

TUTORIAL UJIKOM TKJ 2026

JUNIOR TECHNICAL SUPPORT PUSAT DATA

TUTORIAL PRAKTIK: KELOMPOK PEKERJAAN 1

Durasi: 90 Menit
Fokus: Identifikasi, Konfigurasi Network, Pembuatan Template, Inventarisasi, dan Monitoring.

 **PENTING SEBELUM MULAI:**
Ganti semua tulisan **xx** dengan Nomor Meja / Nomor Urut Anda.
Ganti semua tulisan **y** dengan Nomor Lab tempat Anda ujian / latihan
Contoh: Jika nomor meja/urut 05 dan nomor lab 1 (LAB TKJ 1),

192.168.25 Y .1 XX /24	192.168.251.1 05 /24
1 XX .10 Y .10 Y .101/24	105 .101.101.101/24

SKEMA IP ADDRESS

IP ADDRESS VM / HYPERVISOR

VM / Proxmox	IP Address	Layanan Utama
Proxmox Host (vmbr0)	192.168.25 Y .1 XX /24	Hypervisor, NAT, DNS
Proxmox Host (vmbr1)	1 XX .10 Y .10 Y .1/24	Private Gateway
VM 101 (web)	1 XX .10 Y .10 Y .101/24	Apache2, HestiaCP
VM 102 (sec-gw)	1 XX .10 Y .10 Y .102/24	Nginx Proxy, WireGuard

IP ADDRESS CLIENT (WINDOWS)

IP ADDRESS	192.168.25 Y .2 XX /24
GATEWAY	192.158.25 Y .254
DNS SERVER	192.168.25 Y .1 XX

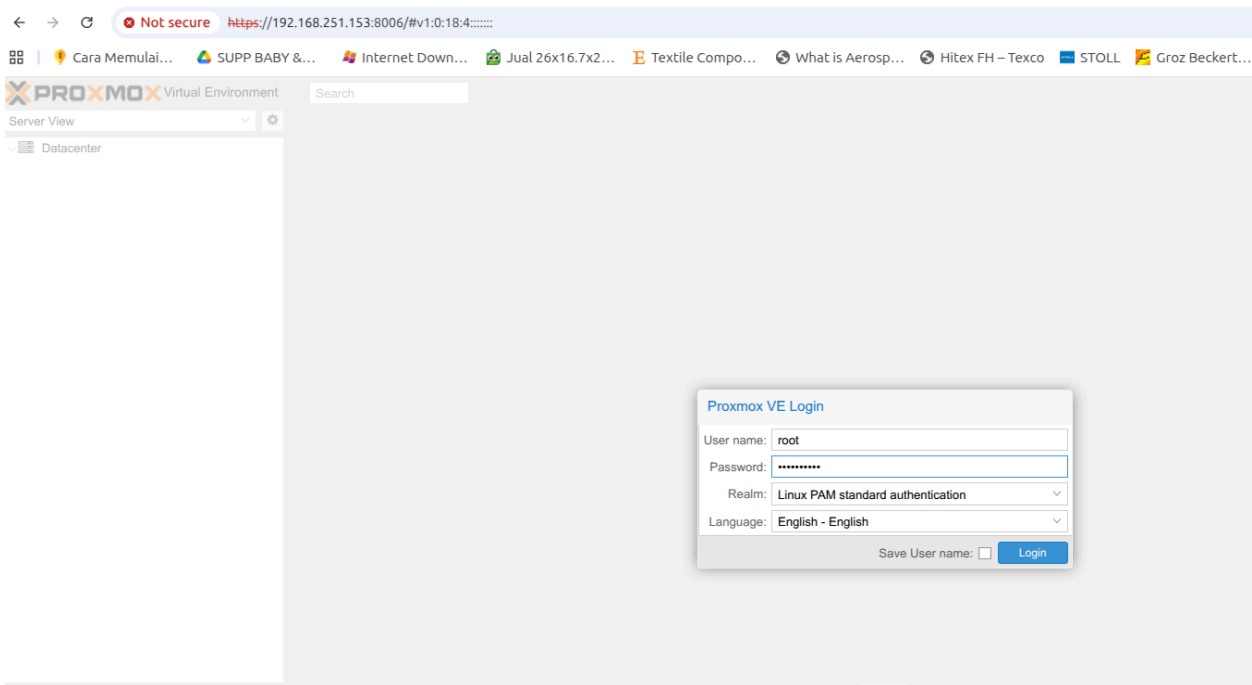
USER DAN PASSWORD PROXMOX

USER	root
PASSWORD	ujikom2026

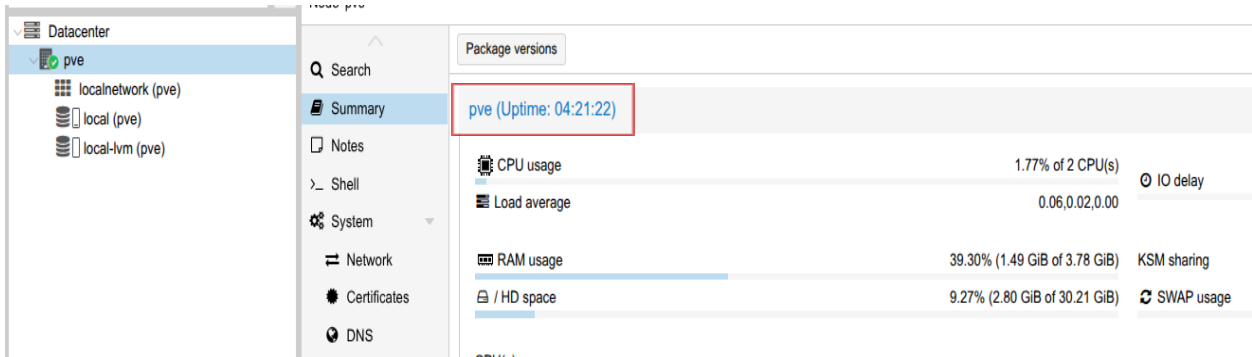
Dalam contoh tutorial ini no urut yang digunakan **53**, dan berada di **Lab TKJ 1**, jadi **XX = 53**, **Y = 1**

LANGKAH 1: Mengidentifikasi Perangkat & Kesehatan Node Proxmox

- 1. Akses Proxmox GUI:
 - o Buka browser di PC Client.
 - o Ketik alamat: `https://192.168.251.153:8006` (Abaikan peringatan "Your connection is not private", klik Advanced → Proceed).
 - o Login dengan User: `root` dan Password: `ujikom2026`.



- 2. Cek Kesehatan Node 'pve':
 - o Klik node `pve` di panel kiri.
 - o Klik tab Summary. Pastikan statusnya *running*, dan perhatikan nilai CPU usage, Memory usage, serta Root Disk usage.



Cara Memastikan Node 'pve' Berjalan Normal / Running di Proxmox

- 1. Cek Status Node di Panel Kiri
 - o Lihat panel kiri (Server View)
 - o Node `pve` harus muncul dengan ikon server berwarna hijau (✅)
 - o Jika berwarna merah atau ada tanda seru (⚠️), berarti ada masalah.

2. Cek Tab "Summary"

- Klik node `pve`
- Lihat tab Summary di panel kanan
- Pastikan informasi berikut muncul dengan benar:
 - Status: `running` atau `online`
 - Uptime: menunjukkan waktu server sudah berjalan (misal: 2 days 05:30:12)
 - CPU usage: ada persentase penggunaan (tidak stuck di 0% atau error)
 - Memory usage: ada nilai RAM yang terpakai
 - Root Disk: ada informasi penggunaan storage

3. Identifikasi Jaringan:

- Klik node `pve` → tab Network.
- Amati sudah terdapat `vmbr0` (caranya dapat dilihat di **vps-proxmox2026-2.pdf** pada halaman 5)

LANGKAH 2: Konfigurasi Network Proxmox (vmbr0 & vmbr1)

1. Konfigurasi `vmbr0` (Publik):
 - Klik `pve` → Network → Pilih `vmbr0` → Klik Edit.
 - Isi IPv4/CIDR: `192.168.25Y.1XX/24`
 - Isi Gateway (IPv4): `192.168.25Y.254`
 - Klik OK.
2. Konfigurasi DNS Server:
 - Klik `pve` → DNS → Klik `Edit`.
 - Isi DNS Server 1: `192.168.25Y.254`
 - Klik OK.
3. Membuat `vmbr1` (Private):
 - Klik tombol Create (di atas tabel Network) → Pilih Linux Bridge.
 - Name: `vmbr1`
 - IPv4/CIDR: `1XX.10Y.10Y.1/24`
 - Klik Create.
4. Apply Configuration:
 - Klik tombol Apply Configuration di bagian atas.
 - Klik Yes pada kotak konfirmasi.
 - Verifikasi: Pastikan kolom "Active" untuk `vmbr0` dan `vmbr1` bernilai Yes.

[Untuk lengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 5 - 7 dengan menyesuaikan IP Address nya]

LANGKAH 3: Membuat Master Template VM (Cloud-Init)

1. Create VM:

- Klik Create VM (pojok kanan atas).
- General: VM ID: `100`, Name: `Debian12-template`. Klik *Next*.
- OS: Pilih Do not use any media. Klik *Next*.
- System: Graphic Card: `Default`, Centang QEMU Agent. Klik *Next*.
- Disks: Hapus disk default (klik icon tempat sampah). Klik *Next*.
- CPU: Default (1 Core). Klik *Next*.
- Memory: `512 MB`. Klik *Next*.

- o Network: Bridge: **vmb1**, Model: **virtio**. Klik **Next** → **Finish**.

