Hostinger VPS Üzerinde Odoo ERP

Kurulum Kılavuzu

FB Software Solutions'tan adım adım bir eğitim kılavuzu. Hesabı, alan adını, web sitesini, e-postayı ve sunucuyu kuracak, işletme verisi sunucuya girmeden önce her şeyi güvenli hâle getireceksiniz.

İçindekiler

	Bu kılavuz nasıl kullanılır
Bölüm 1	Hostinger hesabı ve hPanel
Bölüm 2	Alan adı ve DNS
Bölüm 3	Web sitesi ve WordPress
Bölüm 4	Kurumsal e-posta
Bölüm 5	VPS
Bölüm 6	VPS'i güvenli hâle getirin
Bölüm 7	GitHub reposu
Bölüm 8	Gerçek veriden önce kontrol noktası
Ek A	Sunucunun dışında kalırsanız

Serinin devamında. Docker, Odoo ve PostgreSQL kurulumu, ERP adresi için HTTPS, Odoo sunucu ayarları, giden e-posta, gece yedekleri, modüller ve canlıya geçiş bu eğitimin sonraki bölümlerinde anlatılıyor.

Ekran görüntüleri hakkında. Hostinger ve GitHub panelleri İngilizce olduğu için ekran görüntüleri ve kalın yazılmış düğme adları panelde gördüğünüz gibi İngilizce bırakıldı.

Bu kılavuz nasıl kullanılır

Bölümleri sırayla izleyin. Her bölüm kısa bir kontrolle bitiyor; bir sonraki bölüme geçmeden önce bu kontrolü geçmelisiniz. Sıra önemli: sunucu, üzerine işletme verisi konmadan önce güvenli hâle getiriliyor.

Yer tutucular

Aşağıdaki her değer bir örnek. Nerede görürseniz görün, kendi değerinizle değiştirin.

Yer tutucu	Anlamı	Sizin değeriniz
`example.com`	Alan adınız	
`erp.example.com`	ERP'nizin adresi	
`203.0.113.10`	VPS'inizin genel IP adresi	
`your-vps`	VPS'inizin sunucu adı	
`deploy`	Root olmayan Linux kullanıcınız	
`your-account / your-project`	GitHub hesabınız ve reponuz	
`you@example.com`	E-posta adresiniz	
`your-home-ip`	Kendi internet bağlantınızın genel IP adresi	

Ekran görüntülerinde de aynı yer tutucular kullanılıyor; kırmızı kutular bakmanız gereken yeri gösteriyor. Hostinger panelini sık değiştiriyor, bu yüzden bir düğmenin yeri değişmiş olabilir. Aynı kelimeleri arayın.

Önce verilmesi gereken dört karar

Başlamadan önce bu soruları cevaplayın, çünkü her biri kurulumu değiştiriyor.

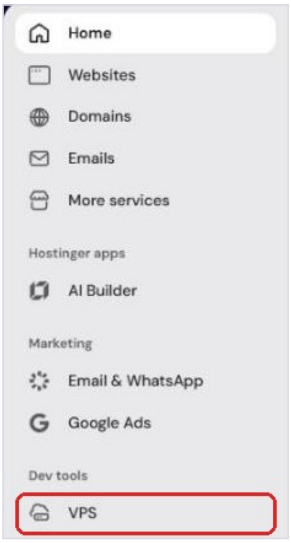
1. **Odoo sürümü ve paketi.** Community ve Enterprise'ın kurulumu ve lisans maliyeti farklı.
2. **Kullanıcı sayısı.** Odoo'nun worker sayısını bu belirliyor.
3. **Dış yedekler.** Yedekler nerede duracak ve depolamayı kim ödeyecek?
4. **Kodun sahipliği.** Teslimde kod kimin olacak, repo müşterinin hesabına taşınacak mı?

BÖLÜM 1

Hostinger hesabı ve hPanel

Hedef: bütün hizmetleri tek bir hesapta bulabiliyorsunuz ve hesabın sahibi doğru kişi.

hPanel, Hostinger'ın kontrol panelidir: hpanel.hostinger.com. Bu kılavuzdaki her şey kenar çubuğunda: **Websites**, **Domains**, **Emails** ve **Dev tools** altında **VPS**.



1. Hostinger hesabını, işletme sahibinin kontrol ettiği bir e-posta adresiyle açın.
2. Hesapta iki adımlı doğrulamayı açın.
3. VPS'i, web hosting'i, alan adını ve e-postayı bu tek hesapta satın alın; böylece faturalar ve yenilemeler bir arada kalır.
4. Bir müşteri için kuruyorsanız hizmetler müşterinin hesabında kalsın. Şifre yerine yönetici erişimi isteyin. Bu erişimi kullanırken hPanel, değişikliklerin sizin değil onların hesabına uygulandığını söyleyen bir uyarı gösterir.
5. Her hizmette otomatik yenilemenin açık olduğunu kontrol edin ve müşteri için her yenileme tarihini ve fiyatını not edin.

