступ к OpenClaw с него. Приложение есть в App Store (iOS) и Play Store (Android).

Шаг 4: Сгенерируйте SSH-ключ

SSH-ключ позволяет входить на сервер безопасно, без пароля.

Проверьте, есть ли он у вас:

```
ls ~/.ssh/id_ed25519.pub
```

Если команда выводит путь к файлу — ключ уже есть. Переходите к следующему шагу.

Если написано «No such file or directory», сгенерируйте ключ:

```
ssh-keygen -t ed25519 -C "openclaw-server"
```

Программа спросит, куда сохранить. Нажмите Enter для пути по умолчанию. Затем запросит пароль (passphrase). Можно нажать Enter дважды, чтобы пропустить (менее безопасно, но проще), или ввести запоминающийся пароль.

Посмотрите открытый ключ:

```
cat ~/.ssh/id_ed25519.pub
```

Команда выведет длинную строку, начинающуюся с ssh-ed25519. Скопируйте её целиком. Она понадобится при создании сервера. Оставьте окно терминала открытым.

Шаг 5: Клонируйте плейбук Ansible

Скачайте плейбук для усиления защиты:

```
cd ~  
git clone https://github.com/Next-Kick/openclaw-hardened-ansible.git  
cd openclaw-hardened-ansible  
chmod +x deploy.sh update-allowlist.sh
```

Если git не установлен, сначала установите:

```
# Mac  
brew install git  
  
# Ubuntu/Debian/WSL  
sudo apt install git -y
```

Затем повторите команду git clone.

Компьютер готов. Пора создавать сервер.

Часть 2А: Создание сервера на Hetzner (рекомендуется)

Шаг 1: Создайте аккаунт Hetzner

Перейдите на <https://www.hetzner.com/cloud> и нажмите «Register». Введите email и создайте пароль. Потребуется подтвердить email и добавить способ оплаты (банковская карта).

Шаг 2: Создайте новый проект

После входа вы увидите Hetzner Cloud Console. Нажмите «New Project» и назовите его, например, «OpenClaw». Войдите в проект.

Шаг 3: Добавьте SSH-ключ

Прежде чем создавать сервер, добавьте SSH-ключ для входа.

Нажмите «Security» в левой панели, затем «SSH Keys», затем «Add SSH Key».

Вставьте скопированный ранее открытый ключ (строку ssh-ed25519 ...). Назовите его, например, «My Laptop». Нажмите «Add SSH Key».

Шаг 4: Создайте сервер

Нажмите «Servers» в левой панели, затем «Add Server».

Location: Выберите ближайшую локацию. В США — Ashburn или Hillsboro. В Европе — Falkenstein или Helsinki. Большого значения не имеет.

Image (операционная система): Выберите Ubuntu 24.04.

Type: В разделе «Shared vCPU» выберите CX22 (2 vCPU, 4 ГБ RAM). Стоимость — 4,35 евро/месяц, этого более чем достаточно для OpenClaw. Если планируете запускать локальную LLM (например, Ollama), понадобится что-то мощнее, но для API Anthropic/OpenAI через LiteLLM хватит CX22.

Networking: Оставьте по умолчанию (Public IPv4 и IPv6).

SSH Keys: Отметьте только что добавленный SSH-ключ.

Name: Дайте серверу имя, например openclaw-server.

Нажмите «Create & Buy Now». Примерно через 30 секунд сервер будет готов. Вы увидите IP-адрес (что-то вроде 49.12.45.67). Запишите или скопируйте — это адрес вашего сервера.

Шаг 5: Проверьте подключение

В терминале проверьте SSH-соединение:

```
ssh root@YOUR_SERVER_IP
```

Замените YOUR_SERVER_IP на IP из шага 4 (например, ssh root@49.12.45.67).

При первом подключении появится вопрос «Are you sure you want to continue connecting?» Введите yes и нажмите Enter.

Если видите приглашение root@openclaw-server:~# — вы подключились. Введите exit для отключения. Если получаете «Permission denied» или «Connection refused» — проверьте, что при создании сервера был выбран ваш SSH-ключ.

Настройка Hetzner завершена. Переходите к Части 3: Развёртывание OpenClaw.

Часть 2B: Создание сервера на AWS

AWS сложнее Hetzner. Если следующие шаги вызывают перегрузку — вернитесь и используйте Hetzner. В выборе простого пути нет ничего зазорного.