[Untuk selengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 8 - 11]

2. Download, Set Serial Console, Resize Disk & Import Disk (via Shell Proxmox):
 - o Klik node **pve** → **Shell**. Ketik perintah berikut satu per satu

```
mkdir -p /var/lib/vz/template/iso
cd /var/lib/vz/template/iso
wget http://192.168.251.252/proxmox/debian-12-generic-amd64.qcow2
qm set 100 --serial0 socket --vga serial0
qemu-img resize debian-12-generic-amd64.qcow 10G
qm importdisk 100 /var/lib/vz/template/iso/debian-12-generic-amd64.qcow2 local-lvm
```

[Untuk selengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 12 - 13]

3. Attach Disk & Boot Order (via GUI):
 - o Klik **VM 100(Debian12- template)** → **Hardware** → **Add** → **Cloudinit Drive**
 - o Bus/Device : **scsi** → **Storage:local-lvm** → Klik **Add**
 - o Langkah berikutnya klik **Unused Disk 0** → Klik **Edit** → **centang Discard** → **Add**.
 - o Klik **Options** → **Boot Order** → **Edit** → **Centang scsi0** (pindahkan ke paling atas) → **OK**.

[Untuk selengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 14 - 15]

4. Konfigurasi Cloud-Init:
 - o Klik **VM 100 (Debian12- template)** → **Cloud-Init** → **Edit**.
 - o User: **root**
 - o Password: **123456**
 - o DNS Server: **1xx.10y.10y.1**
 - o Klik **Regenerate Image**.

[**vps-proxmox2026-2.pdf**, halaman 16]

5. Convert to Template:
 - o Klik kanan pada **VM 100 (Debian12-template)** di panel kiri → Pilih **Convert to template**.

[**vps-proxmox2026-2.pdf**, halaman 16]

LANGKAH 4: Melakukan Inventarisasi Aset Cloud

- Memerikan Notes/Tag:
 - o Klik **VM 100 (Debian12-template)**.
 - o Klik icon Notes (gambar pensil  di pojok kanan atas panel).

Virtual Machine 100 (Debian12-template) on node 'pve'

No Tags 

- o Klik **Add Tag**

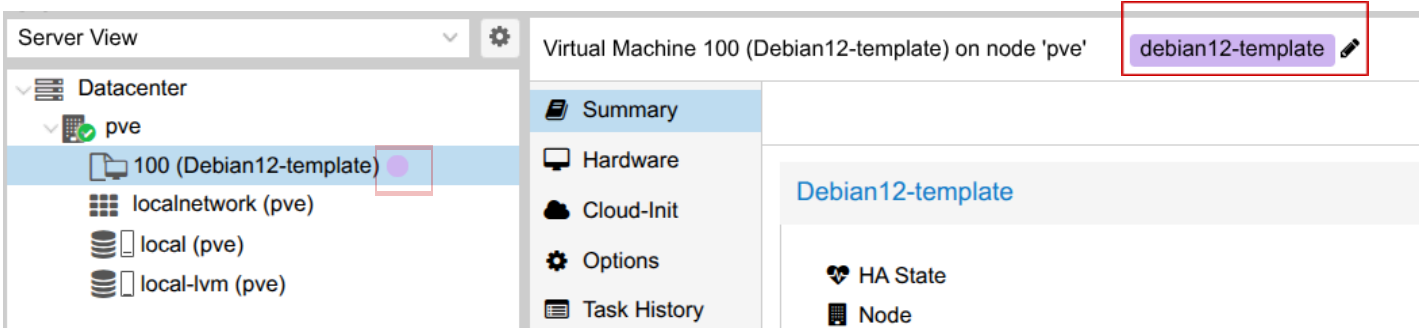
No Tags



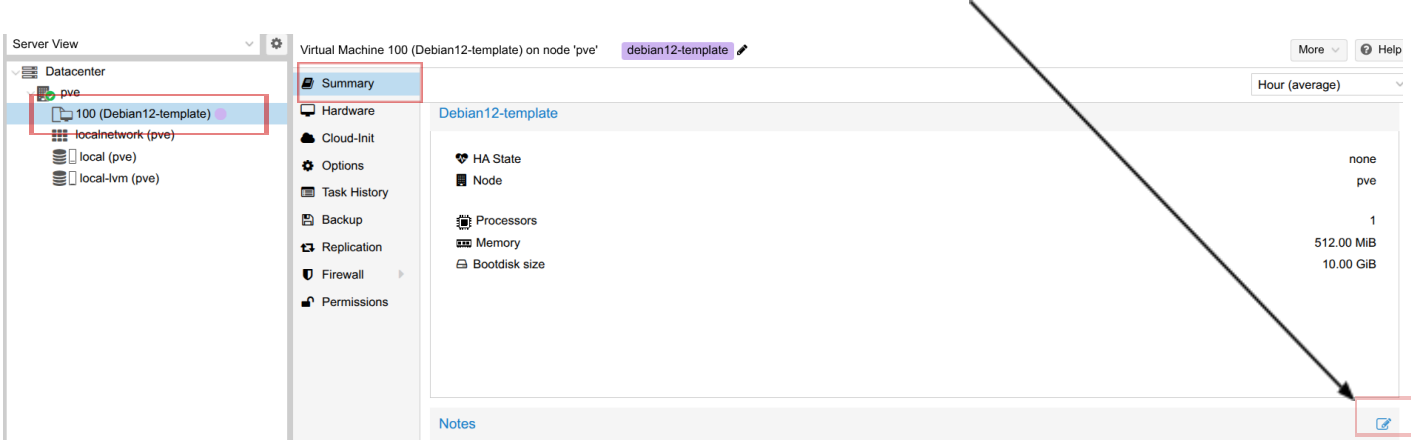
- o Isi Notes **“Debian12-template”** kemudian klik tanda **centang**



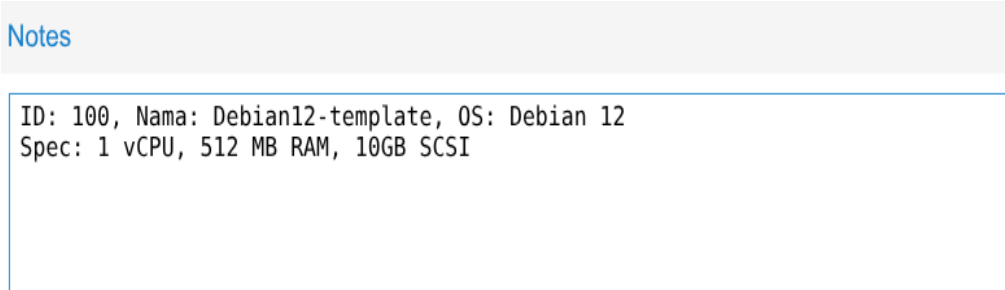
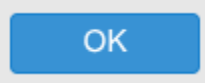
- Hasil akhirnya sebagai berikut



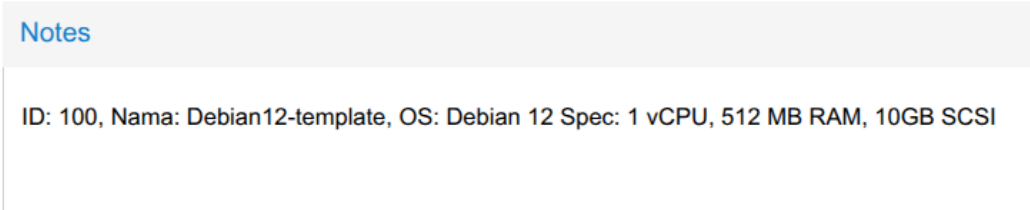
- Menambahkan Label :
 - Klik VM 100 (Debian12-template) → Summary → Edit notes



- Isikan label seperti dibawah ini, setelah selesai kemudian klik



- Hasil Akhir sebagai berikut:



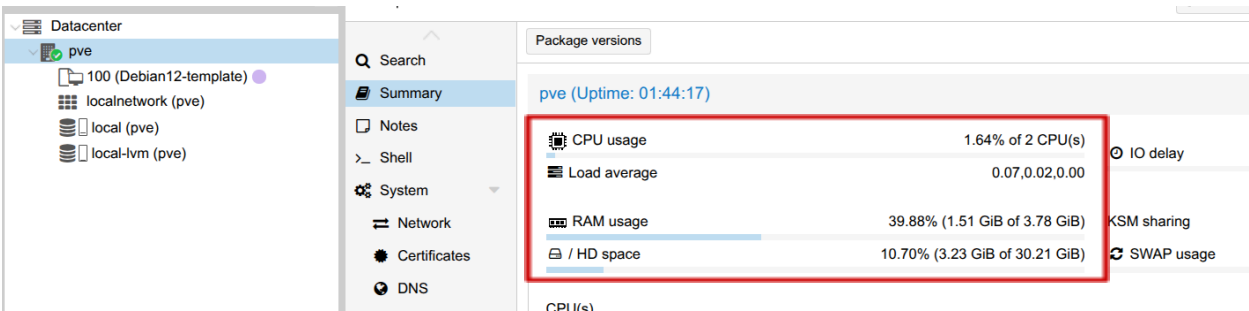
- Kelompokkan di Storage:
 - Pastikan file `.qcow2` terlihat di kategori *Disk image* atau *ISO image*.

```
root@pve:~# ls -l /var/lib/vz/template/iso/
total 436024
-rw-r--r-- 1 root root 446496928 Sep  2 11:27 debian-12-generic-amd64.qcow2
root@pve:~#
```

- Buat Dokumen Inventarisasi:
 - Buka file LEMBAR KERJA ASESI
 - Isikan informasi berisi: ID VM, Nama, vCPU, RAM, Storage, Network, dan Status, pada tabel **Inventarisasi Hardware Virtual**.

LANGKAH 5: Merawat CPU (Monitoring Node Proxmox)

- 1. **Monitoring Resource:**
 - Klik node **pve** → tab **Summary**.
 - Amati dan catat ke dalam kolom sebelah kiri tabel **LOG MONITORING & PERAWATAN NODE** di file LEMBAR KERJA ASESI:
 - CPU usage: _____ %
 - Memory usage: _____ MB / _____ MB
 - Root Disk: _____ GB terpakai.



- 2. **Cek QEMU Agent:**
 - Masih di tab Summary, gulir ke bawah.
 - Pastikan pada bagian QEMU Guest Agent tertulis Running atau Yes.
 - (Ini membuktikan bahwa "sistem pemantau" virtual pada template berfungsi dengan baik).