> **API anahtarları yalnızca kendi hesaplarını görür.** Sizin hesabınızda oluşturulan bir anahtar, müşterinin hesabındaki VPS'i listelemez. Sunucu işlerini SSH ile yapmayı planlayın; müşteriden anahtarı yalnızca API'ye gerçekten ihtiyacınız varsa isteyin.

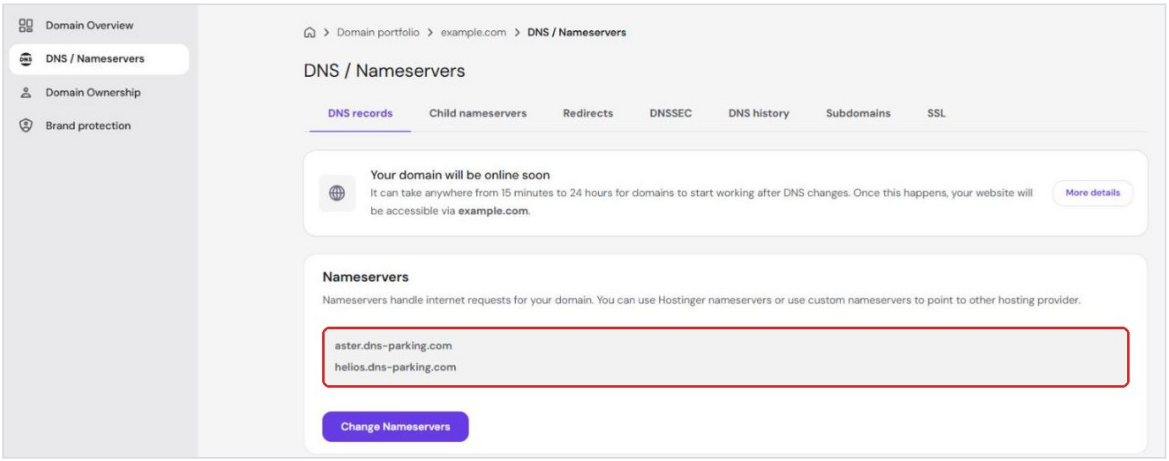
Kontrol: Websites, Domains, Emails ve VPS bölümlerini açabiliyorsunuz ve her birinin ne zaman yenileneceğini biliyorsunuz.

BÖLÜM 2

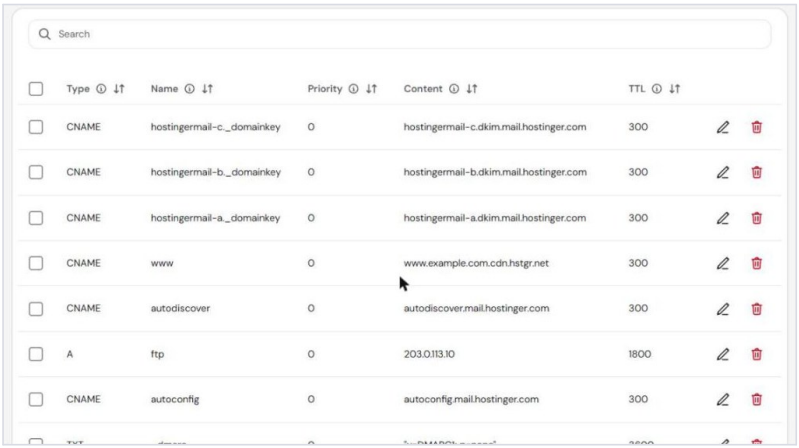
Alan adı ve DNS

Hedef: alan adı aktif ve DNS kayıtlarını okuyabiliyorsunuz.

1. **Domains**'i açın, alan adınızın yanındaki **Manage**'e tıklayın.
2. Durumun **Active** olduğunu ve otomatik yenilemenin açık olduğunu doğrulayın.
3. **DNS / Nameservers**'ı açın. Değiştirmek için bir nedeniniz yoksa Hostinger ad sunucularını olduğu gibi bırakın.



DNS records sekmesi bütün kayıtları listeler. Web sitesi, e-posta ve sunucu farklı kayıtlara bağlıdır:



Kayıt	Ne için	Dokunulur mu?
`@` için A, `www` için CNAME	Herkese açık web sitesi	Hayır
MX	Gelen e-posta	Hayır
SPF ve `_dmarc` için TXT	E-posta güvenilirliği	Sadece Bölüm 4'te
`hostingermail-*._domainkey` için CNAME	DKIM e-posta imzası	Hayır

Kayıt	Ne için	Dokunulur mu?
`erp` için A	ERP'niz	ERP için HTTPS kurarken siz eklersiniz

> **Alan adının kökünü (`@`) ya da `www`'yi VPS'e yönlendirmeyin.** Web sitesi hosting'de kalır. VPS'e yalnızca `erp` alt alan adı gider.

İsteğe bağlı güçlendirme: **DNSSEC** sekmesinden DNSSEC'i açın ve bir CAA kaydı ekleyin. Devam etmek için ikisi de gerekli değil.

