# دليل تشغيل P0-6 — تحصين VPS ووقت تشغيل خط الأنابيب

القسم operations-it-06 النوع runbook الحالة active المالك Founder آخر تحديث 2026-06-21

رفيق لـ `setup-vps.md` (الذي يغطّي *السبب*). هذا الملف هو *الكيفية الدقيقة* — أوامر للنسخ واللصق، بترتيب آمن، مع فحوص تحقّق وملاحظات تراجع.

**الخادم:** IP `72.62.20.20` / **اسم المضيف:** `srv1209075.hstgr.cloud` / Hostinger KVM 2 (2 vCPU / 8 GB / 100 GB NVMe) **نظام التشغيل:** Ubuntu 24.04 LTS · **مستخدم المسؤول:** `adel` (sudo) **الدور:** صندوق خط أنابيب لبيانات عامة فقط — فهرسة RAG، أداة تقييم، تجهيز. ليس أبدًا الإنتاج، وليس أبدًا بيانات شخصية. (انظر `setup-vps.md` ← "Data boundary (PDPL)".)

---

## ⚠️ القواعد الذهبية — اقرأها قبل البدء

1. **لا تُغلق أبدًا جلسة SSH العاملة لديك** حتى تثبت جلسة *جديدة* أنها تعمل مع الإعداد الجديد. الخطوتان 4 و6 قد تحبسانك خارجًا إن تسرّعت.
2. **أبقِ نافذتي طرفية جاهزتين** على الماك للخطوتين 4 و6 — إحداهما خط أمانك، والأخرى الاختبار.
3. **إن حُبست خارجًا:** Hostinger hPanel → VPS → *Browser terminal* (أو وحدة VNC) يمنحك وصول root لا يعتمد على SSH. أوامر التراجع موجودة في أسفل هذا الملف.
4. شغّل الخطوات **بالترتيب**. يأتي تحديث نظام التشغيل أولًا؛ ويأتي تحصين SSH أخيرًا (فهو الأخطر، وعندئذ يكون دخول المفتاح قد ثبت فعلًا).

---

## الخطوة 1 — التحقق من الوصول (خط الأساس)

من طرفية الماك:

```
ssh adel@72.62.20.20
```

ينبغي أن تصل إلى صدفة **دون أن يُطلب منك كلمة مرور** (المفتاح SSH هو من فعلها). إن طُلبت كلمة مرور، توقّف — المفتاح غير مثبّت والخطوة 6 ستحبسك خارجًا. ثم، على الـ VPS:

```
whoami                        # → adel
sudo whoami                   # → root   (may prompt for adel's sudo password — fine)
lsb_release -d                # → Ubuntu 24.04.x LTS
uname -r                      # kernel version
cat ~/.ssh/authorized_keys    # must show your public key — confirms key login survives
Step 6
```

**نقطة فحص:** `adel`، `root`، `Ubuntu 24.04`، و `authorized_keys` غير فارغ. لا تتجاوز الخطوة 6 ما لم يُظهر `authorized_keys` مفتاحك.

---

## الخطوة 2 — تحديث نظام التشغيل

```
sudo apt update
sudo apt full-upgrade -y
sudo apt autoremove --purge -y
```

إن جرى ترقية النواة أو `libc`، أعد التشغيل وأعد الاتصال:

```
sudo reboot
# wait ~30 s, then from the Mac:
ssh adel@72.62.20.20
```

فعّل تحديثات الأمان التلقائية (غير تفاعلية):

```
sudo apt install -y unattended-upgrades
echo 'APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";' | sudo tee /etc/apt/apt.conf.d/20auto-upgrades
```

**نقطة فحص:** ينتهي `apt` دون حزم معلّقة/معطوبة.

---

## الخطوة 3 — تثبيت جدار الحماية fail2bang ووقت تشغيل خط الأنابيب

الأدوات الأساسية (سطر واحد):

```
sudo apt install -y ufw fail2ban git curl ca-certificates build-essential software-
properties-common
```