✓ CHECKLIST VERIFIKASI AKHIR

- IP Proxmox sudah sesuai nomor meja (192.168.251.1XX).
- `vmbr0` dan `vmbr1` sudah aktif (berwarna hijau/Yes).
- VM 100 sudah berstatus Template (ikonnya berubah).
- Notes/Tag sudah terisi dan tersimpan.
- QEMU Agent berstatus Running di Summary.
- Dokumen inventarisasi sudah dibuat di tabel **Inventarisasi Hardware Virtual** dan **LOG MONITORING & PERAWATAN NODE**

TUTORIAL PRAKTIK: KELOMPOK PEKERJAAN 2

Durasi: 150 Menit

Fokus: Deployment VM, Konfigurasi NAT/DNS Host, Instalasi Aplikasi, dan Port Forwarding.

 PENTING SEBELUM MULAI:

Ganti semua tulisan **xx** dengan Nomor Meja / Nomor Urut Anda.

Ganti semua tulisan **y** dengan Nomor Lab tempat Anda ujian / latihan

Contoh: Jika nomor meja/urut 05 dan nomor lab 1 (LAB TKJ 1),

192.168.25 Y .1 XX /24	192.168.251.1 05 /24
1 XX .10 Y .10 Y .101/24	105 .101.101.101/24

LANGKAH 1: Melakukan Setting BIOS (VM System Configuration)

Tujuan: Mengkloning template dan menyiapkan konfigurasi dasar VM.

- Full Clone VM 101 (Web Server):
 - Klik kanan pada VM 100 (Debian12-template) → Pilih Clone.
 - VM ID: **101**, Name: **web**, Mode: Full Clone. Klik Clone.
- Full Clone VM 102 (Security Gateway):
 - Klik kanan pada VM 100 lagi → Pilih Clone.
 - VM ID: **102**, Name: **sec-gw**, Mode: Full Clone. Klik Clone.
- Konfigurasi Cloud-Init IP (VM 101):
 - Klik VM 101 → Tab Cloud-Init → Klik IP Config (net0) → Edit.
 - IPv4/CIDR: **1xx.10y.10y.101/24**
 - Gateway (IPv4): **1xx.10y.10y.1**
 - Klik OK.
 - Klik **Regenerate Image**.
- Konfigurasi Cloud-Init IP (VM 102):
 - Klik VM 102 → Tab Cloud-Init → Klik IP Config (net0) → Edit.
 - IPv4/CIDR: **1xx.10y.10y.102/24**
 - Gateway (IPv4): **1xx.10y.10y.1**
 - Klik OK.
 - Klik **Regenerate Image**.

[Untuk selengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 17 - 18]

- Verifikasi VM System (BIOS Virtual):
 - Pada VM 101 dan 102, klik tab Options → Boot Order.
 - Pastikan **scsi0** dicentang dan berada di urutan paling atas.
 - Pastikan QEMU Agent berstatus *Enabled* (di tab Options atau Summary).
- Start & Verifikasi Booting:
 - Klik tombol Start pada VM 101 dan VM 102.
 - Buka tab Console pada masing-masing VM. Pastikan muncul prompt login Debian.
 - Setelah berhasil login, uji koneksi (ping) ke alamat gateway **1XX.10Y.10Y.1** dari **VM101(web)** dan **VM102(sec-gw)**.

[Untuk selengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 18 - 19]

LANGKAH 2: Konfigurasi NAT & DNS Forwarding di Proxmox Host

Tujuan: Memastikan VM dapat mengakses internet untuk download paket aplikasi.

1. **Buka Shell Proxmox Host** (Klik node `pve` → **Shell**).
2. **Aktifkan IP Forwarding:**

`nano /etc/sysctl.conf`

- Cari baris `#net.ipv4.ip_forward=1`, hapus tanda pagar (#) di depannya.
- Simpan (`Ctrl+O`, `Enter`) dan keluar (`Ctrl+X`).
- Aktifkan perubahan: `sysctl -p`

3. **Konfigurasi NAT Masquerade:**

- Install **iptables-persistent**, supaya rule dapat disimpan secara permanen

`apt install iptables-persistent`

- Buat file konfigurasi untuk NAT, misalnya dengan nama **firewal.sh** di **Shell Proxmox Host**

`nano firewall.sh`

```
root@pve:~#  
root@pve:~# nano firewall.sh
```

misalnya untuk contoh No urut siswa **53**, Lab yang digunakan Lab **TKJ 1**

Setelah file **firewall.sh** terbuka, isikan perintah NAT sebagai berikut :

```
GNU nano 7.2  
iptables -t nat --flush  
iptables -t nat -A POSTROUTING -s 153.101.101.0/24 -j MASQUERADE  
iptables-save > /etc/iptables/rules.v4
```

Setelah selesai simpan kemudian keluar

- ubah izin akses file **firewall.sh**, supaya bisa menjalankan script tersebut.

`chmod 777 firewall.sh`

```
root@pve:~#  
root@pve:~# chmod 777 firewall.sh  
root@pve:~#
```

- Aktifkan NAT dengan menjalankan file **firewall.sh**

`sh firewall.sh`

```
root@pve:~#  
root@pve:~# sh firewall.sh  
root@pve:~#
```

- Setelah mengaktifkan NAT, kita cek konfigurasi NAT tersebut.

iptables -t nat -L

```
root@pve:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  192.168.251.0/24      anywhere
root@pve:~#
```

Jika pada bagian **Chain POSTROUTING** hasilnya seperti diatas, konfigurasi NAT sudah berhasil.

Perintah NAT dibuat di dalam file **firewall.sh** , berbeda dengan seperti biasanya langsung mengetik perintah NAT di prompt terminal. Hal ini kita ubah untuk memudahkan perbaikan kalau terjadi kesalahan ketik/perintah, kita cukup membuka file dan memperbaiki baris yang salah dan jalankan ulang script tersebut.

Cara kerja script ini membaca dan menjalankan perintah dari baris paling atas terus berurutan ke baris - baris di bawahnya, jadi baris pertama kali di dijalankan adalah **-iptables -t nat -flush**, maksud dari perintah ini adalah menghapus semua baris perintah sebelumnya, jadi kalau kita memperbaiki baris perintah yang ada di file ini, script akan menghapus terlebih dulu semua baris sebelumnya, kemudian menjalankan baris - baris yang sudah diperbaiki.

4. **Konfigurasi DNS Forwarding (dnsmasq):**

apt update && apt install dnsmasq -y
nano /etc/dnsmasq.conf

- Hilangkan tanda pagar (#) pada 3 baris ini:

domain-needed
bogus-priv
no-resolv

- Tambahkan baris ini di bagian paling bawah file:

server=8.8.8.8

- Simpan, keluar, lalu restart service: **systemctl restart dnsmasq**

[Untuk lengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 21 - 22]

LANGKAH 3: Instalasi Sistem Operasi (Konfigurasi Pasca-Boot)

Tujuan: Mengaktifkan akses SSH dan memverifikasi konektivitas jaringan dari dalam VM.

1. Konfigurasi SSH di VM 101 & VM 102:
 - o Buka Console VM 101, login: `root / 123456`.
 - o Edit konfigurasi SSH: `nano /etc/ssh/sshd_config`
 - o Cari baris **#PermitRootLogin prohibit-password** ubah menjadi **PermitRootLogin yes** dan hilangkan tanda # di depannya.

PermitRootLogin yes

- o Memberikan tanda pagar di depan baris **PasswordAuthentication no**

#PasswordAuthentication no

- o Simpan, keluar, lalu restart service: `systemctl restart ssh`

[Untuk selengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 19 - 20]

2. Verifikasi Konektivitas (Lakukan di kedua VM):
 - o Ping Gateway: `ping 1XX.10Y.10Y.1` (Harus Reply)
 - o Ping Internet: `ping 8.8.8.8` (Harus Reply, membuktikan NAT berhasil)
 - o Ping Domain: `ping google.com` (Harus Reply, membuktikan DNS Forwarding berhasil)

Keterangan

XX = No Urut/Meja, Y = No Lab misal Lab TKJ 1, Y=1

LANGKAH 4: Instalasi Software Aplikasi

Tujuan: Menginstal layanan utama dan membuka akses dari jaringan publik.

A. Di VM 101 (Instalasi HestiaCP)

1. **Instalasi HestiaCP:** (Proses ini memakan waktu $\pm 10-15$ menit, pastikan internet stabil)
 - o Instalasi paket yang dibutuhkan

apt update && apt install ca-certificates wget -y

- o Install **hestiaCP**

Unduh skrip instalasi HestiaCP terbaru dari repositori GitHub resmi menggunakan perintah wget berikut .

wget <https://raw.githubusercontent.com/hestiacp/hestiacp/release/install/hst-install.sh>

Jalankan skrip instalasi dan ikuti petunjuk di layar.

bash [hst-install.sh](#)

Ketika proses instalasi, ada data-data yang harus di isikan, bisa mengikuti tabel dibawah ini.

user	admin
password	ujikom2627
email address	gunakan email sekolah
FQDN Hostname	web.ujikomxx.net xx : nomor meja /urut

⚠ PENTING: Saat instalasi selesai, layar akan menampilkan URL, Username (admin), dan Password. CATAT PASSWORD INI DI LKS ANDA!