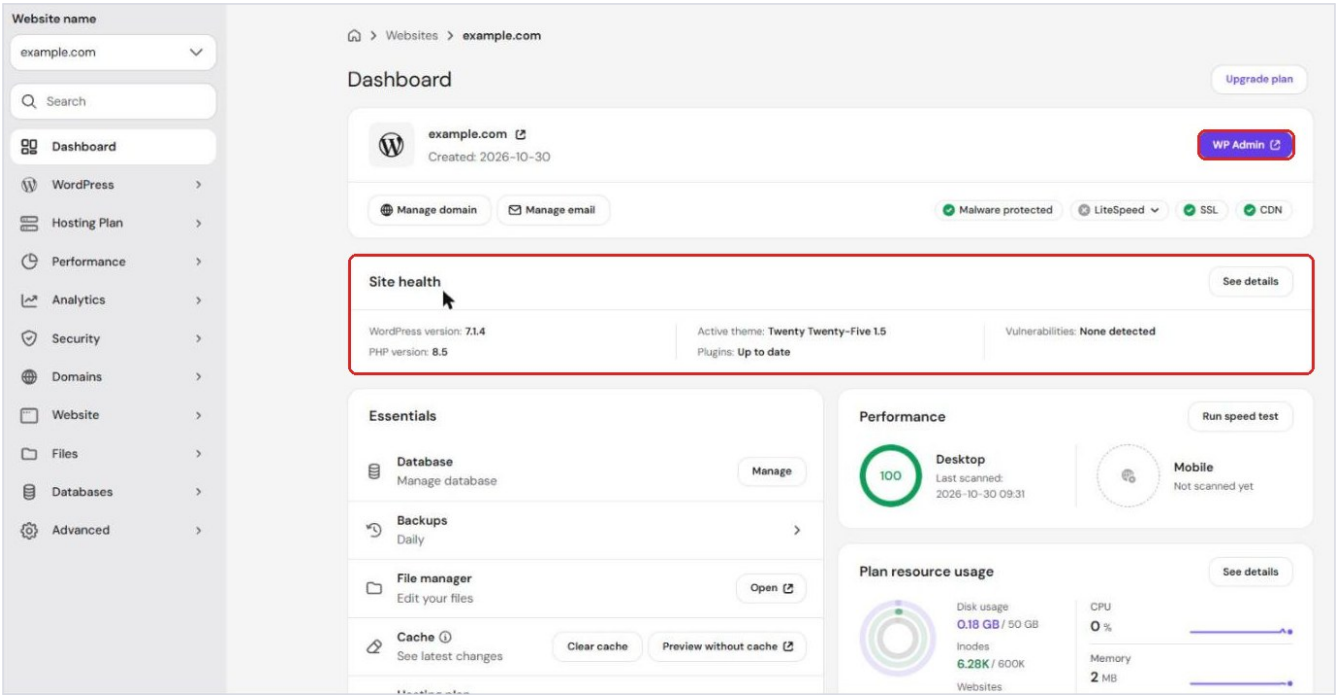
Kontrol: durum Active ve listede MX ile `_dmarc` kayıtlarını bulabiliyorsunuz.

BÖLÜM 3

Web sitesi ve WordPress

Hedef: web sitesi sağlıklı ve ERP'den ayrı.

Websites'i, sonra sitenizi açın. Panel; WordPress ve PHP sürümlerini, SSL'i, kötü amaçlı yazılım korumasını, yedekleri ve hızı tek yerde gösterir.



1. **Site health** altında güvenlik açığı olmadığını ve eklentilerin güncel olduğunu doğrulayın.
2. SSL rozetinin yeşil olduğunu, `http://example.com` ve `www.example.com` adreslerinin `https://example.com`'a yönlendiğini doğrulayın.
3. **Backups**'ın günlük bir zamanlama gösterdiğini doğrulayın. Yeni bir sitede henüz yedek olmayabilir; bir iki gün sonra tekrar bakın.
4. **WP Admin**'i açın, **Settings** ve ardından **General**'a gidin; saat diliminizi ve sloganınızı ayarlayın.
5. Site hazır olduğunda **Settings** ve ardından **Reading** altında gerçek bir ana sayfa seçin.

Yayına almadan önce

Konu	Ne yapılmalı
Bir site için iki veritabanı	`wp-config.php` içinde adı geçeni bulun; diğerini ancak yedek aldıktan sonra silin
Herkese açık kullanıcı API'si	`https://example.com/wp-json/wp/v2/users` yazar isimlerini gösterir. Aşağıdaki kodla ziyaretçilere kapatın

Konu	Ne yapılmalı
Uzun HTML önbelleği	HTML için 7 günlük tarayıcı önbelleği, geri gelen ziyaretçilere eski sayfaları gösterir. Süreyi kısaltın
Güvenlik başlıkları	HSTS ve benzeri başlıkları ekleyin. `curl -I https://example.com` ile kontrol edin