**Python 3.11** — يأتي Ubuntu 24.04 بـ 3.12؛ خط أنابيب RAG يستهدف 3.11، لذا أضفه عبر PPA الخاص بـ deadsnakes (يبقى 3.12 الافتراضي للنظام؛ نضيف 3.11 إلى جانبه فقط):

```
sudo add-apt-repository -y ppa:deadsnakes/ppa
sudo apt update
sudo apt install -y python3.11 python3.11-venv python3.11-dev
python3.11 --version          # → Python 3.11.x
```

Node.js 20 — عبر NodeSource:

```
curl -fsSL https://deb.nodesource.com/setup_20.x | sudo -E bash -
sudo apt install -y nodejs
node --version                # → v20.x
npm --version
```

git (مُثبّت أعلاه):

```
git --version
```

نقطة فحص: `python3.11`، `node v20.x`، `npm`، `git` تبلّغ كلها عن الإصدارات.

---

## الخطوة 4 — تهيئة جدار الحماية (ufw)

⚠️ اسمح بـ SSH *قبل* تفعيل ufw، وإلا حبست نفسك خارجًا. شغّل هذه بالترتيب:

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow OpenSSH            # opens 22/tcp via the app profile
sudo ufw enable                   # answer 'y' at the prompt
sudo ufw status verbose
```

`ufw enable` لا يُسقط اتصالك الحالي (المُنشأ). ومع ذلك، تحقّق: **افتح نافذة طرفية ثانية** على الماك وشغّل `ssh adel@72.62.20.20`. إن اتّصلت، فإن ufw آمن. أبقِ كلتا النافذتين مفتوحتين حتى الخطوة 6.

نقطة فحص: `ufw status verbose` يُظهر `Status: active` وقاعدة `OpenSSH ALLOW`؛ وتتصل جلسة SSH جديدة.

---

## الخطوة 5 — تهيئة fail2ban

يسجّل Ubuntu 24.04 المصادقة إلى journald (لا `/var/log/auth.log` افتراضيًا)، لذا يجب أن يستخدم السجن الخلفية systemd:

```
sudo tee /etc/fail2ban/jail.local > /dev/null <<'EOF'
[DEFAULT]
bantime  = 1h
findtime = 10m
maxretry = 5
backend  = systemd

[sshd]
enabled = true
EOF

sudo systemctl enable --now fail2ban
sudo systemctl restart fail2ban
sudo systemctl is-active fail2ban     # → active
sudo fail2ban-client status           # → Jail list: sshd
sudo fail2ban-client status sshd      # → shows the sshd jail detail
```

نقطة فحص: `fail2ban` في حالة `active` و `fail2ban-client status` يدرج `sshd`.

---

## الخطوة 6 — تحصين SSH (دخول root + مصادقة كلمة المرور مُعطّلة)

⚠️ أخطر خطوة. أبقِ جلستك الحالية مفتوحة. لتكن لديك نافذة ثانية جاهزة.

أولًا، انظر ما هو موجود فعلًا (تأتي صور السحابة أحيانًا بـ drop-in يعيد تفعيل مصادقة كلمة المرور):

```
ls -la /etc/ssh/sshd_config.d/
sudo grep -RinE 'passwordauthentication|permitrootlogin' /etc/ssh/sshd_config
/etc/ssh/sshd_config.d/
```

أنشئ الـ drop-in الخاص بنا. سمّي `01-` كي يُرتّب **أولًا** — في `sshd_config`، القيمة الأولى تفوز، لذا يتجاوز هذا أي `50-cloud-init.conf` لاحق:

```
sudo tee /etc/ssh/sshd_config.d/01-flygaca-hardening.conf > /dev/null <<'EOF'
# Fly GACA VPS hardening — P0-6
PermitRootLogin no
PasswordAuthentication no
KbdInteractiveAuthentication no
PubkeyAuthentication yes
PermitEmptyPasswords no
MaxAuthTries 3
EOF
```

اختبر الصيغة، ثم افحص الإعداد **المُدمج الفعّال** — هذا هو الاختبار الحقيقي:

```
sudo sshd -t && echo "syntax OK"
sudo sshd -T | grep -Ei
'permitrootlogin|passwordauthentication|kbdinteractive|pubkeyauthentication'
```

المُخرج المتوقع:

```
permitrootlogin no
pubkeyauthentication yes
passwordauthentication no
kbdinteractiveauthentication no
```

إن كان `passwordauthentication` لا يزال يُظهر `yes`، فإن drop-in متعارضًا يُقرأ أولًا — افتح الملف المخالف من `grep` أعلاه وعلّق سطره، ثم أعد الفحص. **لا تُعد تشغيل ssh حتى يُظهر `sshd -T` القيم الأربع المتوقعة.**

طبّق:

```
sudo systemctl restart ssh
```

**الآن تحقّق قبل إغلاق أي شيء.** في نافذة الطرفية *الثانية*:

```
ssh adel@72.62.20.20      # must log in with the key
ssh root@72.62.20.20      # must be REFUSED
```

فقط بمجرد أن تعمل جلسة `adel` الجديدة **و** يُرفض root، أغلق النافذة القديمة.

**نقطة فحص:** يعمل دخول مفتاح `adel` الجديد؛ ويُرفض دخول `root`؛ ويُظهر `sshd -T` القيم الأربع المتوقعة.

---

## الخطوة 7 — التأكيد وتسجيل المنطقة

```
curl -s ipinfo.io
```

دوّن حقول `city` / `region` / `country` / `org`. قارن مع *Overview* ← VPS ← Hostinger hPanel ← موقع مركز البيانات (اللوحة مرجعية؛ `ipinfo.io` هو تحديد جغرافي وقد يكون تقريبيًا). موقع في أوروبا (ألمانيا أو فرنسا) متوقّع ومقبول — يحوي الـ VPS بيانات عامة فقط.

سجّل المنطقة المؤكَّدة في `../phase0.md` (الخطوة 8).

---

## الخطوة 8 — تسجيل النتيجة

حدّث `../phase0.md` ← P0-6: ضع علامة على مربعات الاختيار المنجزة، اضبط الحالة إلى `Done`، واملأ المنطقة وإصدارات وقت التشغيل المثبّتة. (تم في مساحة عمل Cowork إلى جانب دليل التشغيل هذا.)

---

## الحالة النهائية — كيف يبدو "المُنجز"

| البند | المتوقع |
|---|---|
| نظام التشغيل | Ubuntu 24.04 LTS، محدّث بالكامل، تحديثات الأمان التلقائية مفعّلة |
| SSH | بالمفتاح فقط؛ دخول root معطّل؛ مصادقة كلمة المرور معطّلة |
| جدار الحماية | `ufw` نشط — فقط OpenSSH (22) واردًا |
| الحماية من القوة الغاشمة | `fail2ban` نشط، سجن `sshd` مفعّل |
| Python | x.3.11 متاح ( `python3.11` ) إلى جانب 3.12 للنظام |
| Node.js | v20.x + npm |
| git | مُثبّت |
| المنطقة | مؤكّدة ومُسجّلة في `phase0.md` |

---

## التراجع — إن حدث خطأ ما

استخدم Hostinger hPanel → VPS → Browser terminal / VNC console لكل هذه. إنها وحدة root لا تعتمد على SSH أو جدار الحماية.

محبوس خارجًا بعد الخطوة 6 (تحصين SSH):

```
rm /etc/ssh/sshd_config.d/01-flygaca-hardening.conf
systemctl restart ssh
```

محبوس خارجًا بعد الخطوة 4 (جدار الحماية):

```
ufw disable
```

fail2ban حظر عنوان IP الخاص بك:

```
fail2ban-client set sshd unbanip <your-ip>
```

(اعثر على عنوان IP الخاص بك بـ `curl -s ifconfig.me` من الماك.)

---

*جزء من جولات إعداد المرحلة 0 لـ Fly GACA. ليست استشارة قانونية؛ حدّ بيانات نظام حماية البيانات الشخصية (PDPL) بحسب `setup-vps.md`.*