VPS Setup Guide 4

Sunucuyu güvenli hâle getirmek ve Coolify'ı kurmak

Bu bölüm VPS Setup Guide 3'ün devamı. `203.0.113.10`, `deploy` ve `example.com` gibi yer tutucuları kendi değerlerinizle değiştirin.

> **Neden Coolify?** Tek bir VPS'i Odoo ve n8n gibi ayrı uygulamalara böler; her birinin kendi adresi olur.

İçindekiler

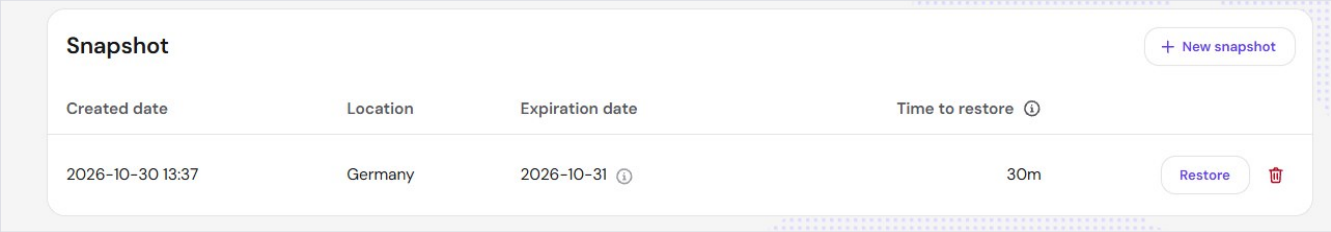
Adım 1	Snapshot alın
Adım 2	Güncellemeler ve temel araçlar
Adım 3	Girişi güvenli hâle getirin
Adım 4	Güvenlik duvarını oluşturun
Adım 5	Coolify'ı kurun
Adım 6	Coolify'a kendi adresini verin
Adım 7	Coolify'a yalnızca kendi IP'nizden erişin
Adım 8	Her şeyi Cloudflare'den geçirin
Adım 9	Her yolu test edin

> **Ekran görüntüleri hakkında.** hPanel, Cloudflare ve Coolify İngilizce olduğu için ekran görüntüleri ve kalın yazılmış düğme adları panelde gördüğünüz gibi İngilizce bırakıldı.

ADIM 1

Snapshot alın

hPanel'de **VPS**, ardından **Manage**, **Backups & Monitoring** ve **Snapshots & Backups**'ı açın ve **New snapshot**'a tıklayın. Sunucunun bir kopyası alınır ve hiçbir şey kapanmaz.



Expiration date sütununa bakın. Örnek kurulumda snapshot ertesi gün siliniyordu; yani yalnızca çalışırken sizi korur, gerçek yedeklerin yerini tutmaz.

ADIM 2

Güncellemeler ve temel araçlar

root olarak giriş yapın ve şunu çalıştırın:

```
apt update && apt full-upgrade -y
apt install -y fail2ban
timedatectl set-timezone Europe/Istanbul
cat > /etc/fail2ban/jail.d/sshd.local <<'EOF'
[sshd]
enabled = true
backend = systemd
EOF
systemctl enable --now fail2ban
systemctl restart fail2ban
```

Saat dilimini kendi bölgenize göre değiştirin. Sonrasında `/var/run/reboot-required` dosyası varsa `systemctl reboot` çalıştırın, tekrar giriş yapın ve `systemctl --failed` yazın. Hiçbir şey listelenmemeli.

ADIM 3

Girişi güvenli hâle getirin

Kişisel bir kullanıcı oluşturun. `deploy` yerine kendi adınızı yazın:

```
adduser --disabled-password --gecos "" deploy
usermod -aG sudo,docker deploy
install -d -m 700 -o deploy -g deploy /home/deploy/.ssh
install -m 600 -o deploy -g deploy /root/.ssh/authorized_keys \
  /home/deploy/.ssh/authorized_keys
echo 'deploy ALL=(ALL) NOPASSWD:ALL' > /etc/sudoers.d/90-deploy
chmod 440 /etc/sudoers.d/90-deploy
```

Bu kullanıcının şifresi yok; yalnızca SSH anahtarınızla giriş yapılabilir. Anahtarı kaybederseniz hPanel'deki **Web console**'u kullanın.

İkinci bir pencerede çalıştığını kontrol edin: `ssh deploy@203.0.113.10`, ardından `sudo whoami`. Sonuç `root` olmalı.