[Untuk lengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 32 - 34]

B. Di VM 102 (Security Gateway)

- 1. Aktifkan IP Forwarding di dalam VM:

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sysctl -p
```

- 2. Instal Nginx & WireGuard

```
apt update && apt install nginx wireguard -y
```

- 3. Cek hasil instalasi **nginx** dan **wireguard**

Cek hasil instalasi nginx

```
root@sec-gw:~#
root@sec-gw:~# dpkg -l | grep nginx
ii  nginx                      1.22.1-9+deb12u9
ii  nginx-common               1.22.1-9+deb12u9
root@sec-gw:~#
```

Cek hasil instalasi wireguard

```
root@sec-gw:~#
root@sec-gw:~# dpkg -l | grep wireguard
ii  wireguard                  1.0.20210914-1
ii  wireguard-tools            1.0.20210914-1+b1
root@sec-gw:~#
```

Kalau setelah di cek, hasilnya seperti yang ada di kotak merah, **nginx** dan **wireguard** sudah berhasil di install.

- 4. Generate Key WireGuard:
 - Generate Key Server
wg genkey | tee server_private.key | wg pubkey > server_public.key
 - Generate Key Client
wg genkey | tee client_private.key | wg pubkey > client_public.key

[**vps-proxmox2026-2.pdf**, halaman 41]

C. Konfigurasi Port Forwarding (Di Proxmox Host)

- Buka Shell Proxmox Host (node pve).
- Buka file [firewall.sh](#) , kemudian tambahkan perintah DNAT seperti gambar dibawah ini

```
iptables -t nat --flush
iptables -t nat -A POSTROUTING -s 153.101.101.0/24 -j MASQUERADE

# 1. Akses Reverse Proxy (Web Publik)
iptables -t nat -A PREROUTING -p tcp -d 192.168.251.153 --dport 80 -j DNAT --to 153.101.101.102:80

# 2. Akses VPN WireGuard
iptables -t nat -A PREROUTING -p udp -d 192.168.251.153 --dport 51820 -j DNAT --to 153.101.101.102:51820

# 3. Akses SSH ke VM 101
iptables -t nat -A PREROUTING -p tcp -d 192.168.251.153 --dport 2201 -j DNAT --to 153.101.101.101:22

# 4. Akses HestiaCP (Setup Awal)
iptables -t nat -A PREROUTING -p tcp -d 192.168.251.153 --dport 8301 -j DNAT --to 153.101.101.101:8083

iptables-save > /etc/iptables/rules.v4
```

Keterangan :

192.168.251.153, berasal dari format 192.168.25Y.1XX,

153.101.101.101 berasal dari format 1XX.10Y.10Y.101 dimana :

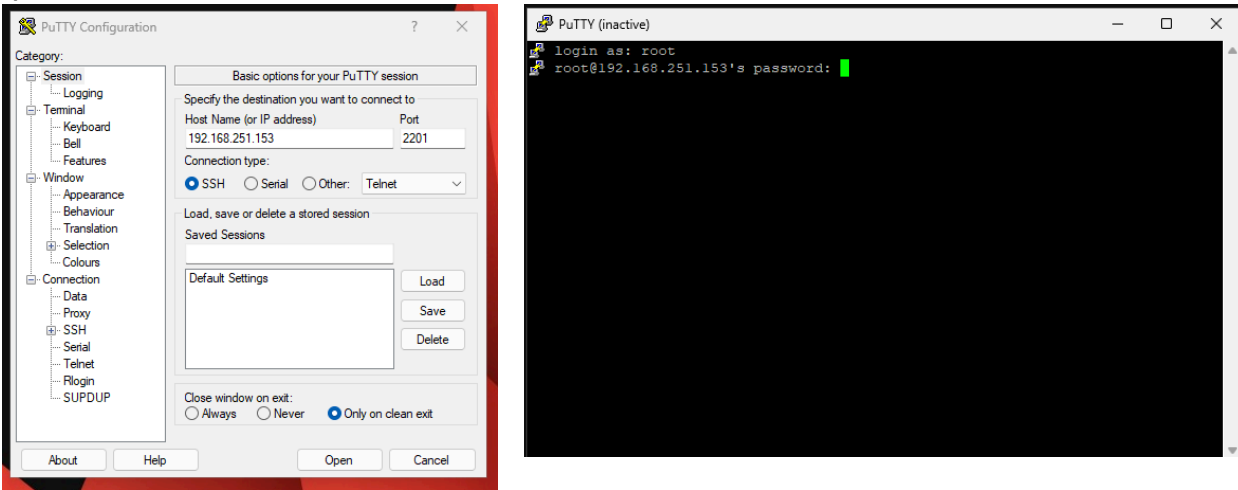
Y adalah nomor Lab TKJ, dalam contoh diatas misalnya siswa di Lab TKJ 1.

XX adalah Nomor urut / meja siswa, dalam contoh diatas misalnya nomor urut siswa 53.

untuk oktet terakhir 101 dan 102 tidak perlu diubah

[Lihat ketentuan IP Address di halaman 1 Tutorial ini]

- Menguji perintah NAT
 - Akses SSH ke VM 101, menggunakan **putty**, kemudian login dengan user: **root**, password: **123456**

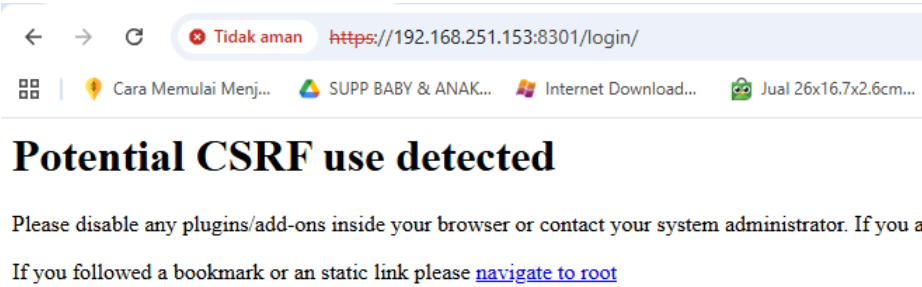


```
192.168.251.153 - PuTTY
login as: root
root@192.168.251.153's password:
Linux web.ujikom53.net 6.1.0-43-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.162-1 (2026-02-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep  7 07:23:41 2026 from 192.168.251.252
root@web:~#
```

- Akses HestiaCP, menggunakan web browser dengan alamat **https://192.168.251.153:8301**



HestiaCP Error CSRF: Jangan panik, itu normal dan memang disengaja dalam skenario ini untuk memaksa kita menggunakan VPN.

[Untuk lebih lengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 34 - 37]

Untuk menguji **Akses Reverse Proxy** dan **Akses VPN** di Kelompok Kerja 3

✓ CHECKLIST VERIFIKASI AKHIR

- VM 101 (web) dan VM 102 (sec-gw) berstatus Running.
- Cloud-Init IP sudah terpasang (1XX.10Y.10Y.101 dan 1XX.101.101.102).
- Perintah ping 8.8.8.8 dan ping google.com dari dalam VM berhasil (Reply).
- HestiaCP, nginx, Wireguard sudah berhasil di install.
- Key Wire Guard sudah dibuat.
- Perintah - perintah NAT sudah di konfigurasi di Proxmox Host.
- SSH sudah bisa diakses dari Client (Windows)
- HestiaCP sudah berjalan di VM 101 (bisa diakses via web browser).
- Password Admin HestiaCP sudah dicatat di LKS.

TUTORIAL PRAKTIK: KELOMPOK PEKERJAAN 3

Durasi: 120 Menit
Fokus: Maintenance, DNS/Reverse Proxy, Backup/Restore, dan Keamanan VPN.

⚠ PENTING SEBELUM MULAI:

Ganti semua tulisan **xx** dengan Nomor Meja / Nomor Urut Anda.
Ganti semua tulisan **y** dengan Nomor Lab tempat Anda ujian / latihan
Contoh: Jika nomor meja/urut 05 dan nomor lab 1 (LAB TKJ 1),

192.168.25 Y .1 XX /24	192.168.251. 105 /24
1 XX .10 Y .10 Y .101/24	105 .101.101.101/24

LANGKAH 1: Merawat Sistem Operasi (Patching)

Tujuan: Memastikan sistem operasi terbaru dan aman dari kerentanan.

- Update VM 101 (Web Server):
 - Buka Console VM 101, login `root` / `123456`.
 - Jalankan perintah:

```
root@web:~# apt update && apt upgrade -y
```

- Tunggu hingga selesai. Pastikan tidak ada pesan error.

- Update VM 102 (Security Gateway):
 - Buka Console VM 102, login `root` / `123456`.
 - Jalankan perintah yang sama

```
root@sec-gw:~# apt update && apt upgrade -y
```

- Dokumentasi: Catat di tabel **Log Patching** pada file Lembar Kerja Asesi bahwa patching berhasil dilakukan tanpa error.

LANGKAH 2: Setup DNS Lokal & Reverse Proxy

Tujuan: Mengarahkan domain `www.ujikomXX.net` ke VM 101 melalui VM 102.

- Konfigurasi DNS Lokal (Di Proxmox Host):
 - Buka Shell Proxmox Host.
 - Buat file konfigurasi: `nano /etc/dnsmasq.d/domain.conf`
 - Isi dengan baris berikut (ganti XX dan Y):

```
address=/www.ujikomXX.net/192.168.25Y.1XX
```

- Simpan dan keluar
- Restart service: `systemctl restart dnsmasq`

- Konfigurasi Reverse Proxy (Di VM 102):
 - Buka Console VM 102.
 - Install **nginx**
 - Buat file konfigurasi Nginx:

```
nano /etc/nginx/sites-available/proxy
```

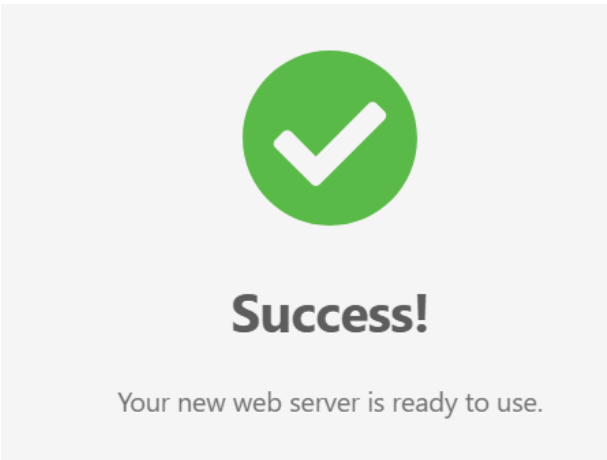
- Isi dengan konfigurasi berikut (ganti **XX** dan **Y**):