Шаг 1: Создайте аккаунт AWS

Перейдите на <https://aws.amazon.com> и нажмите «Create an AWS Account». Понадобятся email, банковская карта и номер телефона. У AWS есть бесплатный уровень, но подходящие инстансы слишком слабы для OpenClaw. Рассчитывайте на \$8–15/месяц.

Шаг 2: Перейдите в EC2

В AWS Console введите «EC2» в строке поиска. Нажмите «EC2» в результатах. Это сервис виртуальных серверов AWS.

Шаг 3: Импортируйте SSH-ключ

В панели EC2 нажмите «Key Pairs» в левой панели под «Network & Security». Нажмите «Actions» «Import Key Pair».

Назовите `openclaw-key`. Вставьте открытый ключ (строку `ssh-ed25519 . . .`). Нажмите «Import Key Pair».

Шаг 4: Создайте группу безопасности

Группа безопасности (security group) — это файрвол для сервера. Нажмите «Security Groups» под «Network & Security». Нажмите «Create Security Group».

Name: `openclaw-sg` **Description:** OpenClaw server firewall **VPC:** По умолчанию.

Inbound rules: Нажмите «Add Rule».

- Type: SSH, Source: My IP (подставится ваш текущий IP)

Единственное нужное входящее правило. Всё остальное обрабатывает Tailscale.

Outbound rules: По умолчанию (весь трафик разрешён).

Нажмите «Create Security Group».

Шаг 5: Запустите инстанс

Нажмите «Instances», затем «Launch Instances».

Name: `openclaw-server`

Application and OS Images: Нажмите «Ubuntu», выберите Ubuntu Server 24.04 LTS.

Instance type: `t3.medium` (2 vCPU, 4 ГБ RAM). Примерно \$0,0416/час, около \$30/месяц. Дешевле — `t3.small` (2 vCPU, 2 ГБ RAM), ~\$15/месяц, но производительность впритык.

Key pair: Выберите `openclaw-key`.

Network settings: Нажмите «Edit». В «Firewall (security groups)» выберите «Select existing security group» `openclaw-sg`.

Configure storage: Измените на 30 ГиБ (стандартные 8 ГБ слишком мало).

Нажмите «Launch Instance». Через минуту нажмите «View all instances». Инстанс покажет статус «Running» с публичным IPv4. Скопируйте адрес.

Шаг 6: Проверьте подключение

`ssh ubuntu@YOUR_SERVER_IP`

Примечание: инстансы Ubuntu на AWS используют пользователя `ubuntu`, а не `root`.

Если видите `ubuntu@ip-xxx:~$` — подключились. Введите `exit`.

Важно для части 3: Используйте `ubuntu` как SSH-пользователя вместо `root`.

Настройка AWS завершена. Переходите к Части 3.

Часть 2С: Настройка локального оборудования

Нужен запасной компьютер, выделенный под OpenClaw. Старый ноутбук, Mac Mini, десктоп на пенсии или Raspberry Pi 5 (8 ГБ RAM).

Шаг 1: Установите Ubuntu Server

Скачайте Ubuntu Server 24.04 LTS с <https://ubuntu.com/download/server>.

Понадобится USB-флешка (≥ 4 ГБ). Создайте загрузочный USB:

Mac: balenaEtcher (<https://etcher.balena.io>).

Windows: Rufus (<https://rufus.ie>).

Linux: dd или balenaEtcher.

Подключите флешку к запасному компьютеру, загрузитесь с USB (F12/F2/Del/Esc при старте). Следуйте установщику:

- Язык и раскладка клавиатуры
- «Ubuntu Server» (не минимальная версия)
- Сеть: DHCP (по умолчанию)
- Пропустите прокси
- Зеркало по умолчанию
- Весь диск (разметка по умолчанию)
- Пользователь: openclaw, надёжный пароль
- OpenSSH server: обязательно отметить
- Snap-пакеты: не выбирать
- Завершение перезагрузка извлечь флешку

Шаг 2: Узнайте IP-адрес

Войдите на сервер и выполните:

```
ip addr show | grep "inet " | grep -v 127.0.0.1
```

Строка типа 192.168.1.105/24 — часть до / и есть локальный IP.