Bunu temanızın `functions.php` dosyasına ya da bir kod parçacığı eklentisine ekleyin:

```
add_filter('rest_endpoints', function ($endpoints) {
    if (!is_user_logged_in()) {
        unset($endpoints['/wp/v2/users']);
        unset($endpoints['/wp/v2/users/(?P<id>[\d]+)']);
    }
    return $endpoints;
});
```

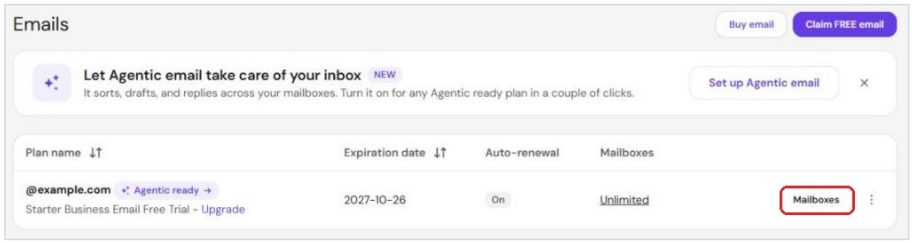
Kontrol: site HTTPS ile açılıyor ve oturum kapalıyken kullanıcı API'si adresi hata veriyor.

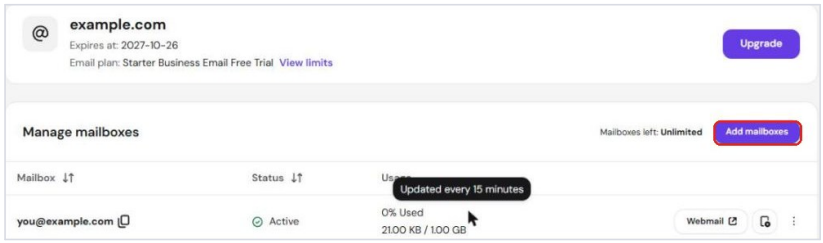
BÖLÜM 4

Kurumsal e-posta

Hedef: e-posta çalışıyor ve ERP'nin kendi e-posta kutusu var.

Emails'i açın, alan adınızın yanındaki **Mailboxes**'a tıklayın.





1. Alan adı kurulumunun **Connect domain: Completed** gösterdiğini doğrulayın.
2. Günlük kullanım kutusunu açın, örneğin `info@example.com`.
3. **Add mailboxes**'a tıklayın ve ERP için ayrı bir kutu açın, örneğin `erp@example.com`. Bu kutuda bir sorun olursa kişisel e-postanız etkilenmez.
4. Odoo'nun e-posta ayarı için giden sunucuyu not edin: `smtp.hostinger.com`, port 465 ya da 587.
5. **View limits** ile paketinizin gönderim sınırlarını kontrol edin ve ERP'den beklediğiniz e-posta hacmiyle karşılaştırın.
6. Ücretsiz deneme süresi varsa bitiş tarihini not edip müşteriye bildirin.

DMARC'ı sıkılaştırın

DMARC, kontrollerden geçemeyen e-postalara ne yapılacağını diğer e-posta sunucularına söyler. Yeni bir alan adı genellikle rapor olmadan `p=none` ile başlar. `_dmarc` TXT kaydını aşama aşama düzenleyin:

1. Bir rapor adresi ekleyin: `v=DMARC1; p=none; rua=mailto:you@example.com`
2. Raporları birkaç hafta okuyun ve gerçek e-postalarınızın kontrolden geçtiğini doğrulayın.
3. Sıkılaştırın: `v=DMARC1; p=quarantine; rua=mailto:you@example.com`

> **ERP e-postasını asla doğrudan VPS'ten göndermeyin.** SPF kaydı yalnızca Hostinger'ın e-posta sunucularına izin verir; doğrudan gönderilen e-posta spam'e düşer ya da reddedilir. Her zaman `smtp.hostinger.com` üzerinden gönderin.

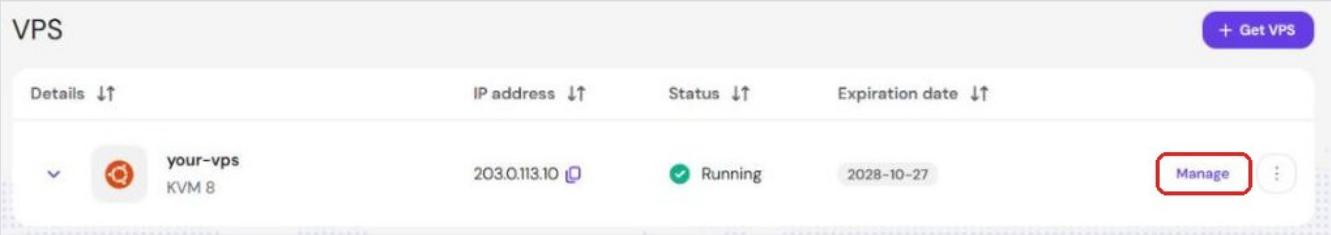
Kontrol: her kutudan dışarıdaki bir adrese e-posta gönderin ve cevap verin.

