

PANDUAN PRAKTIKUM

ADMINISTRASI SISTEM JARINGAN

**PROXMOX
VERSI 8.0**

I PUTU HARIYADI

WWW.IPUTUHARIYADI.NET

**PANDUAN PRAKTIKUM
ADMINISTRASI SISTEM JARINGAN**

**OLEH
I PUTU HARIYADI**

www.iputuhariyadi.net

KATA PENGANTAR

Puji syukur penyusun panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmatnya sehingga “**Panduan Praktikum Administrasi Sistem Jaringan**” ini dapat terselesaikan. Modul ini dibuat sebagai panduan bagi mahasiswa yang memprogramkan matakuliah “**Administrasi Sistem Jaringan**” di **Program Studi Teknologi Informasi, Universitas Bumigora**.

Penyusun menyadari bahwa modul pelatihan ini masih jauh dari sempurna. Untuk itu kritik dan saran demi pengembangan modul pelatihan ini sangat diharapkan. Kritik dan saran dapat dikirimkan melalui email dengan alamat: putu.hariyadi@universitasbumigora.ac.id atau admin@iputuhariyadi.net. Terimakasih.

Mataram, 16 September 2023

Penyusun

DAFTAR ISI

Halaman Judul	(i)
KATA PENGANTAR	(ii)
DAFTAR ISI	(iii)
PENDAHULUAN	(1)
BAB I INSTALASI DAN KONFIGURASI PROXMOX VE 8.0 PADA ORACLE VIRTUALBOX	(2)
BAB II MENONAKTIFKAN PESAN NOTIFIKASI “NO VALID SUBSCRIPTION” PADA PROXMOX VE 8.0	(29)
BAB III MANAJEMEN REPOSITORY PADA PROXMOX VE 8.0	(33)
BAB IV INSTALASI DAN KONFIGURASI MIKROTIK CLOUD HOSTED ROUTER (CHR) SEBAGAI INTERNET GATEWAY PADA ORACLE VIRTUALBOX	(37)
BAB V INSTALASI DAN KONFIGURASI MIKROTIK CLOUD HOSTED ROUTER (CHR) PADA PROXMOX VE 8.0	(47)
BAB VI INSTALASI DAN KONFIGURASI LINUX CONTAINER (LXC) CENTOS 9 STREAM PADA PROXMOX VE 8.0	(75)
BAB VII MANAJEMEN USER DAN PERMISSION PADA PROXMOX VE 8.0	(90)
BAB VIII BACKUP DAN RESTORE PADA PROXMOX VE 8.0	(101)
BAB IX MANAJEMEN FIREWALL PADA PROXMOX VE 8.0	(116)
BAB X PROTEKSI BRUTE FORCE PADA PROXMOX VE 8.0 MENGUNAKAN FAIL2BAN	(131)

BAB XI - KONFIGURASI LINUX CONTAINER (LXC) CENTOS 9	
SEBAGAI STREAM SERVER INTERNET PADA PROXMOX VE 8.0	(141)
DAFTAR REFERENSI	(154)
TENTANG PENULIS	(155)

PENDAHULUAN

Adapun kebutuhan perangkat keras (*hardware*) dan lunak (*software*) yang diperlukan untuk dapat mengujicoba materi yang terdapat pada modul pelatihan ini adalah sebagai berikut:

A. Kebutuhan *Hardware*

Satu unit komputer dengan rekomendasi spesifikasi sebagai berikut:

1. CPU: 64 bit.
2. RAM: 8 GB.
3. Hard drive.
4. 1 (satu) *Network Interface Card*.

B. Kebutuhan *Software*

1. *Proxmox Virtual Environment (VE)* versi 8.0 yang dapat diunduh pada situs *Proxmox* di alamat <https://www.proxmox.com/en/downloads>
2. *Oracle VirtualBox* versi 6.1 atau yang lebih baru.
3. *Putty SSH Client* yang dapat diunduh pada alamat <https://www.putty.org/>
4. *Browser Chrome* yang dapat diunduh pada alamat <https://www.google.com/chrome/>.
5. *Mikrotik Cloud Hosted Router (CHR)* dan *Winbox* yang dapat diunduh pada situs *Mikrotik* pada alamat <https://mikrotik.com/download>
6. *Linux Container Image Templates* untuk *Proxmox* yang dapat diunduh pada alamat <http://download.proxmox.com/images/system/>
7. *WinSCP* untuk melakukan file transfer dari Windows ke Proxmox yang dapat diunduh pada alamat <https://winscp.net/eng/index.php>

Selain itu juga diperlukan koneksi *Internet* untuk mengunduh perangkat lunak tersebut dan ujicoba materi.

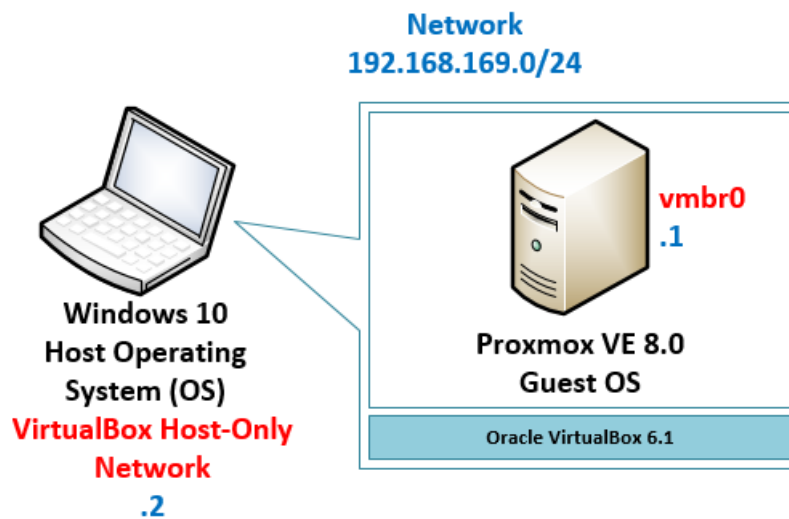
BAB I

INSTALASI DAN KONFIGURASI PROXMOX VE 8.0

PADA ORACLE VIRTUALBOX 6.1

A. Rancangan Jaringan Ujicoba

Rancangan jaringan ujicoba terdiri dari 1 unit *notebook* dengan sistem operasi *Windows 10* yang telah diinstalasi *Oracle VirtualBox 6.1* sebagai *hosted hypervisor*, seperti terlihat pada gambar berikut:

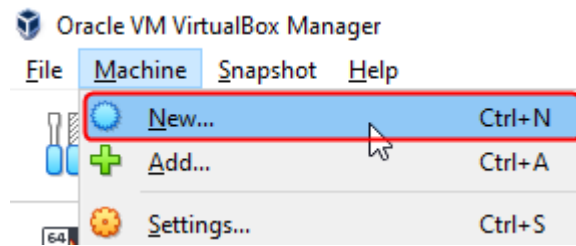


Pada *Oracle VirtualBox* akan dibuat *Guest Virtual Machine* dengan *Operating System (OS) Proxmox VE 8.0*. Alamat jaringan yang digunakan adalah *192.168.169.0/24* dengan alokasi pengalamatan IP meliputi *192.168.169.1* untuk *interface vmbr0* di *Guest OS Proxmox* dan *192.168.169.2* untuk *interface VirtualBox Host-Only Network* di *Windows 10*.

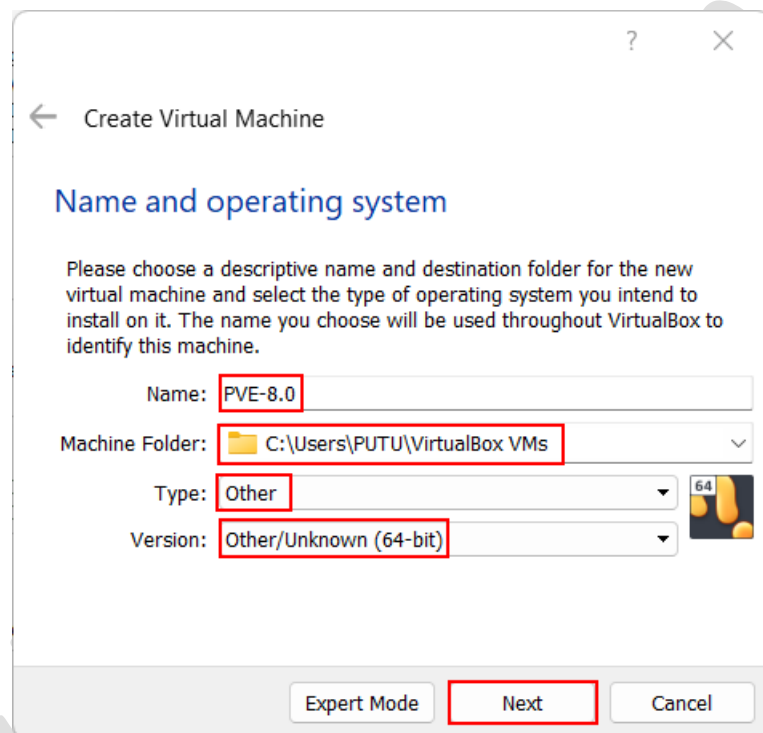
B. Instalasi Proxmox VE 8.0

Adapun langkah-langkah instalasi dan konfigurasi *Proxmox VE 8.0* pada *Oracle VirtualBox 6.1* adalah sebagai berikut:

1. Jalankan aplikasi *Oracle VirtualBox* melalui **Start > Oracle VM VirtualBox > Oracle VM VirtualBox**.
2. Tampil aplikasi *Oracle VM VirtualBox Manager*. Untuk membuat *virtual machine* baru, pilih menu **Machine > New ...**, seperti terlihat pada gambar berikut:



3. Tampil kotak dialog *Create Virtual Machine* untuk menentukan nama pengenal, lokasi penyimpanan dan jenis serta versi dari sistem operasi yang ingin dibuat pada *virtual machine*, seperti terlihat pada gambar berikut:



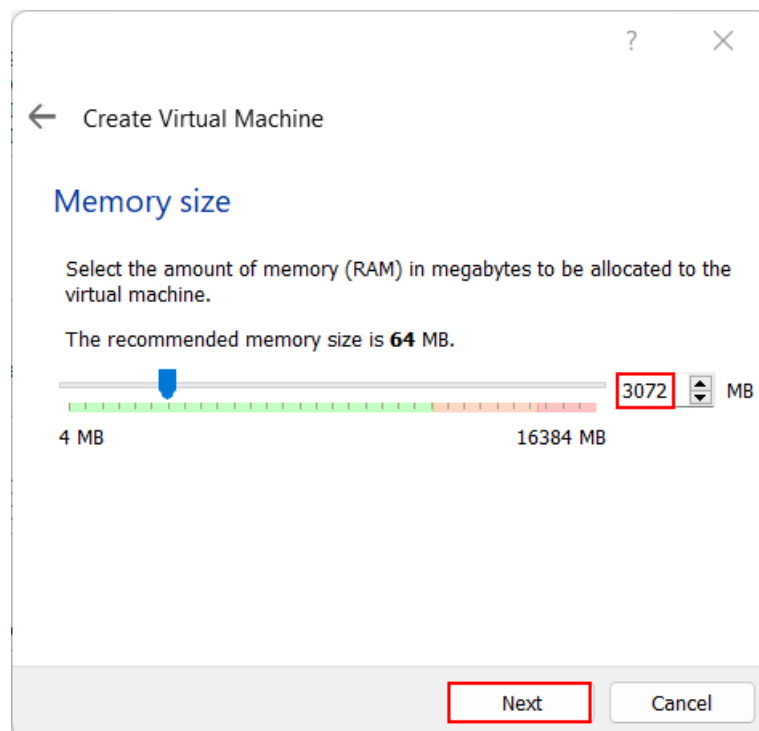
Lengkapi isian beberapa parameter berikut:

- Name:** dengan nama pengenal dari *virtual machine*, sebagai contoh **PVE-8.0**.
- Machine Folder** digunakan untuk menentukan lokasi penyimpanan *file virtual machine* yang dibuat yaitu secara *default* disimpan di **C:\Users\NamaLogin\VirtualBox VMs**. **NamaLogin** merupakan nama login pengguna yang digunakan untuk akses ke sistem *Windows*, sebagai contoh **ASUS** sehingga nilai pada *dropdown Machine Folder* adalah **C:\Users\PUTU\VirtualBox VMs**. Apabila ingin menyimpan di lokasi lain maka pilih **Other...** pada *dropdown Machine Folder* tersebut dan arahkan ke lokasi direktori penyimpanan baru yang diinginkan.

- c. **Type** digunakan untuk menentukan jenis sistem operasi yang akan diinstalasi pada *virtual machine* yaitu **Other**.
- d. **Version** digunakan untuk menentukan versi dari sistem operasi yang akan diinstalasi pada *virtual machine* yaitu **Other/Unknown (64 bit)**.

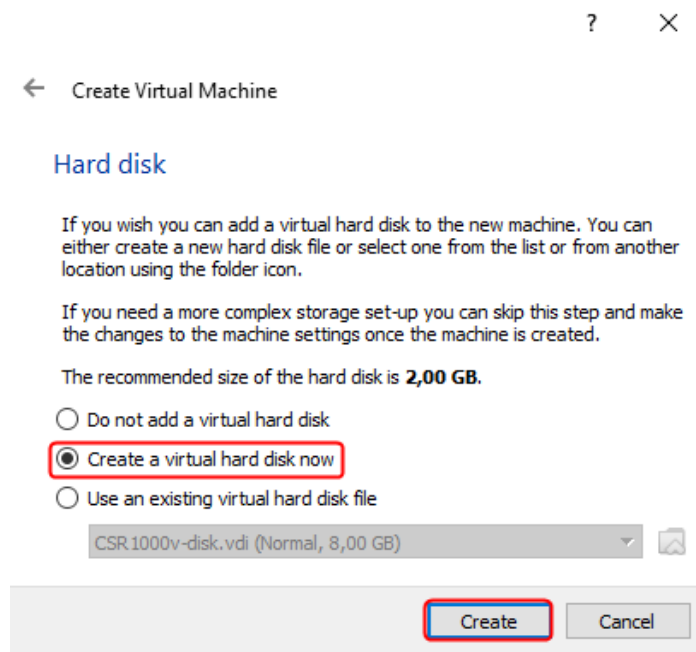
Klik tombol **Next** untuk melanjutkan.

4. Tampil kotak dialog *Memory size* untuk menentukan ukuran memori yang dialokasikan bagi *virtual machine* yang dibuat. Sebagai contoh dialokasikan **3072 MB**, seperti terlihat pada gambar berikut:



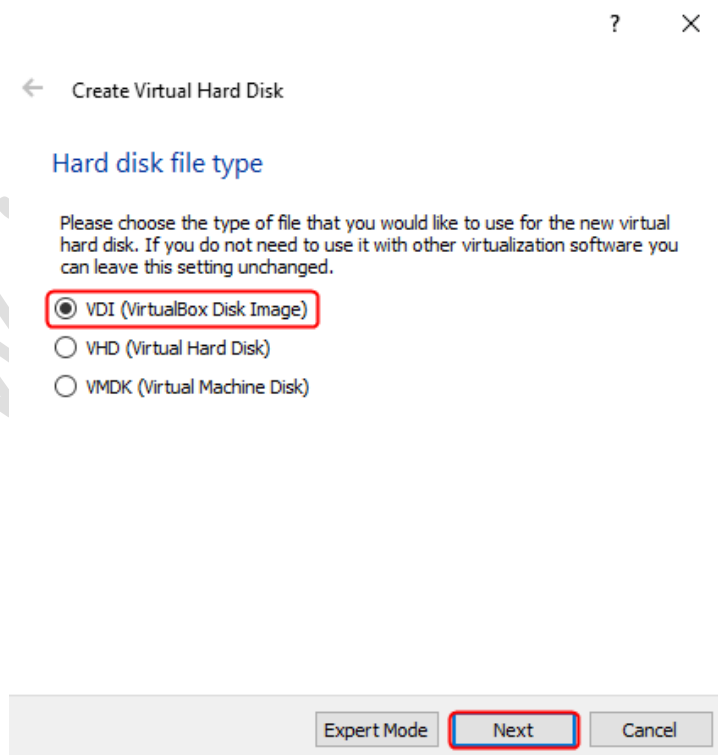
Klik tombol **Next** > untuk melanjutkan.