```
server {  
    listen 80;  
    server_name www.ujikomXX.net;  
  
    location / {  
        proxy_pass http://153.10Y.10Y.101;  
        proxy_set_header Host $host;  
        proxy_set_header X-Real-IP $remote_addr;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
    }  
}
```

- Simpan dan keluar.
- **Aktifkan konfigurasi:**

```
In -s /etc/nginx/sites-available/proxy /etc/nginx/sites-enabled/  
  
nginx -t # Pastikan output "syntax is ok" dan "test is successful"  
  
systemctl restart nginx
```

- 3. Uji Akses (Di PC Client Windows):
 - Buka browser, ketik: `http://www.ujikomXX.net`
 - Hasil yang diharapkan: Muncul halaman web dengan tulisan "**Success**"



[[vps-proxmox2026-2.pdf](#), halaman 28 - 31]

LANGKAH 5: Setup VPN WireGuard & Konfigurasi HestiaCP

Tujuan: Mengamankan akses HestiaCP agar terhindar dari error CSRF.

A. Konfigurasi Server VPN (Di VM 102)

- 1. Buka Console VM 102.
- 2. Edit file konfigurasi: `nano /etc/wireguard/wg0.conf`
- 3. Isi dengan template berikut (**Ganti bagian <...> dengan key yang Anda generate di Kelompok Pekerjaan 2**):

```
[Interface]
Address = 10.20.20.1/24
ListenPort = 51820
PrivateKey = <TEMPEL_SERVER_PRIVATE_KEY_DISINI>
PostUp = sysctl -w net.ipv4.ip_forward=1
PostUp = iptables -t nat -A POSTROUTING -s 10.20.20.0/24 -j MASQUERADE
PostDown = iptables -t nat -D POSTROUTING -s 10.20.20.0/24 -j MASQUERADE

[Peer]
PublicKey = <TEMPEL_CLIENT_PUBLIC_KEY_DISINI>
AllowedIPs = 10.20.20.2/32
```

systemctl enable --now wg-quick@wg0

5. Cek konfigurasi Wireguard, hasilnya harus seperti dibawah ini

```
root@sec-gw:~# wg show
interface: wg0
  public key: s1WmUM0tjsC+O/x2U0KJe/62SlGD64+b0yWt1WMVQTY=
  private key: (hidden)
  listening port: 51820

peer: ANSw9DdNB1gJAcMa9gX+2DA4OS1q+4u79A6UTC6Pbw8=
  allowed ips: 10.20.20.2/32
root@sec-gw:~#
```

```
root@vpn:~# ip a
```

```
    inet6 fe80::be24:11ff:fe96:1d58/64 scope link
        valid_lft forever preferred_lft forever
4: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue
    link/none
    inet 10.20.20.1/24 scope global wg0
        valid_lft forever preferred_lft forever
root@vpn:~#
```

B. Konfigurasi Client VPN (Di PC Client Windows)

1. Buka Notepad, buat file baru.
2. Isi dengan template berikut (**Ganti bagian < . . . >**):

```
[Interface]
PrivateKey = <TEMPEL_CLIENT_PRIVATE_KEY_DISINI>
Address = 10.20.20.2/32

[Peer]
PublicKey = <TEMPEL_SERVER_PUBLIC_KEY_DISINI>
Endpoint = 192.168.25Y.1XX:51820
```

3. `AllowedIPs = 10.20.20.0/24, 1XX.10Y.10Y.0/24`
4. Buka aplikasi wireGuard di windows → import tunnel(s) from file → Pilih **wg0.conf** → Klik Activate.

5. Cek konfigurasi (Client dan VPN Server sudah terkoneksi melalui **Tunnel** 10.20.20.0/24)
- Cek di **Server (VM102)**, konfigurasi berhasil kalau hasilnya seperti

```
root@sec-gw:~# wg show
interface: wg0
  public key: s1WmUM0tjsC+O/x2U0KJe/62SlGD64+b0yWt1WMVQTY=
  private key: (hidden)
  listening port: 51820

peer: ANSw9DdNB1gJAcMa9gX+2DA4OS1q+4u79A6UTC6Pbw8=
  endpoint: 192.168.251.253:54483
  allowed ips: 10.20.20.2/32
  latest handshake: 5 seconds ago
  transfer: 125.50 KiB received, 1.11 MiB sent
root@sec-gw:~#
```

- Cek Client (windows) ke VPN Server (10.20.20.1)

```
C:\Users\admin>ping 10.20.20.1

Pinging 10.20.20.1 with 32 bytes of data:
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
```

- Cek koneksi dari Windows ke local (VM) misalnya web server (153.101.101.101)

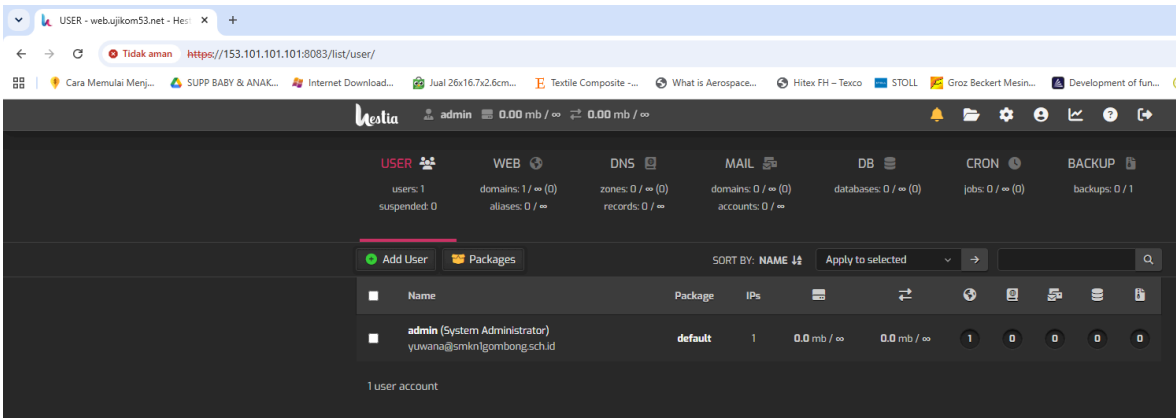
```
C:\Users\admin>ping 153.101.101.101