BÖLÜM 5

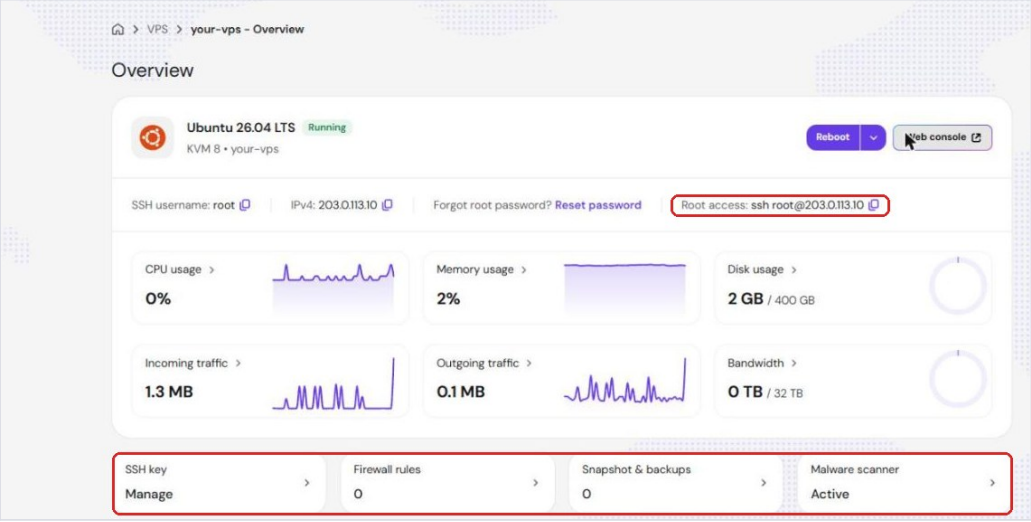
VPS

Hedef: bir şeyi değiştirmeden önce elinizde ne olduğunu biliyorsunuz.

VPS'i açın, sonra **Manage**'e tıklayın.



Overview sayfası ana üssünüz. Alt satır, Bölüm 6'da düzelteceğiniz üç şeyi gösterir: SSH anahtarı, güvenlik duvarı kuralları ve snapshot ile yedekler.



1. IPv4 adresini ve SSH kullanıcı adını not edin.
2. İşletim sistemini doğrulayın. Örnek kurulum Ubuntu 26.04 LTS kullanıyor.
3. Kaynakları doğrulayın. Örnek kurulum KVM 8 paketini kullanıyor (8 CPU, 32 GB RAM, 400 GB disk); bu, başlangıçtaki bir Odoo için fazlasıyla yeterli. Paketi kullanıcı sayınıza göre seçin.
4. **Web console** düğmesini aklınızda tutun. Tarayıcınızda bir terminal açar ve SSH çalışmadığında bile çalışır.

> **Ubuntu yeni, bu yüzden Docker kullanın.** Odoo'nun yepyeni bir Ubuntu sürümüne desteği geriden gelebilir. Odoo'yu Docker içinde çalıştırınca ana işletim sisteminin önemi çok azalır.

Kontrol: IP adresi elinizde ve durum Running gösteriyor.

BÖLÜM 6

VPS'i güvenli hâle getirin

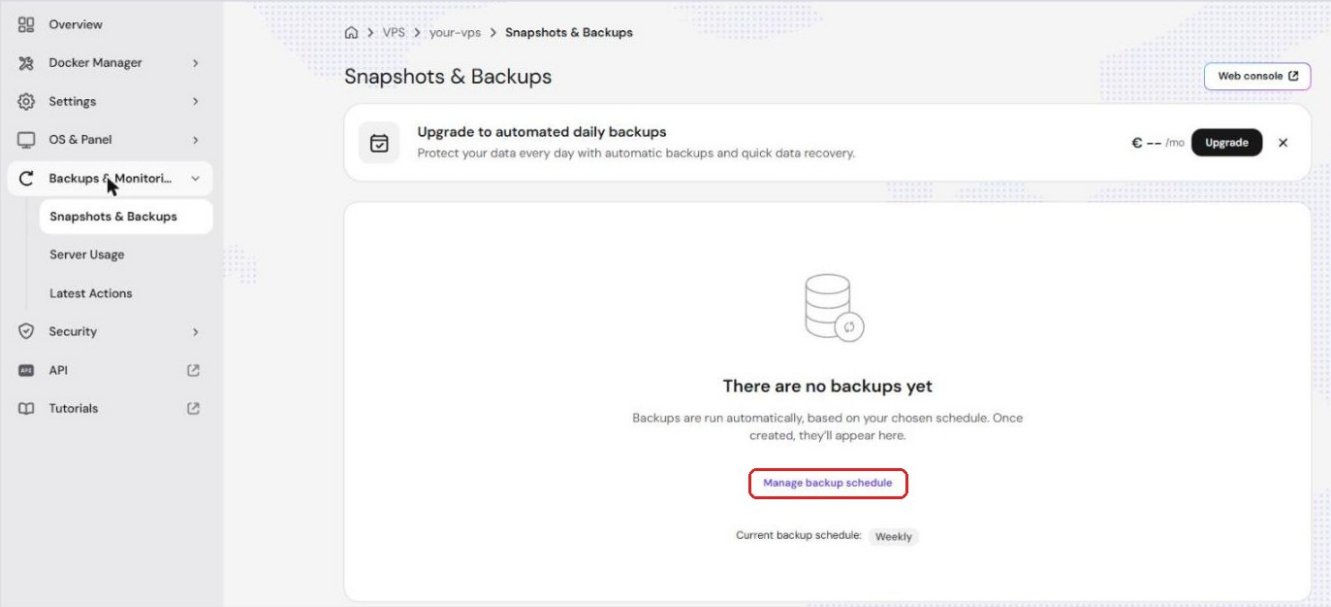
Hedef: yalnızca sizin anahtarınız giriş yapabiliyor, yalnızca 22, 80 ve 443 portları açık ve bir hatadan geri dönebiliyorsunuz.