Sonra şifreyle girişi kapatın. İlk satır bir güvenlik ağıdır: siz iptal etmezseniz değişikliği 5 dakika sonra geri alır.

```
sudo systemd-run --unit=ssh-rollback --on-active=5min /bin/sh -c \
  'rm -f /etc/ssh/sshd_config.d/00-hardening.conf; systemctl reload ssh'
sudo tee /etc/ssh/sshd_config.d/00-hardening.conf > /dev/null <<'EOF'
PasswordAuthentication no
KbdInteractiveAuthentication no
PermitRootLogin prohibit-password
EOF
sudo sshd -t && sudo systemctl reload ssh
```

Coolify kendi sunucusuna root olarak anahtarla bağlanır, bu yüzden root'un anahtarla girişi açık kalır. Yeni bir pencereden anahtarınızın hâlâ çalıştığını ve şunun reddedildiğini test edin:

```
ssh -o PubkeyAuthentication=no deploy@203.0.113.10
```

Her şey yolundaysa güvenlik ağını iptal edin:

```
sudo systemctl stop ssh-rollback.timer
```

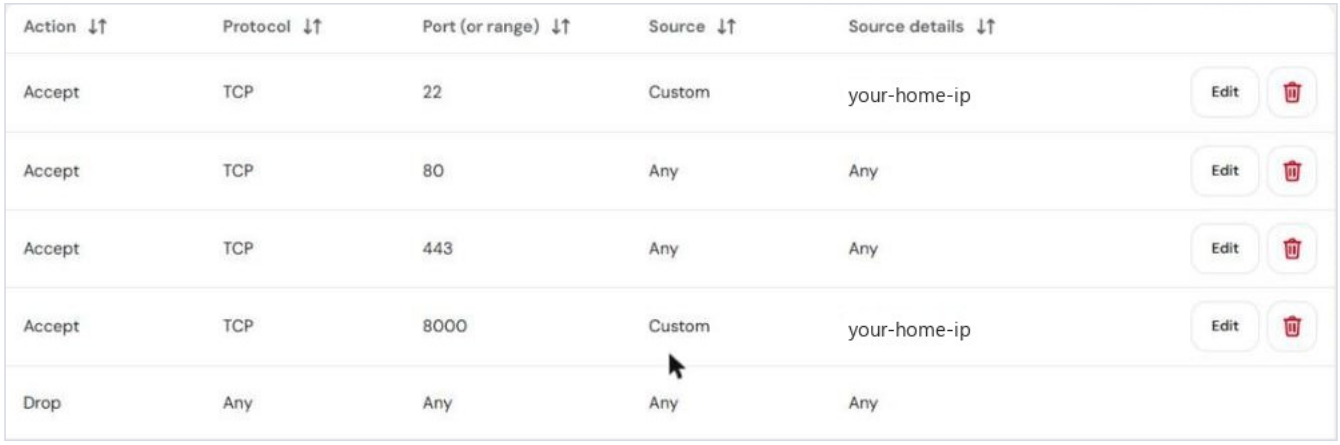
ADIM 4

Güvenlik duvarını oluşturun

Ev IP adresinizi api.ipify.org adresinden öğrenin. hPanel'de **Security**, ardından **Firewall** ve **+ Firewall**'ı açın. Bir ad verin, **Edit** ile açın ve şu kuralları ekleyin:

Action	Protocol	Port	Source
Accept	TCP	22	Custom: `your-home-ip`
Accept	TCP	80	Anywhere
Accept	TCP	443	Anywhere
Accept	TCP	8000	Custom: `your-home-ip`, kısa bir süre için

En alttaki **Drop** satırı otomatik eklenir ve geri kalan her şeyi engeller.



Güvenlik duvarı listesine dönün, anahtarı açın ve **Activate**'e tıklayın. SSH pencerenizi açık tutun ve hemen yeni bir girişi test edin.

> **Her değişiklikten sonra Synchronize.** Yeni bir güvenlik duvarı, onu etkinleştirdiğinizde uygulanır. Kuralları sonradan düzenlerseniz sarı bir çubuk çıkar ve **Synchronize**'a tıklayana kadar sunucuda hiçbir şey değişmez.
>
> **Ev IP'niz değişirse SSH çalışmaz.** hPanel'de kuralı güncelleyin ve **Synchronize**'a tıklayın.