Pinging 153.101.101.101 with 32 bytes of data:
Reply from 153.101.101.101: bytes=32 time=1ms TTL=63
Reply from 153.101.101.101: bytes=32 time=1ms TTL=63
Reply from 153.101.101.101: bytes=32 time=1ms TTL=63
Reply from 153.101.101.101: bytes=32 time=1ms TTL=63
```

- Akses ke HestiaCP di web server (1XX.10Y.10Y.101) dari web browser :

[https ://1XX.10Y.10Y.101:8083](https://1XX.10Y.10Y.101:8083)

user: admin, password: 123456



[Untuk lebih lengkapnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 34 - 37]

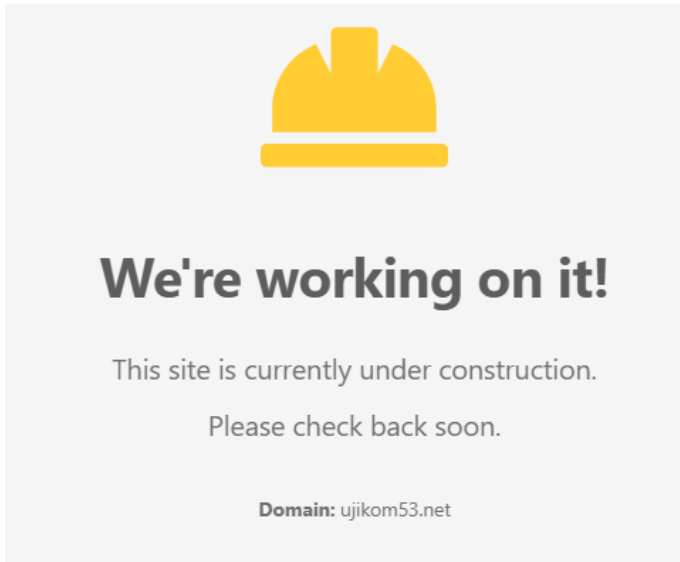
C. Konfigurasi HestiaCP

Langkah berikutnya adalah menambah domain dan user di HestiaCP, sebagai berikut :

user	userxx (xx = nomor urut / meja)
password	Tekaje2026
Domain	www.ujikomxx.net

Hasil akhirnya adalah sebagai berikut :

www.ujikomXX.net



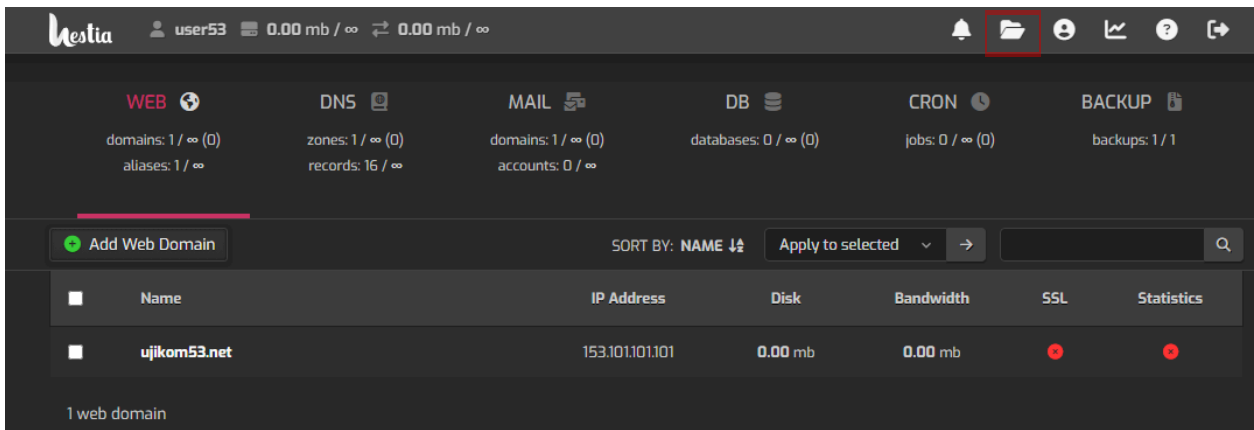
[langkah-langkahnya bisa dilihat file **vps-proxmox2026-2.pdf**, halaman 52 - 55]

LANGKAH 6: Mengelola Konten Web via HestiaCP File Manager

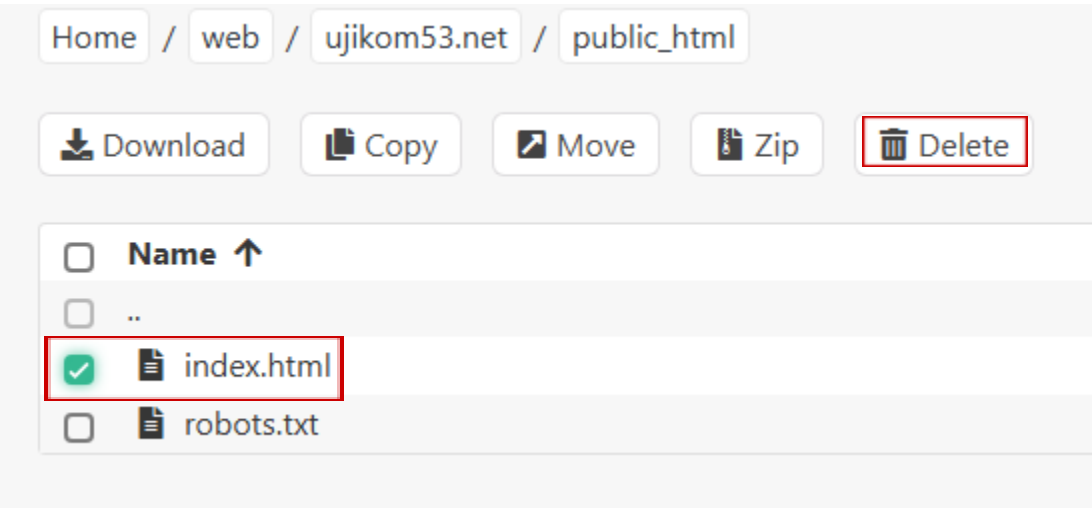
Prasyarat: Pastikan Anda sudah membuat user `userXX` dan domain `www.ujikomXX.net` di HestiaCP.

Langkah-langkah:

- 1. Login ke HestiaCP:
 - Buka browser (pastikan VPN WireGuard aktif).
 - Akses `https://10.10.10.11:8083`
 - Login menggunakan user: `userXX` dan password: `Tekaje2026`.
- 2. Buka File Manager:
 - Klik ikon Folder (File Manager) di sebelah kanan domain tersebut.

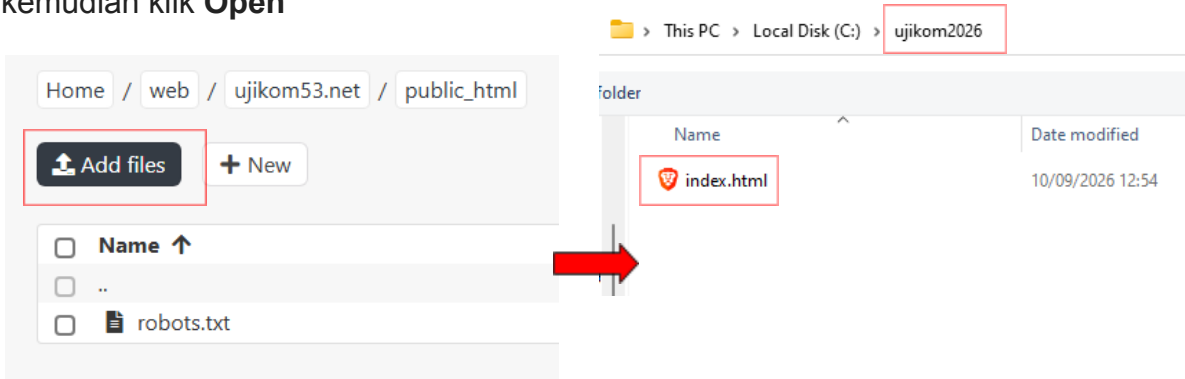


- 3. Masuk ke Direktori Web Root:
 - Anda akan berada di direktori `/home/userXX/`.
 - Klik folder `web` -> lalu klik folder `www.ujikomXX.net` -> lalu klik folder `public_html`.
 - *(Ini adalah folder root di mana file website harus disimpan).*
- 4. Menghapus File HTML default:
 - Jika ada file `index.html` default, klik ikon Sampah (Delete) untuk menghapusnya.

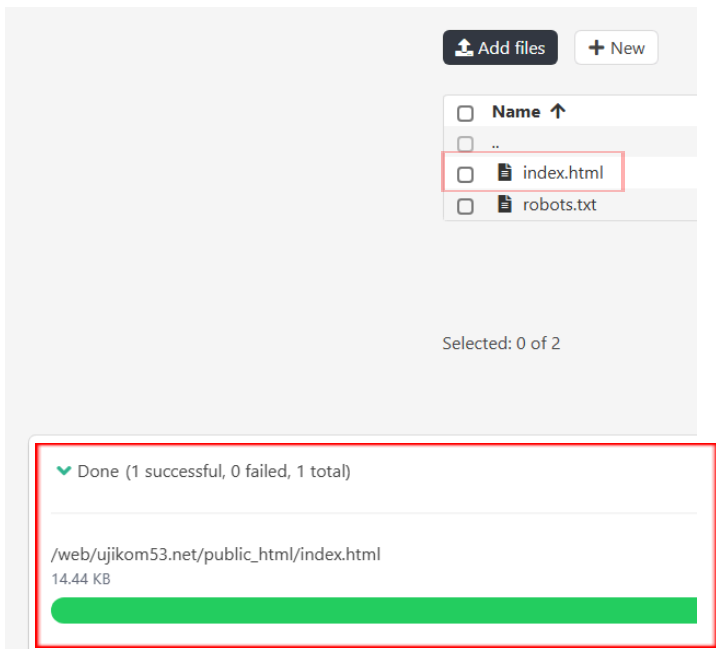


- 5. Upload file HTML ke Server
 - Upload file `index.html` yang berada di folder `c:\ujkom2026`, langkah-langkahnya adalah sebagai berikut:

Klik **Add files**, masuk ke folder **ujikom2026** di drive **C**, pilih file **index.html**, kemudian klik **Open**