Bu adımları sırayla yapın. Yepyeni bir sunucu 0 güvenlik duvarı kuralı, SSH anahtarı yok ve 0 yedek gösterebilir. Bu normal, ama işletme verisi için güvenli değil.

> **Erişimi değiştirirken oturumu açık tutun.** İkinci bir pencere yeni ayarın çalıştığını kanıtlayana kadar çalışan SSH pencerenizi kapatmayın. Yine de dışarıda kalırsanız Ek A'ya bakın.

6.1 Snapshot alın

Backups & Monitoring, ardından **Snapshots & Backups**'ı açın ve bir snapshot oluşturun. Sonraki bir adım ters giderse geri dönebilirsiniz.



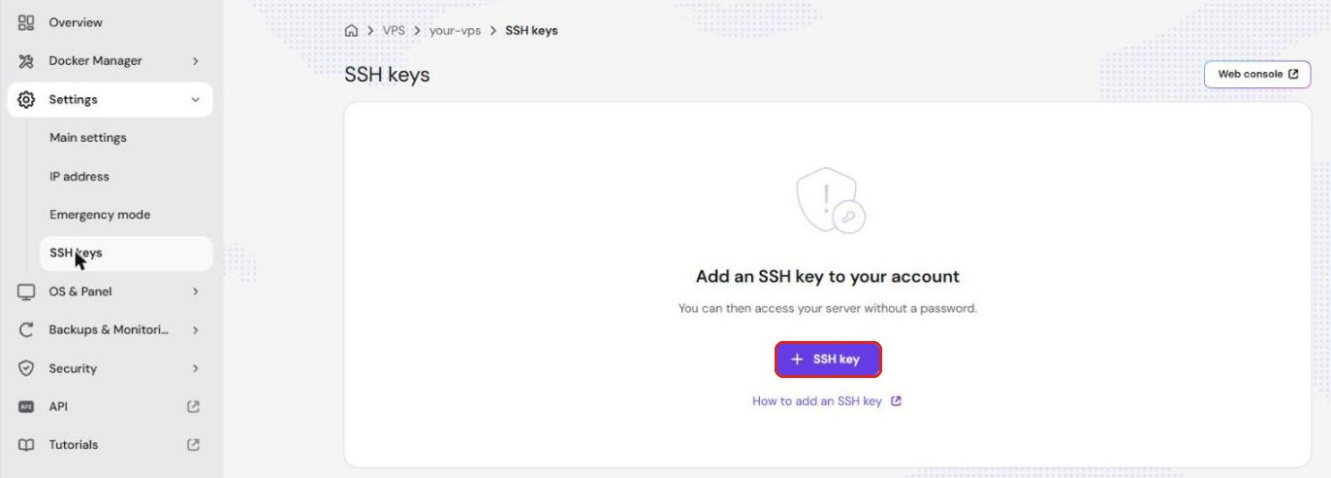
6.2 SSH anahtarı oluşturun ve ekleyin

Kendi bilgisayarınızda, PowerShell ya da Terminal'de şunu çalıştırın:

```
ssh-keygen -t ed25519 -C "you@example.com"
cat ~/.ssh/id_ed25519.pub
```

Sorulduğunda bir parola belirleyin. `.pub` dosyası açık anahtarınızdır ve paylaşmak güvenlidir. `.pub` olmayan dosya ise özel anahtarınızdır: onu asla bir sunucuya, bir sohbete ya da bir repoya kopyalamayın.

hPanel'de **Settings**, ardından **SSH keys**'i açın, **+ SSH key**'e tıklayın ve açık anahtarı yapıştırın.



Deneyin:

```
ssh root@203.0.113.10
```

6.3 Root olmayan bir kullanıcı oluşturun

Root olarak giriş yapın ve şunları çalıştırın; isterseniz `deploy` yerine başka bir ad kullanın:

```
adduser deploy
usermod -aG sudo deploy
rsync --archive --chown=deploy:deploy ~/.ssh /home/deploy
```

İkinci bir pencerede yeni kullanıcının giriş yapıp sudo kullanabildiğini doğrulayın:

```
ssh deploy@203.0.113.10
sudo whoami
```

Son komut `root` yazdırmalı.