ADIM 5

Coolify'ı kurun

Resmî kurulum betiğini root olarak çalıştırın:

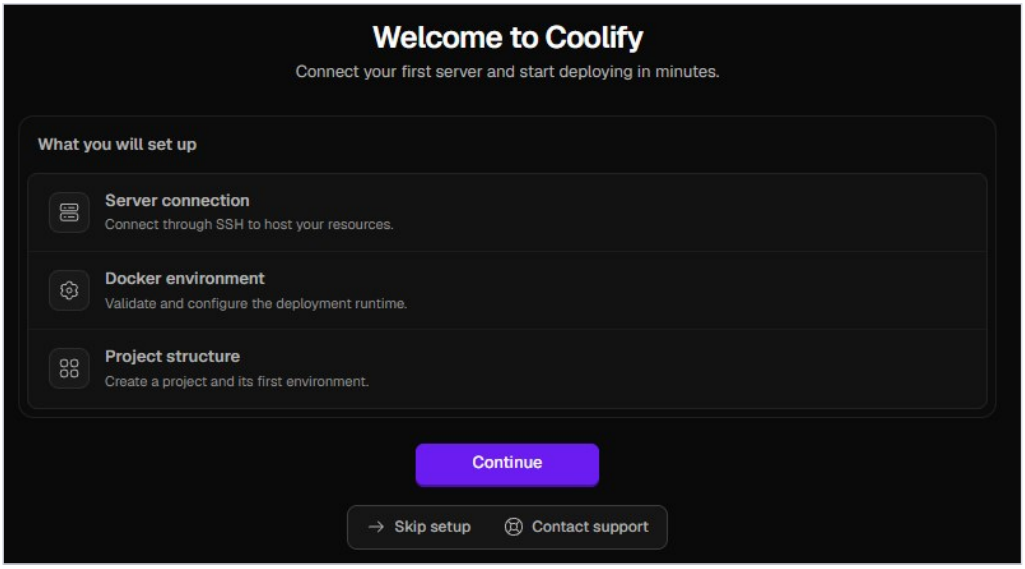
```
curl -fsSL https://cdn.coollabs.io/coolify/install.sh -o coolify-install.sh
bash coolify-install.sh
```

Örnek kurulumda bir dakikadan kısa sürdü; Docker zaten kuruluysa onu kullanır.

Yönetici hesabını oluşturmak için 10 dakikanız var. Hemen `http://203.0.113.10:8000` adresini açın. Süre dolarsa `docker restart coolify` çalıştırın. Şifrenizi kendiniz yazın.

> **root'un anahtar dosyasını kontrol edin.** Örnek kurulumda kurulum betiği kendi anahtarını `/root/.ssh/authorized_keys` dosyasındaki son satırın sonuna ekledi, çünkü dosya bir satır sonuyla bitmiyordu. Sizin anahtarınız çalışmaya devam etti ama Coolify'ınki çalışmazdı. `cut -d" " -f3 /root/.ssh/authorized_keys` çalıştırın; her anahtar kendi satırında görünmeli. İki ad birleşmişse dosyayı `nano` ile düzeltin.

Karşılama ekranlarında **Continue**'ya tıklayın, **This machine**'ı seçin ve ilk projeyi oluşturun.



> **.env dosyasını saklayın.** `/data/coolify/source/.env` dosyasının bir kopyasını şifre yöneticinizde tutun. Coolify'ın gizli anahtarlarını içerir; asla bir depoya göndermeyin ya da bir sohbete yapıştırmayın.

ADIM 6

Coolify'a kendi adresini verin

1. Cloudflare'de **DNS**, ardından **Records** ve **Add record**'ı açın. Tür `A`, ad `coolify`, VPS IP'niz; proxy açık kalsın.
2. Coolify'da **Settings**'i açın, **URL** alanına `https://coolify.example.com` yazın ve kaydedin.
3. Adresi açın. Geçerli bir sertifikayla Coolify giriş sayfasını görmelisiniz.

Hata gibi görünen ama hata olmayan iki durum:

- Kendi bilgisayarınızda "Could not resolve host", modeminizin eski bir cevabı hatırladığı anlamına gelebilir. Kendiliğinden düzelir; örnek kurulumda yaklaşık 10 dakika sürdü.
- IP adresi ve 8000 portuyla çalışırken Coolify "Cannot connect to real-time service" uyarısı verebilir ve proxy'yi **Exited** gösterebilir. Güvenlik duvarı o ek portları engelliyor. Proxy'yi `docker ps` ile kontrol edin. **Acknowledge & Disable**'a tıklamayın.

ADIM 7

Coolify'a yalnızca kendi IP'nizden erişin

Bunun bilinen yolu Cloudflare Access, ama ücretsiz paketi bile kart bilgisi istiyor. Bir müşterinin hesabında bunun yerine kart gerektirmeyen şu ücretsiz kuralı kullanın.