File berhasil di upload, kalau ada file **index.html** kembali, dan ada pemberitahuan keberhasilan (*successful*) file yang di upload



6. Verifikasi Tampilan:
- Buka tab baru di browser PC Client.
 - Ketik alamat: **http://www.ujikomXX.net**
 - Screenshot halaman tersebut untuk bukti di LKS.

www.ujikomXX.net



LANGKAH 7: Backup & Snapshot (Proxmox)

Tujuan: Membuat titik pemulihan sebelum melakukan simulasi kerusakan.

Snapshot adalah perekam kondisi sementara (seperti tombol save game) untuk **uji coba** atau **pembaruan konfigurasi**.

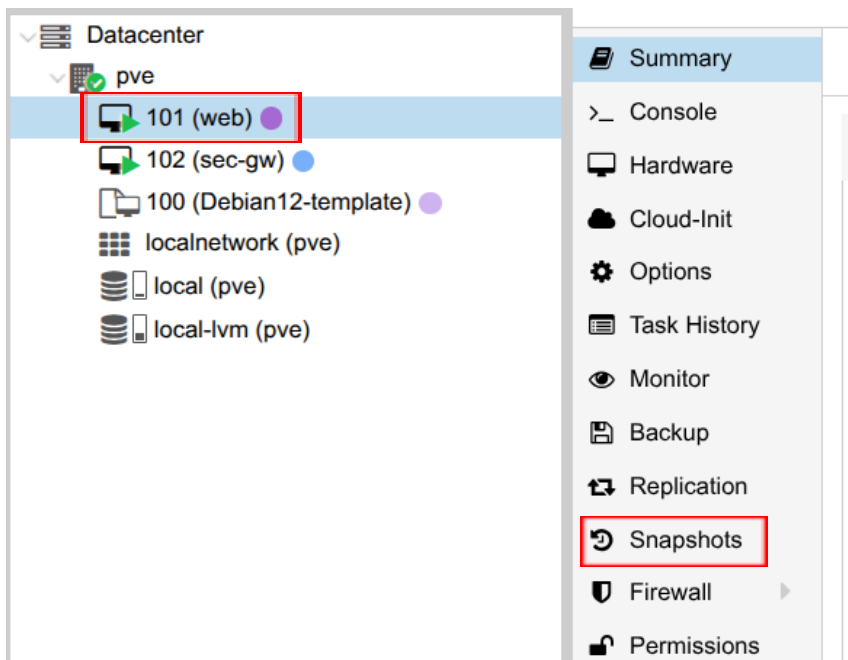
- **Sifat:** Proses instan, pemulihan sangat cepat, dan disimpan di **storage yang sama** dengan VM.
- **Risiko:** Jika disk utama rusak total, snapshot ikut hilang.

Backup adalah salinan utuh dari seluruh data VM untuk **keamanan jangka panjang** (*Disaster Recovery*).

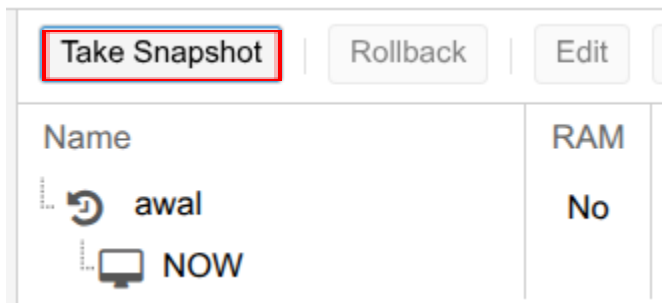
1. **Sifat:** Proses lebih lama, dikompresi menjadi file arsip, dan wajib disimpan di **storage terpisah** (seperti NAS atau Proxmox Backup Server).
2. **Keunggulan:** Aman digunakan untuk memulihkan data meskipun server utama rusak total.

Langkah-langkah untuk membuat Snapshots

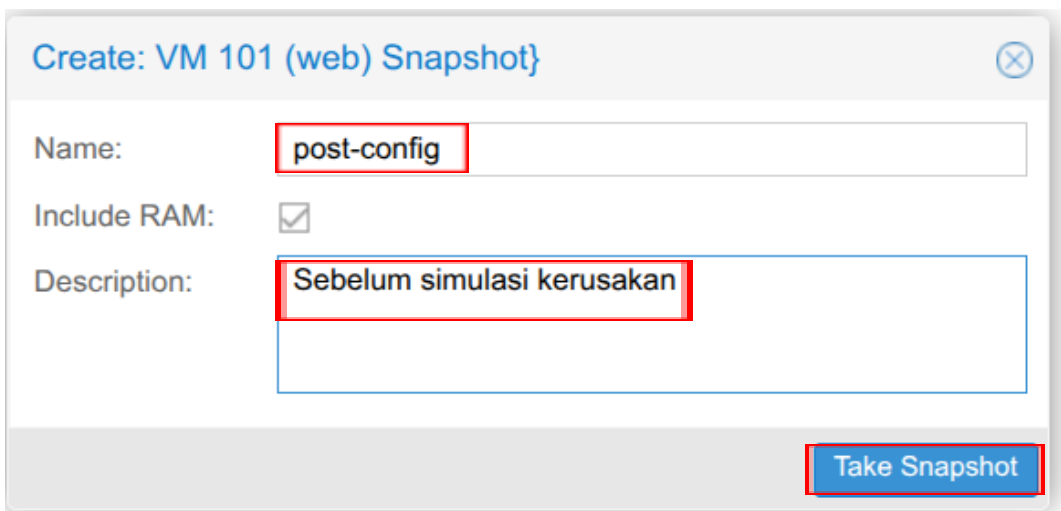
1. Buat Snapshot VM 101:
 - Di Proxmox GUI, klik **VM 101** → Tab **Snapshots**.



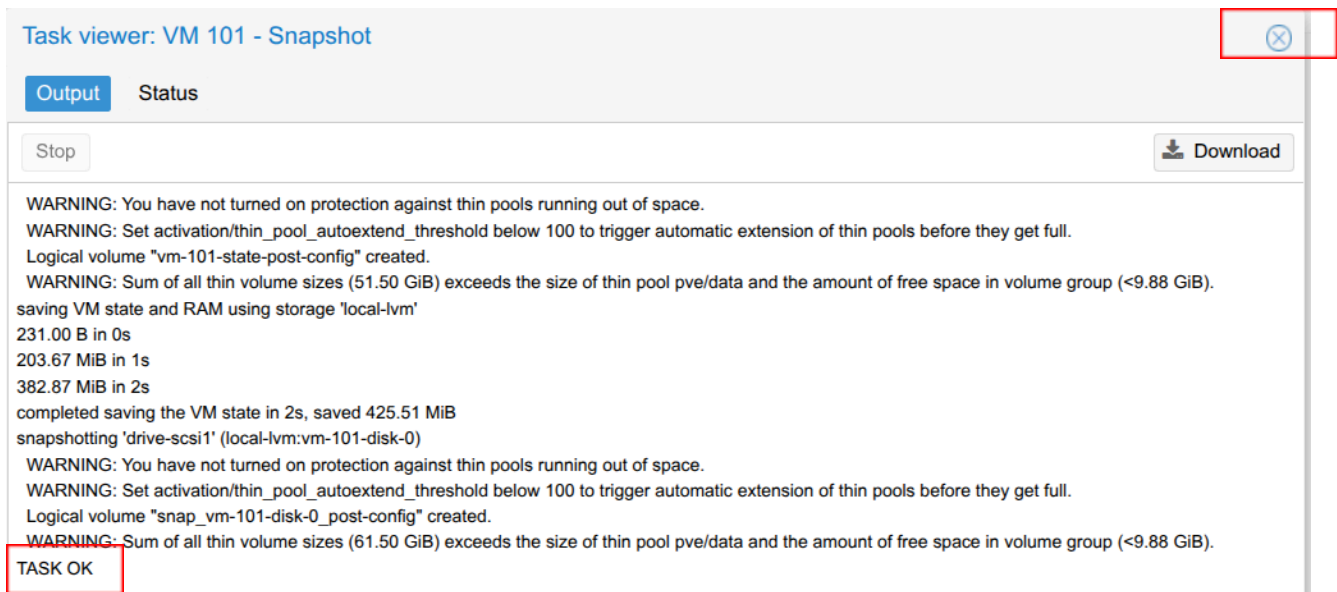
- Klik **Take Snapshot**.



- Name: **post-config**, Description: **Sebelum simulasi kerusakan**. Klik **Take Snapshot**.



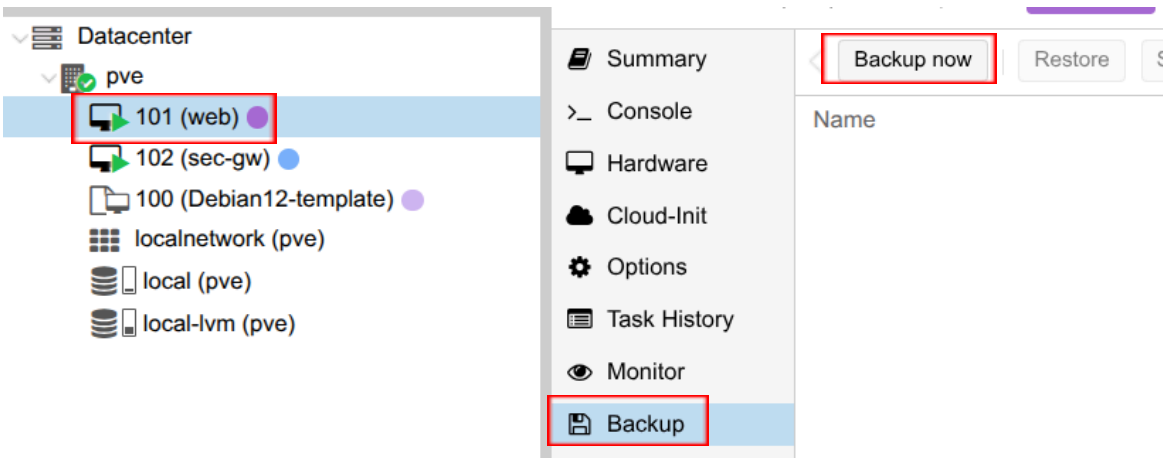
- Tunggu proses **Snapshot** sampai muncul **TASK OK** (artinya proses Snapshot sudah berhasil), kemudian **close**



- Setelah proses berhasil akan muncul tampilan dibawah ini yang berisi **nama** dan **deskripsi** dari Snapshot

Take Snapshot Rollback Edit Remove			
Name	RAM	Date/Status	Description
awal	No	2026-09-07 09:23:27	
post-config	Yes	2026-09-12 08:26:38	Sebelum simulasi kerusakan
NOW			You are here!

- 2. Buat Snapshot VM 102:
 - Ulangi langkah yang sama untuk VM 102 dengan nama **post-config**.
- 3. Backup VZDump :
 - Klik VM 101 → Tab Backup → Backup now.



- Mode: **Snapshot**, Storage: **local**. Klik Backup.

Backup VM 101 (web)

Storage: local

Mode: Snapshot