Шаг 3: Скопируйте SSH-ключ на сервер

С основного компьютера:

```
ssh-copy-id openclaw@YOUR_SERVER_LOCAL_IP
```

Шаг 4: Проверьте подключение

```
ssh openclaw@YOUR_SERVER_LOCAL_IP
```

Если вошли без пароля — SSH-ключ работает. Введите exit.

Шаг 5: Сделайте IP статическим (рекомендуется)

В роутере (обычно `http://192.168.1.1`) найдите DHCP-резервирование. Или настройте на сервере:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

```
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: no
      addresses:
        - 192.168.1.105/24
      routes:
        - to: default
          via: 192.168.1.1
  nameservers:
    addresses:
      - 1.1.1.1
      - 8.8.8.8
```

```
sudo netplan apply
```

Переходите к Части 3.

Часть 3: Развёртывание OpenClaw

Здесь тяжёлую работу берёт на себя плейбук Ansible. Процесс одинаков для Hetzner, AWS и локального оборудования.

Шаг 1: Перейдите в каталог плейбука

На вашем компьютере (не на сервере):

```
cd ~/openclaw-hardened-ansible
```

Шаг 2: Выберите провайдера LLM

OpenClaw нужна языковая модель. Три варианта:

Anthropic (рекомендуется): API-ключ с <https://console.anthropic.com>. Начинается с `sk-`, `ant-`. \$10–30/месяц.

OpenAI: API-ключ с <https://platform.openai.com/api-keys>.

Ollama (бесплатно, но нужно мощное железо): Локальная модель. RAM 16 ГБ+, желательно GPU. На Hetzner за 4 евро непрактично.

Далее предполагаем Anthropic. Плейбук поддерживает все три.

Шаг 3: Запустите развёртывание

Вариант А: Интерактивный (рекомендуется)

```
./deploy.sh
```

Вариант В: С SSH-ключом (для VPS)

```
./deploy.sh \
--target YOUR_SERVER_IP \
--ssh-user root \
--ssh-key ~/.ssh/id_ed25519
```

Вариант С: Продвинутый (пример с Ollama)

```
./deploy.sh \
-t 10.0.110.100 \
--ssh-user fernando \
--ask-pass \
-p ollama \
-m "deepseek-r1:8b" \
-u "http://10.0.100.25:11434" \
--non-interactive
```

Скрипт задаст вопросы:

- «Enter Target Host IP:» — IP сервера
- «Enter Initial SSH User:» — root (Hetzner), ubuntu (AWS), openclaw (локальный)
- «Select LLM Provider:» — 2 для Anthropic
- «Enter API Key:» — ваш API-ключ

Подтвердите и ждите. Плейбук выполняется 10–20 минут.

Часть 4: Что плейбук сделал

Понимать все детали необязательно, но вот что произошло.

Плейбук создал пользователя `openclaw`, отключил вход по паролю и настроил файрвол (UFW), блокирующий всё кроме SSH и порта OpenClaw.

Установил Podman (среда выполнения контейнеров) и развернул три контейнера:

- **openclaw-agent:** Сам OpenClaw. Обеспечивает HTTPS через самоподписанный сертификат. Изолирован в приватной сети, не может напрямую выходить в интернет.
- **openclaw-litellm:** Прокси между OpenClaw и провайдером ИИ. Хранит настоящий API-ключ и устанавливает лимиты бюджета, чтобы агент не потратил тысячи долларов случайно.
- **openclaw-squid:** Веб-прокси-«вышибала». OpenClaw может обращаться только к явно разрешённым сайтам (GitHub, Telegram). Всё остальное блокируется.

Несколько уровней изоляции: сервер отделён от компьютера, контейнеры — друг от друга, сеть заблокирована.

Часть 5: Текущее обслуживание

Усиление защиты — не разовое мероприятие. 30 минут раз в месяц.

Ежемесячный чек-лист

Подключитесь к серверу:

```
ssh -i ssh-keys/YOUR_HOSTNAME.pem openclaw@YOUR_SERVER_IP
```

Проверьте контейнеры:

```
podman ps
```

Три контейнера со статусом «Up». Если что-то «Exited»:

```
cd ~/openclaw-docker  
podman-compose down  
podman-compose up -d
```

Обновите систему:

```
sudo apt update && sudo apt upgrade -y
```

Проверьте журналы безопасности:

```
cat ~/openclaw-docker/security-audit-*.*.log | tail -50
```

Ищите «CRITICAL» и «WARNING».