5. Tampil kotak dialog *Hard disk* untuk menentukan *virtual hardisk* yang digunakan oleh *virtual machine* yang dibuat. Secara default telah terpilih **Create a virtual hard disk now** untuk membuat *virtual hard disk* bagi *virtual machine* baru yang dibuat, seperti terlihat pada gambar berikut:



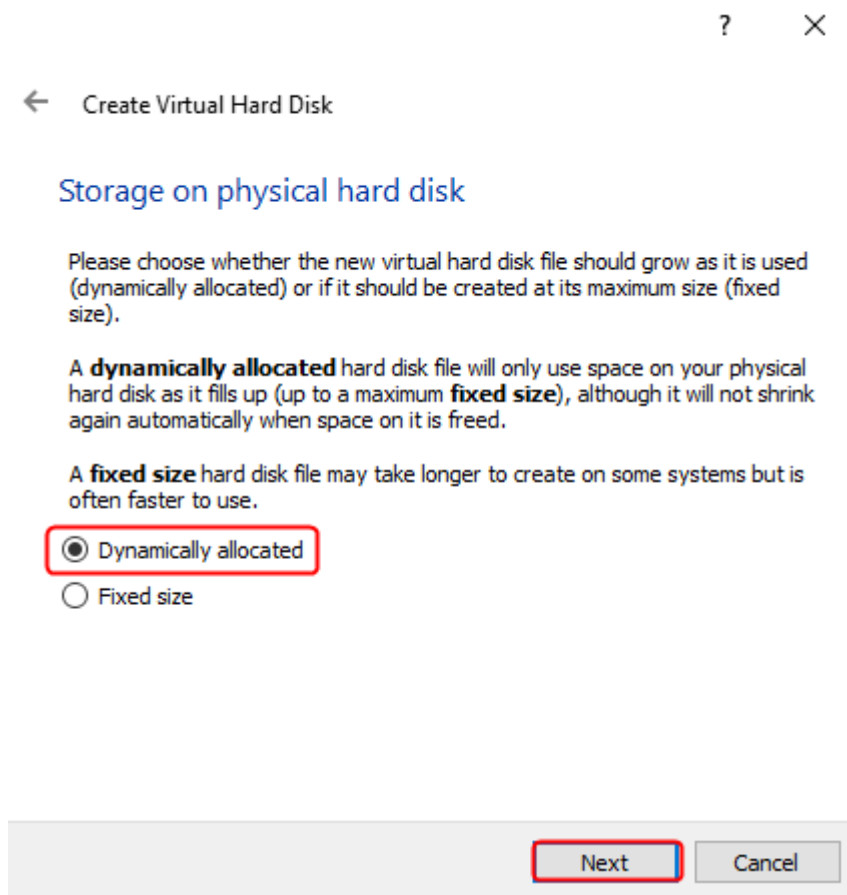
Klik tombol **Create** untuk melanjutkan.

6. Tampil kotak dialog Hard disk file type untuk menentukan jenis file yang digunakan untuk virtual hard disk baru yang dibuat. Secara default telah terpilih **VDI (VirtualBox Disk Image)**, seperti terlihat pada gambar berikut:



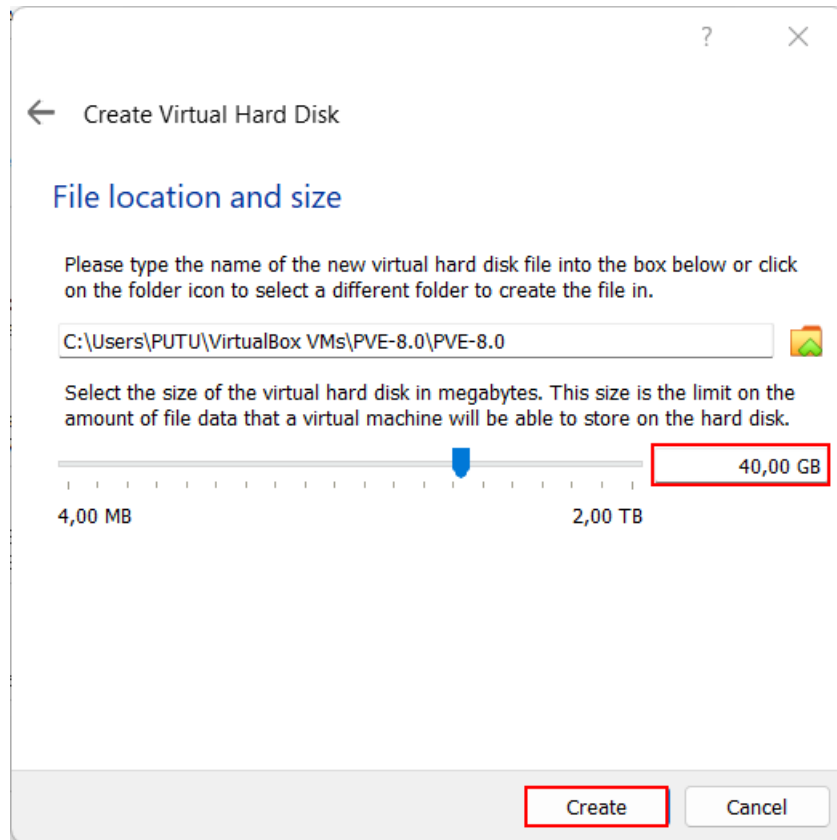
Klik tombol **Next** untuk melanjutkan.

7. Tampil kotak dialog **Storage on physical hard disk** untuk menentukan apakah *file virtual hard disk* yang baru dibuat harus bertumbuh mengikuti penggunaan (**dynamically allocated**) atau dibuat ke ukuran maksimumnya (**fixed size**). Secara *default* telah terpilih **Dynamically allocated**, seperti terlihat pada gambar berikut:

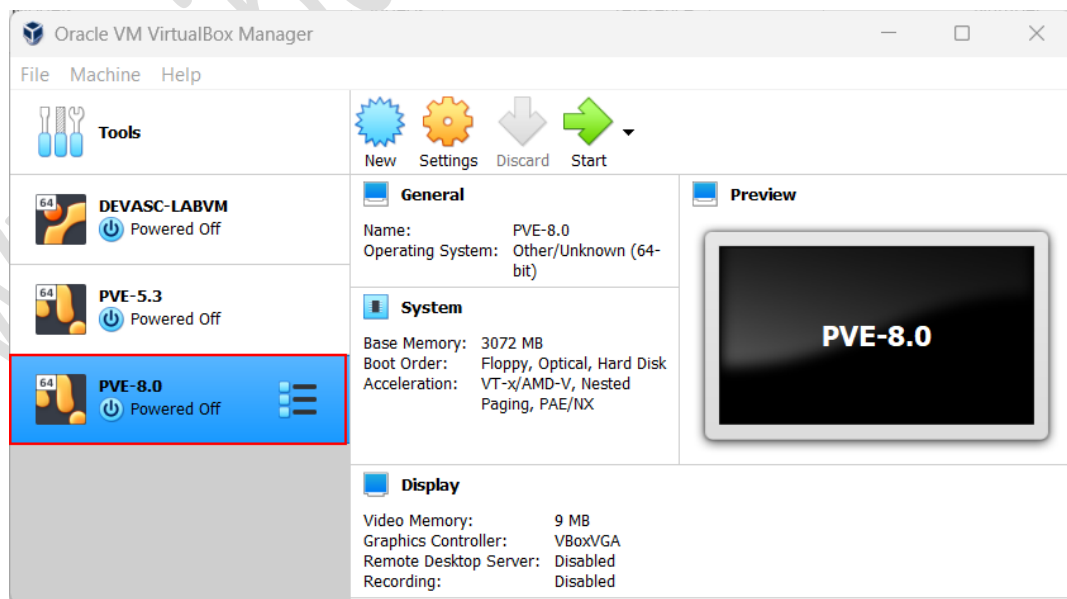


Klik tombol **Next** untuk melanjutkan.

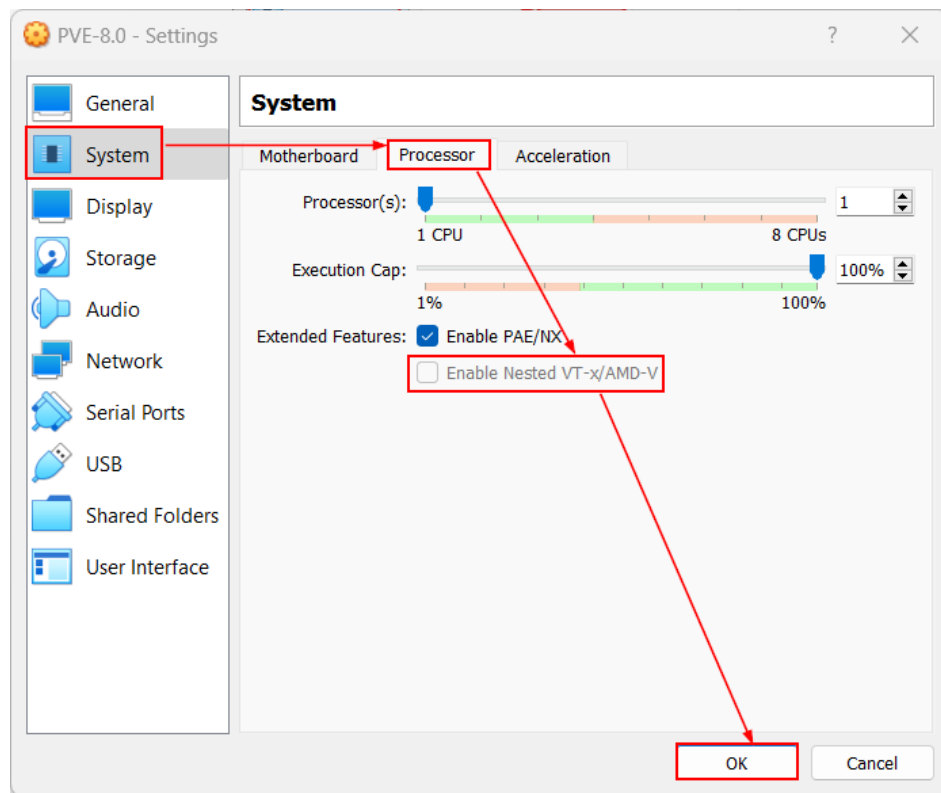
8. Tampil kotak dialog *File location and size* untuk menentukan lokasi dan ukuran *virtual hard disk* yang dapat digunakan oleh *virtual machine* sebagai penyimpanan. Sebagai contoh dialokasikan **40,00 GB**, seperti terlihat pada gambar berikut:



Klik tombol **Create** untuk melanjutkan. Tunggu beberapa saat, proses pembuatan *virtual machine* sedang dilakukan. Apabila proses pembuatan VM berhasil dilakukan maka pada daftar dari **Oracle VM VirtualBox Manager** akan memperlihatkan VM dengan nama pengenal **PVE-8.0**.



9. Mengaktifkan **nested VT-X/AMD-V** di *VirtualBox* untuk VM dengan nama **PVE-8.0**. Secara *default* fitur tersebut tidak dapat diaktifkan. Hal ini dapat diverifikasi dengan mengakses **PVE-8.0 - Settings** melalui pemilihan **Settings** pada *toolbar* dari *Oracle VM VirtualBox Manager*. Pada kotak dialog **PVE-8.0 – Settings** yang tampil, pilih **System** pada panel menu sebelah kiri dan pada panel detail sebelah kanan memilih tab **Processor**, seperti yang ditunjukkan pada gambar berikut:



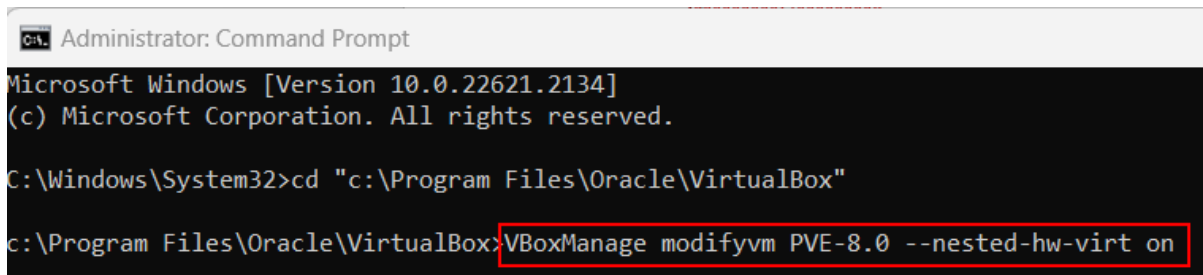
Pengaktifan *nested virtualization* ini dapat dilakukan melalui **command prompt Windows** yang dijalankan sebagai *administrator* (**Run as administrator**).