Cloudflare'de **Security**, ardından **Security rules**'u açın ve **Custom rules**'un yanındaki **Create rule**'a tıklayın. **Edit expression**'a tıklayın, kendi değerlerinizle şunu yapıştırın, eylem olarak **Block**'u seçin ve **Deploy**'a tıklayın:

```
http.host eq "coolify.example.com" and ip.src ne your-home-ip and not
starts_with(http.request.uri.path, "/.well-known/acme-challenge/")
```

Son kısım sertifikanın yenilenebilmesini sağlar. O olmazsa yenileme yaklaşık 3 ay sonra başarısız olur. Ev IP'niz değişirse bu kuralı da güncelleyin.

ADIM 8

Her şeyi Cloudflare'den geçirin

Bu adım önemli. Örnek kurulumda 7. adımdaki kural, doğrudan sunucunun IP adresine bağlanarak aşılabiliyordu. Docker ayrıca 8000 gibi başka portları da dışarı açıyor.

Şunu `/usr/local/sbin/cf-only.sh` olarak kaydedin ve `chmod 750` uygulayın. Adres listelerini cloudflare.com/ips ile karşılaştırın, çünkü değişebilirler.

```
#!/bin/bash
# Docker'ın açtığı web portlarına yalnızca Cloudflare erişebilsin.
set -u
CF4="173.245.48.0/20 103.21.244.0/22 103.22.200.0/22 103.31.4.0/22
141.101.64.0/18 108.162.192.0/18 190.93.240.0/20 188.114.96.0/20
197.234.240.0/22 198.41.128.0/17 162.158.0.0/15 104.16.0.0/13
104.24.0.0/14 172.64.0.0/13 131.0.72.0/22"
CF6="2400:cb00::/32 2606:4700::/32 2803:f800::/32 2405:b500::/32
2405:8100::/32 2a06:98c0::/29 2c0f:f248::/32"
WAN=$(ip -o route get 1.1.1.1 | sed -n 's/.* dev \([^ ]*\).*/\1/p')

apply() {
    local ipt=$1; shift
    $ipt -N CF-ONLY 2>/dev/null || $ipt -F CF-ONLY
    $ipt -A CF-ONLY -m conntrack --ctstate RELATED,ESTABLISHED -j RETURN
    for net in "$@"; do
      $ipt -A CF-ONLY -s "$net" -p tcp -m conntrack --ctorigdstport 80 -j RETURN
      $ipt -A CF-ONLY -s "$net" -p tcp -m conntrack --ctorigdstport 443 -j RETURN
    done
    $ipt -A CF-ONLY -j DROP
    $ipt -C DOCKER-USER -i "$WAN" -j CF-ONLY 2>/dev/null || \
      $ipt -I DOCKER-USER 1 -i "$WAN" -j CF-ONLY
}

apply iptables $CF4
apply ip6tables $CF6
```

Her yeniden başlatmadan sonra çalışması için `/etc/systemd/system/cf-only.service` dosyasını oluşturun:

```
[Unit]
Description=Allow only Cloudflare to reach Docker web ports
After=docker.service
Requires=docker.service
PartOf=docker.service

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStartPre=/bin/sleep 5
ExecStart=/usr/local/sbin/cf-only.sh

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

Sonra etkinleştirin:

```
systemctl daemon-reload
systemctl enable --now cf-only.service
```

Son olarak hPanel'de 8000 portu kuralını silin ve **Synchronize**'a tıklayın.

ADIM 9

Her yolu test edin

Her satırı deneyin; sunucuyu yeniden başlattıktan sonra da aynı sonuçları almalısınız:

Test	Beklenen sonuç
Kendi IP'nizden `https://coolify.example.com`	Coolify giriş sayfası
Aynı adres başka herhangi bir IP'den	403, Cloudflare engeller
Doğrudan sunucunun IP'sine, 443 portundan	Cevap yok
`http://203.0.113.10:8000`	Cevap yok
Anahtarla SSH	Çalışır
Şifreyle SSH	Reddedilir
Web siteniz ve iki yönde e-posta	Çalışır

Kontrol: Tablodaki her satır beklenen sonucu veriyor.

Sıradaki adımlar

Bir sonraki bölümde Coolify'da iki adımlı girişi açacağız, sunucu dışı yedeklemeyi kuracağız ve Odoo'yu `erp.example.com` adresine yükleyeceğiz.