6.4 Şifreyle girişi ve root girişini kapatın

`deploy` olarak bir ayar dosyası oluşturun. Adı `00-` ile başlıyor ki ilk o okunsun, çünkü SSH bulduğu ilk değeri kullanır:

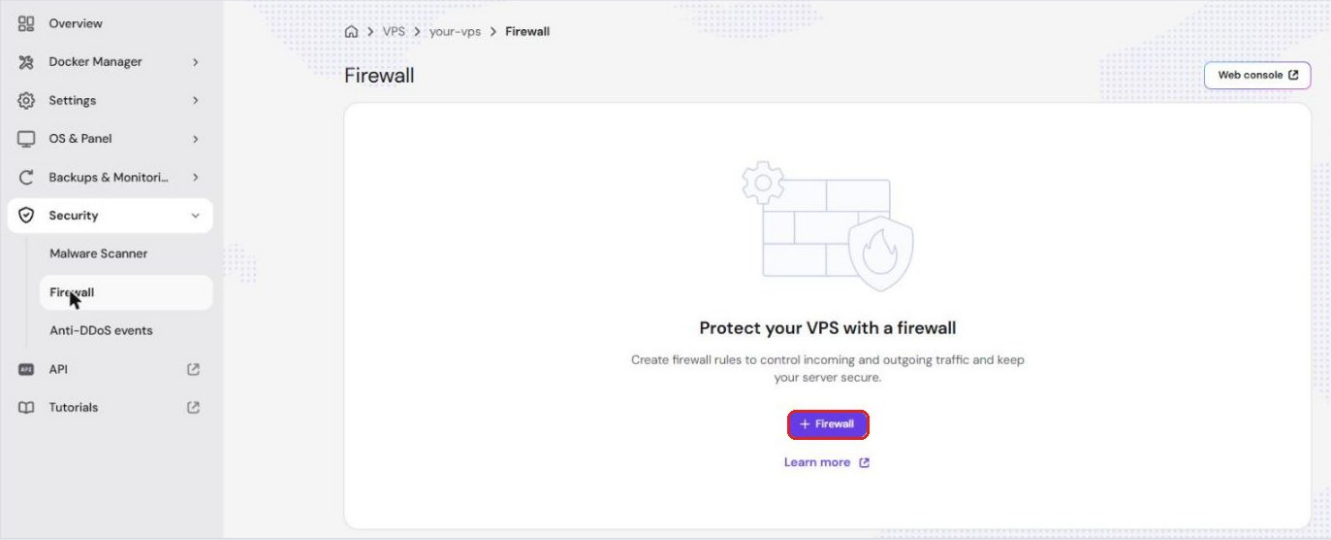
```
sudo tee /etc/ssh/sshd_config.d/00-hardening.conf > /dev/null <<'EOF'
PasswordAuthentication no
KbdInteractiveAuthentication no
PermitRootLogin no
EOF
sudo sshd -t
sudo systemctl reload ssh
sudo sshd -T | grep -E \
  '^(passwordauthentication|kbdinteractiveauthentication|permitrootlogin)'
```

`sshd -t` hiçbir şey yazdırmamalı, son komut da üçünün de `no` olduğunu göstermeli. Sonra ikinci bir pencereden deneyin. Bu ikisi de reddedilmeli:

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

6.5 Güvenlik duvarını kurun

Security, ardından **Firewall**'u açın ve **+ Firewall**'a tıklayın. Bir ad verin ve şu kuralları ekleyin:



İşlem	Protokol	Port	Kaynak
Accept	TCP	22	Yalnızca `your-home-ip`
Accept	TCP	80	Her yerden (Anywhere)
Accept	TCP	443	Her yerden (Anywhere)

Güvenlik duvarını etkinleştirin, sonra kendi bilgisayarınızdan PowerShell ile deneyin. Port 22 başarılı olmalı, port 8069 başarısız olmalı:

```
Test-NetConnection 203.0.113.10 -Port 22
Test-NetConnection 203.0.113.10 -Port 8069
```

8069 (Odoo) ve 5432 (PostgreSQL) portlarını asla internete açmayın. Odoo'ya trafik yalnızca 443 üzerindeki HTTPS proxy'den ulaşır.

Ev IP adresiniz değişirse SSH çalışmayı durdurur. hPanel'e girip kuralı güncelleyin. Başka hiçbir şey etkilenmez.

Yalnızca ufw'ye güvenmeyin. Docker port yayınlarken ufw'yi atlayabilir; bu yüzden hPanel güvenlik duvarını kullanın, Odoo ve PostgreSQL'i iç Docker ağlarında tutun.