Protected: ☐

?

PBS change detection mode: Default

Notes: {{guestname}}

Compression: ZSTD (fast and good)

Notification mode: Auto

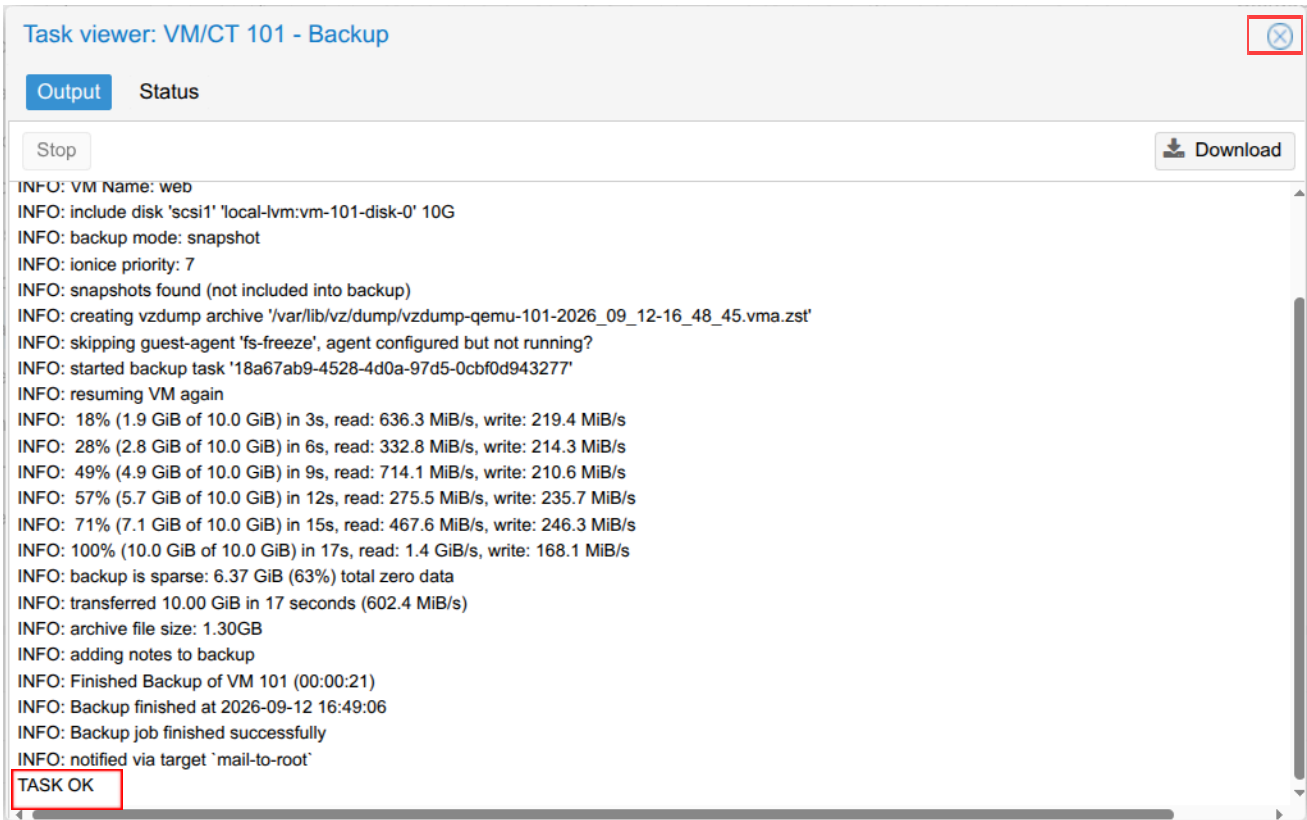
Send email to: none

Possible template variables are: {{cluster}}, {{guestname}}, {{node}}, {{vmid}}

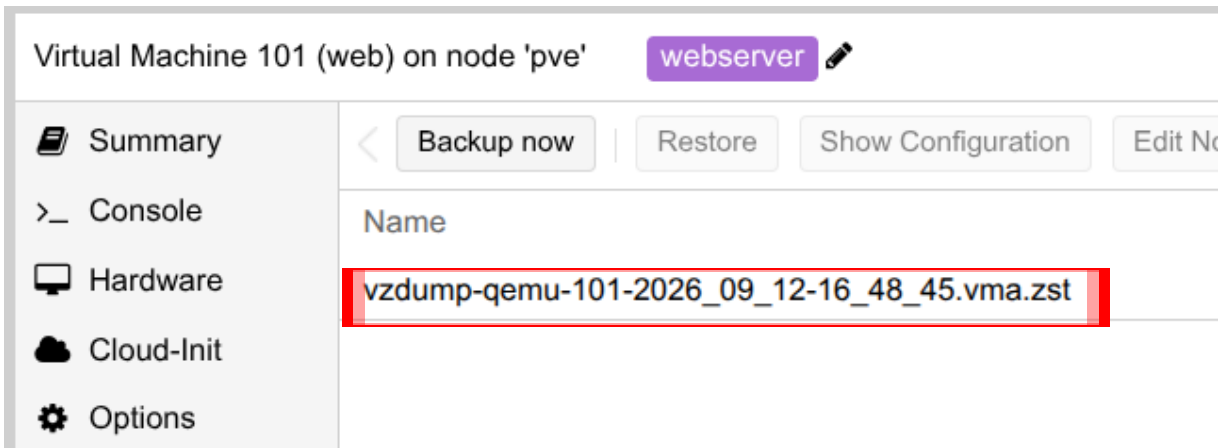
Help

Backup

- Tunggu proses **Backup** sampai muncul **TASK OK** (artinya proses **Backup** sudah berhasil), kemudian **close**.



- **Bagaimana tahu kalau backup kita sudah sukses?**
- Untuk mengetahui backup sudah berhasil. Masuk ke tab menu **Backup** pada VM 101. Jika di dalam tabel sudah muncul daftar file dengan ekstensi **.vma.zst**, itu tandanya *virtual machine* berhasil di backup.

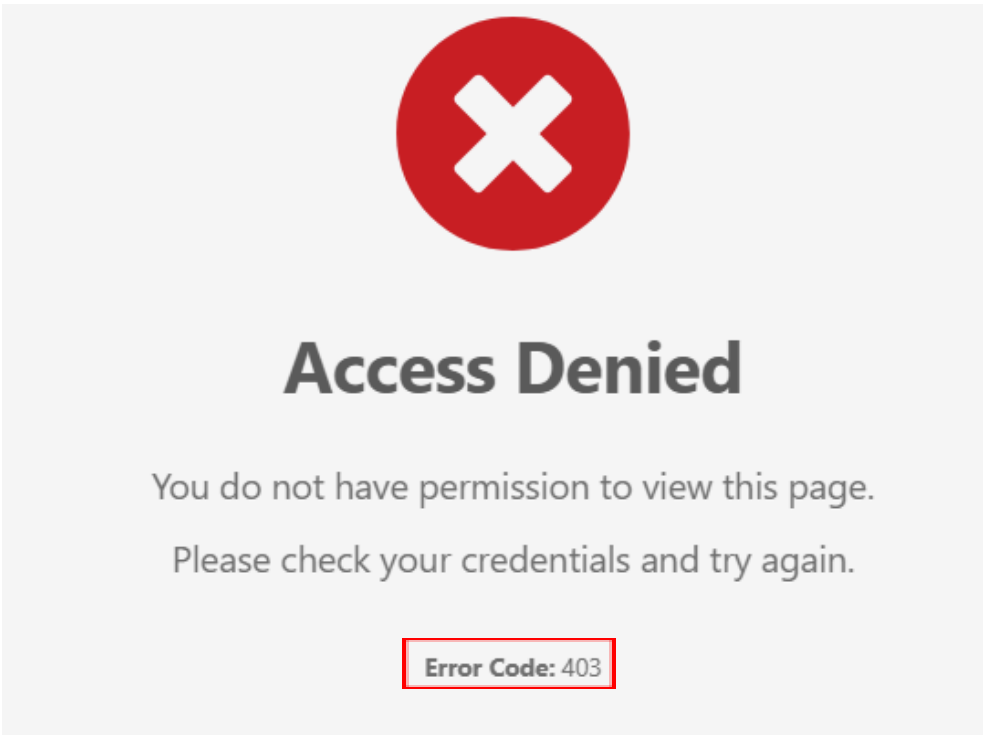


- Ulangi untuk VM 102.

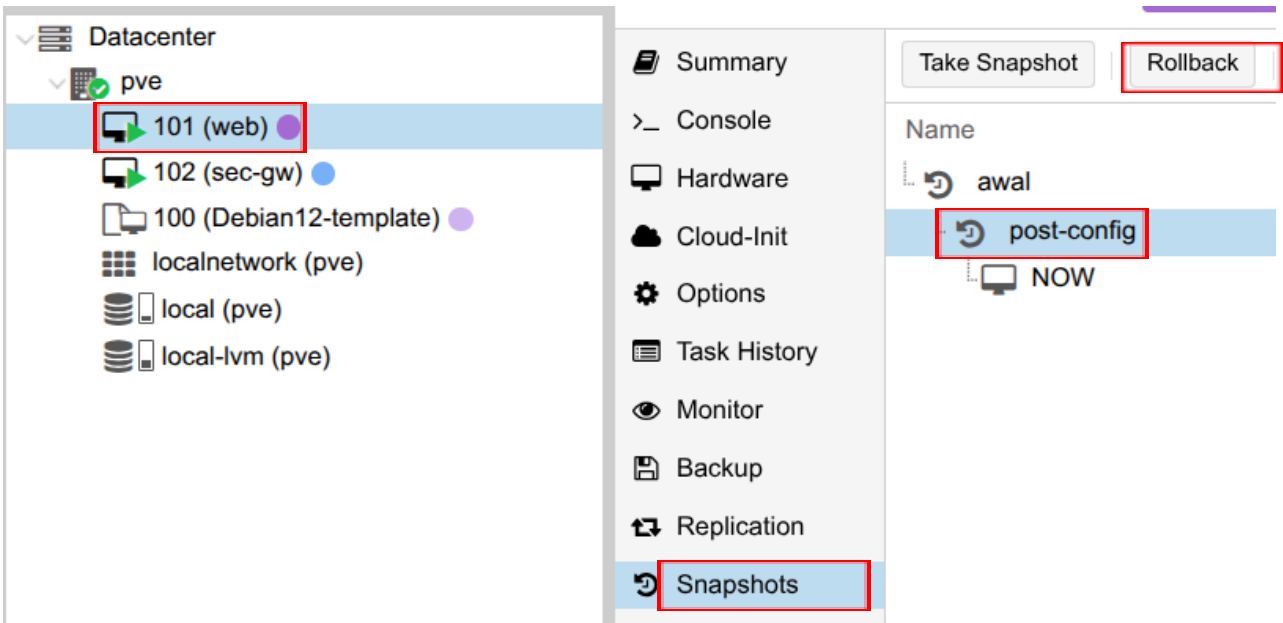
4. Dokumentasi: Catat nama snapshot, tanggal, dan lokasi storage di LKS.

LANGKAH 8: Simulasi Disaster Recovery (Rollback)

- 1. Simulasi Kerusakan: Di HestiaCP File Manager, hapus file `index.html`.
[cara menghapus file `index.html` dapat dilihat pada **LANGKAH 6: Mengelola Konten Web via HestiaCP File Manager**, point 1 s.d 4]
- 2. Verifikasi: Refresh browser → Error 403/404.



- 3. Rollback: Di Proxmox GUI, **VM 101** → **Snapshots** → **Pilih post-config** → **Rollback**.



4. Verifikasi: Refresh browser → Kembali ke tampilan web seperti semula.



✓ CHECKLIST VERIFIKASI AKHIR

- apt update && apt upgrade berhasil di VM 101 & 102 tanpa error.
- DNS Lokal (www.ujikomXX.net) resolve ke IP Proxmox. (kalau di ping www.ujikomXX.net reply berasal dari IP Proxmox [192.168.25Y.1XX])
- Reverse Proxy Nginx berhasil meneruskan traffic ke VM 101. (dapat membuka www.ujikomXX.net dari web browser)
- Tunnel WireGuard di Windows berstatus Active. (
- Ping ke 10.20.20.1 dan 1XX.10Y.10Y.101:8083) dapat diakses TANPA error CSRF.
- User userXX dan Domain www.ujikomXX.net sudah berhasil ditambahkan di HestiaCP.
- Tampilan halaman web sudah berhasil diubah.
- Snapshot post-config dan Backup berhasil dibuat di VM 101 & 102.
- Simulasi kerusakan (hapus index.html) berhasil di-rollback dan web normal kembali.
- LKS/Dokumentasi sudah diisi lengkap.