Логи Squid (заблокированные запросы):

```
podman logs openclaw-squid --since 720h | grep TCP_DENIED | tail -20
```

Чтобы разрешить домен:

```
echo ".example.com" >> ~/openclaw-docker/allowlist.txt  
podman exec openclaw-squid squid -k reconfigure
```

Проверьте расход API на <https://console.anthropic.com>.

Часть 6: Типичные задачи

Перезапуск OpenClaw

```
ssh -i ssh-keys/YOUR_HOSTNAME.pem openclaw@YOUR_SERVER_IP  
cd ~/openclaw-docker  
podman-compose restart
```

Полная остановка

```
cd ~/openclaw-docker  
podman-compose down
```

Запуск после остановки

```
cd ~/openclaw-docker  
podman-compose up -d
```

Просмотр логов

```
cd ~/openclaw-docker  
podman-compose logs -f
```

Ctrl+C для выхода.

Добавление домена в allowlist

```
echo ".newdomain.com" >> ~/openclaw-docker/allowlist.txt  
podman exec openclaw-squid squid -k reconfigure
```

Обновление OpenClaw

```
cd ~/openclaw-docker  
podman-compose pull  
podman-compose up -d
```

Полный сброс

Hetzner: Удалите сервер, создайте новый, запустите плейбук.

AWS: Завершите инстанс, запустите новый, запустите плейбук.

Локальный: Переустановите Ubuntu, запустите плейбук.

Плейбук рассчитан на повторный запуск. Секреты сохраняются, если .env на месте.

Часть 7: Экстренные процедуры

Если подозреваете компрометацию — действуйте быстро.

Шаг 1: Убейте его

```
ssh -i ssh-keys/YOUR_HOSTNAME.pem openclaw@YOUR_SERVER_IP  
cd ~/openclaw-docker  
podman-compose down  
sudo ufw deny out to any  
sudo ufw deny in from any
```

Шаг 2: Отзовите всё

С другого устройства:

- API-ключ Anthropic: <https://console.anthropic.com/settings/keys>
- API-ключ OpenAI: <https://platform.openai.com/api-keys>
- Подключённые аккаунты: отзовите доступ в настройках каждого сервиса
- Смените все пароли, даже одноразовых аккаунтов

Шаг 3: Пересоберите

Не пытайтесь «вычистить» скомпрометированный сервер. Уничтожьте и начните заново.

```
cd ~/openclaw-hardened-ansible  
./deploy.sh
```

Используйте новый API-ключ. Не переиспользуйте учётные данные от скомпрометированного развёртывания.

Устранение неполадок

«Не могу подключиться по SSH» — Проверьте IP, имя пользователя и SSH-ключ. Hetzner: root/openclaw. AWS: ubuntu/openclaw.

«Панель не загружается» — Используйте HTTPS: <https://100.x.x.x:18789>. Проверьте Tailscale. Проверьте podman ps.

«Браузер пишет, что соединение небезопасно» — Ожидаемо при самоподписанных сертификатах. «Дополнительно» ✎ «Продолжить».

«Не могу войти в панель» — Проверьте gateway token: cat ~/openclaw-docker/.env | grep OPENCLAW_GATEWAY_TOKEN

«Ansible упал на середине» — Перезапустите ./deploy.sh с теми же настройками.

«Забыл IP сервера» — Hetzner: <https://console.hetzner.cloud>. AWS: EC2 Instances. Tailscale: <https://login.tailscale.com/admin/machines>.

«Сколько это стоит?» — Hetzner: ~\$4/мес. Anthropic API: \$10–30/мес. Tailscale: бесплатно. Итого: \$15–35/мес.

Что не вошло в руководство

- Ручное развёртывание без Ansible
- Детальные объяснения каждого уровня защиты
- Продвинутые конфигурации (политики исполнения, профили рисков, ротация учётных данных)
- Полный список запрещённых аккаунтов
- От чего защита не спасает (инъекция промптов, атаки на цепочку поставок)

Помните правила. Только одноразовые аккаунты. Ежемесячное обслуживание. Подозрительно — сначала отключите, разбирайтесь потом. Плейбук автоматизировал сложную часть, но бдительность — ваша задача.

Ссылки

- OpenClaw Security Guide: Step-by-Step Hardening by Tier: <https://nextkicklabs.substack.com>
- OpenClaw Hardened Ansible Playbook: <https://github.com/Next-Kick/openclaw-hardened-ansible>