6.6 Otomatik güvenlik güncellemelerini açın

```
sudo apt update && sudo apt full-upgrade -y
sudo apt install -y unattended-upgrades
sudo dpkg-reconfigure -plow unattended-upgrades
cat /etc/apt/apt.conf.d/20auto-upgrades
```

Çıktıdaki iki satır da `"1";` ile bitmeli. Ardından `/var/run/reboot-required` dosyası varsa sunucuyu hPanel'den yeniden başlatın.

6.7 Yedeklerinizi planlayın

hPanel'in yedek zamanlaması bir ERP için yeterli değil. Haftalık bir yedek, 7 güne kadar işin kaybolması demek. hPanel yedeklerini bir güvenlik ağı olarak tutun; eğitimin ilerleyen bölümlerinde her gece sunucu dışına alınan kopyalar ekleyeceksiniz.

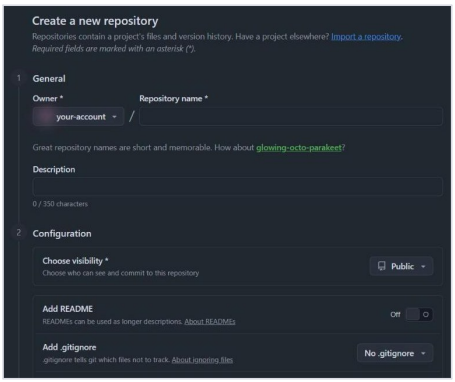
Her büyük değişiklikten önce snapshot alın. Kötü amaçlı yazılım tarayıcısı varsayılan olarak açıktır; otomatik temizleme isteğe bağlıdır.

Kontrol: Overview sayfası bir SSH anahtarı, 0'dan fazla güvenlik duvarı kuralı ve en az bir snapshot gösteriyor.

BÖLÜM 7

GitHub reposu

Hedef: sunucuyu yeniden kurmak için gereken her şey özel bir repoda ve içinde hiçbir gizli bilgi yok.



1. github.com/new adresini açın.
2. Repoya bir ad verin ve görünürlüğü **Private** yapın. Varsayılan Public olduğu için bunu her seferinde kontrol edin.
3. İlk gerçek commit'ten önce bir `.gitignore` ekleyin:

```
.env
*.dump
*.sql
*.sql.gz
filestore/
backups/
```

Sonraki bölümlerin dolduracağı bu yapıyı koruyun:

Yol	İçinde ne var
`docker-compose.yml`	Odoo, PostgreSQL ve proxy konteynerleri
`.env.example`	Sahte değerlerle ayar adları. Gerçek `.env` yalnızca sunucuda durur
`addons/`	Kendi Odoo modülleriniz
`docs/`	Bu kılavuz ve kendi notlarınız

Teslimde kodun kime ait olacağını yazılı olarak kararlaştırın. Kurulum sırasında reponun kişisel hesabınızda olması sorun değil; daha sonra devredilebilir.

> **Bir şifre GitHub'a giderse şifreyi değiştirin.** Dosyayı silmek onu geçmişten silmez.

Kontrol: repo Private rozeti gösteriyor ve `.env`, `.gitignore` içinde listeleniyor.

BÖLÜM 8

Gerçek veriden önce kontrol noktası

Her kutu işaretlenmeden bu sayfadan ileri geçmeyin.

- [ ] Hostinger ve GitHub'da iki adımlı doğrulama açık
- [ ] Bütün hizmetlerde otomatik yenileme açık ve tarihler not edildi
- [ ] Giriş, root olmayan bir kullanıcıyla ve SSH anahtarıyla çalışıyor
- [ ] Şifreyle giriş ve root girişi reddediliyor
- [ ] hPanel güvenlik duvarı yalnızca 22, 80 ve 443'e izin veriyor; 22 yalnızca sizin IP'nize açık
- [ ] 8069 ve 5432 portlarına dışarıdan ulaşılamıyor
- [ ] Otomatik güvenlik güncellemeleri açık
- [ ] Bir snapshot var
- [ ] ERP'ye özel bir e-posta kutusu var
- [ ] Repo özel ve içinde gizli bilgi yok
- [ ] Kılavuzun başındaki dört karar cevaplandı

EK A

Sunucunun dışında kalırsanız

Sorun	Çözüm
SSH zaman aşımına uğruyor	Ev IP adresiniz büyük olasılıkla değişti. hPanel güvenlik duvarındaki port 22 kuralını güncelleyin
Permission denied (publickey)	VPS Overview sayfasında **Web console**'u açın. `/home/deploy/.ssh/authorized_keys` içindeki anahtarı kontrol edin
SSH ayarları bozuldu	**Settings**, ardından **Main settings** altında **Reset SSH configuration**'ı kullanın. Sonra 6.4'ü tekrarlayın
Güvenlik duvarı kuralları sizi engelledi	Kuralları **Security**, ardından **Firewall** altında düzenleyin. Sorun sunucudaki ufw ya da iptables ise **Settings**, ardından **Main settings** altında **Reset firewall configuration**'ı kullanın
Hiçbir şey çalışmıyor	Snapshot'ı **Snapshots & Backups**'tan geri yükleyin. Snapshot'tan sonra yapılan her değişiklik kaybolur