Pada kotak dialog **command prompt** yang tampil, lakukan eksekusi perintah `cd "C:\Program Files\Oracle\VirtualBox"` untuk berpindah ke lokasi direktori yang memuat instalasi *VirtualBox* yaitu di **"C:\Program Files\Oracle\VirtualBox"**, seperti yang ditunjukkan oleh gambar berikut:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>cd "c:\Program Files\Oracle\VirtualBox"
```

Silakan menyesuaikan jika lokasi direktori instalasi dari *VirtualBox* yang dimiliki berbeda.

Sintak perintah untuk mengaktifkan *nested VT-X/AMD-V* adalah **VBoxManage modifyvm <virtual_machine_name> --nested-hw-virt on** dimana **<virtual_machine_name>** merupakan nama *virtual machine* yang akan diubah yaitu **PVE-8.0**. Sehingga perintah pengaktifan virtualisasi yang dieksekusi menjadi **VBoxManage modifyvm PVE-8.0 --nested-hw-virt on**, seperti ditunjukkan pada gambar berikut:

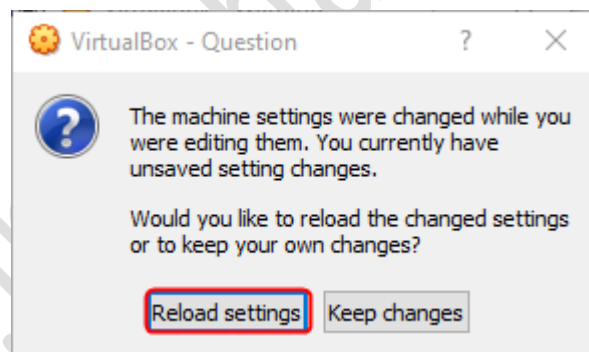


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.2134]
(c) Microsoft Corporation. All rights reserved.

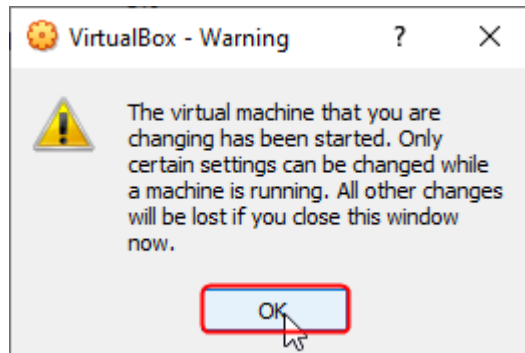
C:\Windows\System32>cd "c:\Program Files\Oracle\VirtualBox"
c:\Program Files\Oracle\VirtualBox>VBoxManage modifyvm PVE-8.0 --nested-hw-virt on
```

Tutup kotak dialog **Command Prompt**.

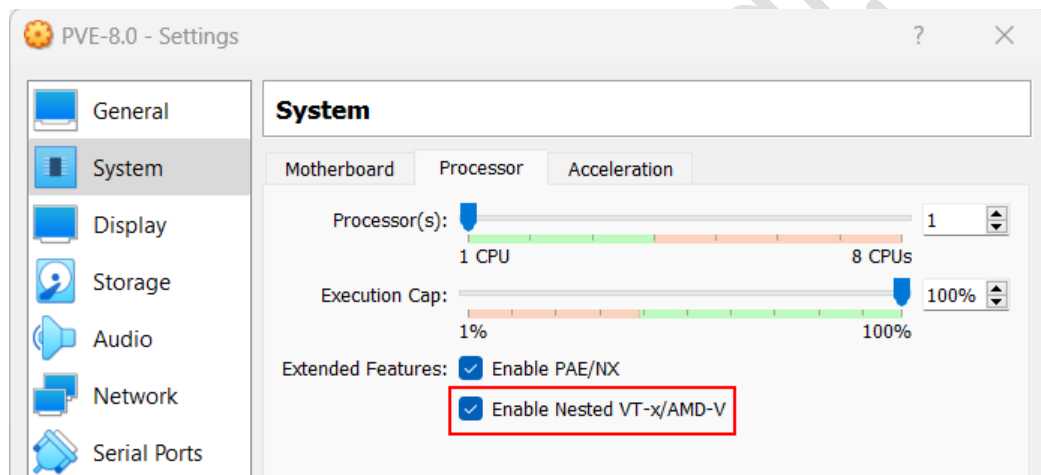
Kembali ke **Oracle VM VirtualBox Manager** maka akan tampil kotak dialog **VirtualBox – Question** yang menginformasikan bahwa terdapat perubahan pada pengaturan *virtual machine* sebagai dampak pengaktifan *Nested Virtualization* melalui perintah yang dieksekusi pada *command prompt*, seperti terlihat pada gambar berikut:




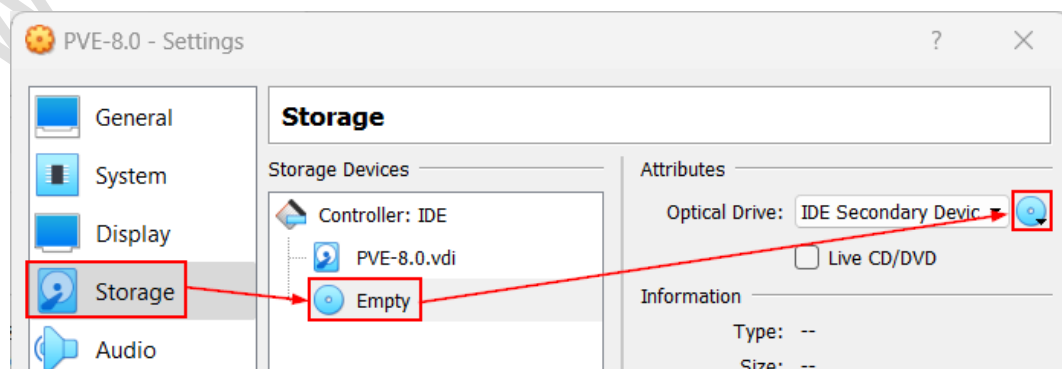
Klik tombol **Reload settings** untuk memuat ulang perubahan pengaturan yang dilakukan pada *virtual machine*. Selanjutnya tampil kotak dialog **VirtualBox – Warning** yang menginformasikan bahwa perubahan pada *virtual machine* telah dijalankan, seperti terlihat pada gambar berikut:



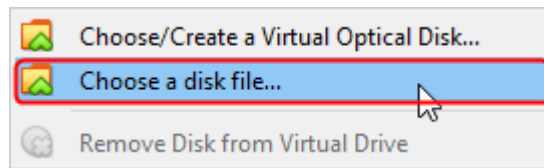
Klik tombol **OK**. Selanjutnya pada **PVE-8.0 Settings** yaitu di bagian **Extended Features** dari **Processor**, pilihan **Enable Nested VT-X/AMD-V** telah tercentang (✓) yang menandakan bahwa fitur *nested virtualization* telah berhasil diaktifkan, seperti terlihat pada gambar berikut:



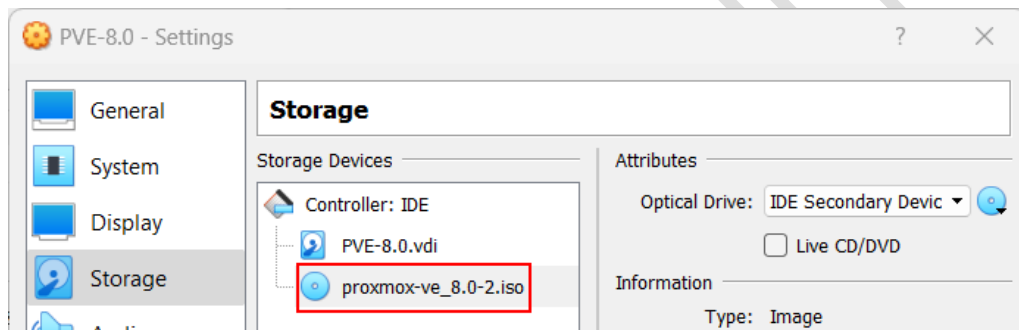
10. Mengubah pengaturan **storage** untuk mengarahkan ke lokasi penyimpanan **file ISO** dari **Proxmox VE 8.0**. Pada panel sebelah kiri dari **PVE-8.0 Settings**, pilih **Storage** dan pada panel detail sebelah kanan yaitu di bagian **Storage Devices**, pilih **Empty** yang ditandai dengan **icon CD**. Selanjutnya di bagian **Attributes**, klik pada **icon CD** dengan **tanda panah bawah**  dari pilihan **Optical Drive**, seperti yang ditunjukkan pada gambar berikut:



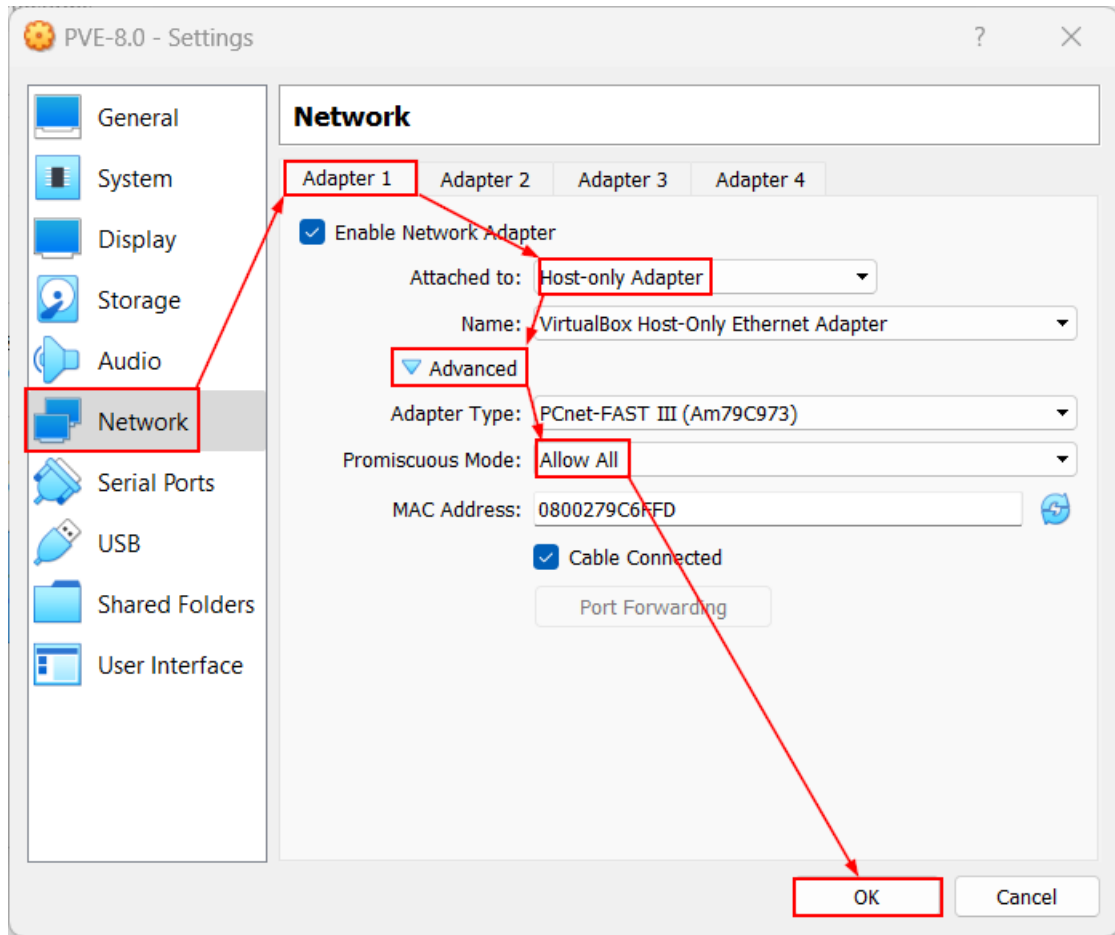
Pada *dropdown* yang tampil, pilih **Choose a disk file...**, seperti terlihat pada gambar berikut:



Arahkan ke lokasi penyimpanan **file ISO** dari **Proxmox VE 8.0**, sebagai contoh di **D:\Master\ proxmox-ve_8.0-2.iso**. **Silakan menyesuaikan dengan lokasi file ISO yang tersimpan di komputer masing-masing**. Pilih *file* dengan nama **proxmox-ve_8.0-2.iso** yang terdapat di direktori tersebut dan klik tombol **Open** sehingga hasilnya akan terlihat seperti pada gambar berikut:

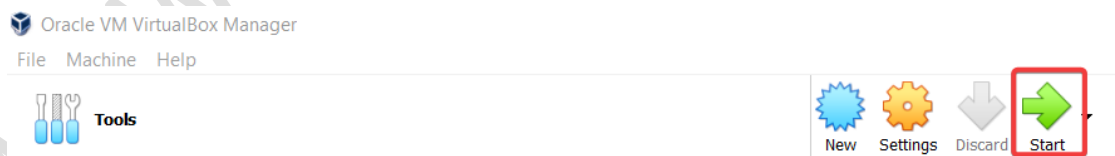


11. Mengubah pengaturan **network adapter** terkait jenis dan **promiscuous mode**. Pada panel sebelah kiri dari **PVE-8.0 Settings**, pilih **Network**. Sedangkan pada panel detail sebelah kanan yaitu di tab **Adapter 1**, klik pada *dropdown Attached to* dan pilih **Host-only Adapter**, seperti yang ditunjukkan pada gambar berikut:

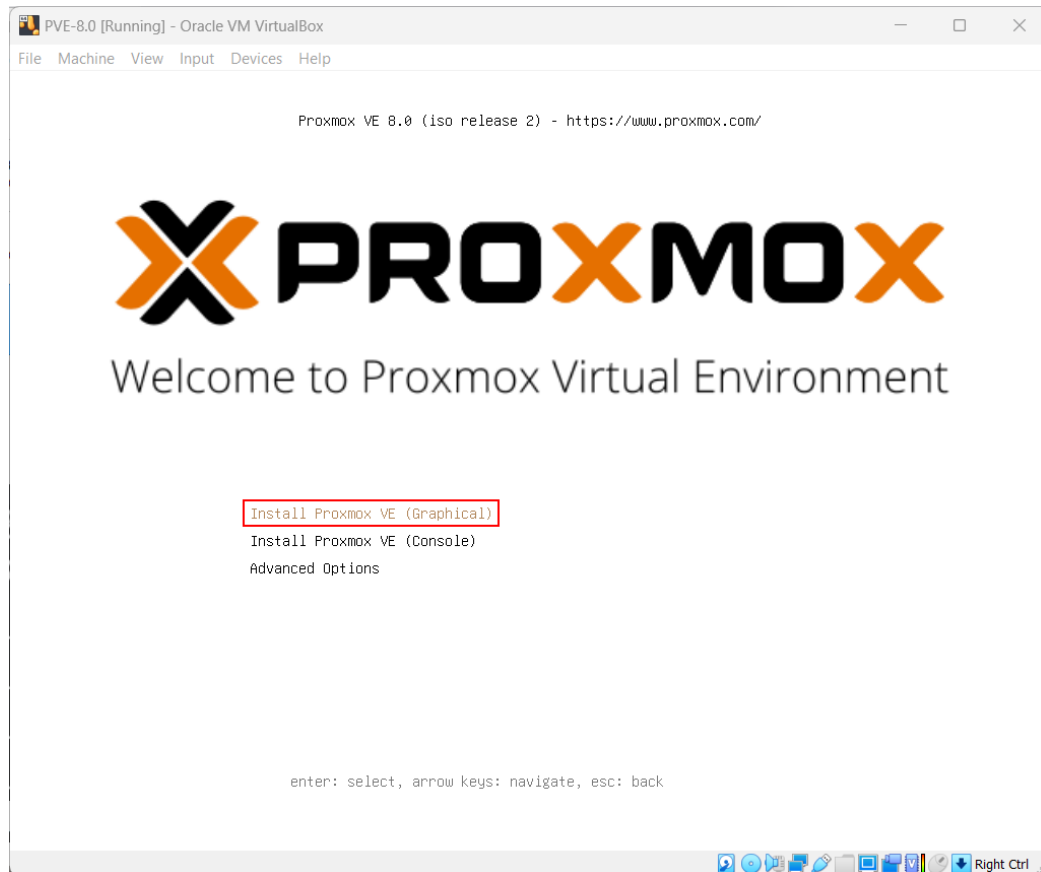


Selanjutnya klik bagian **Advanced** dan pada *dropdown Promiscuous Mode*, pilih **Allow All**. Klik tombol **OK** untuk menyimpan pengaturan.

12. Menjalankan VM dengan memilih **PVE-8.0** pada daftar dari *Oracle VM VirtualBox Manager* dan memilih **Start** pada *toolbar*, seperti yang ditunjukkan pada gambar berikut:

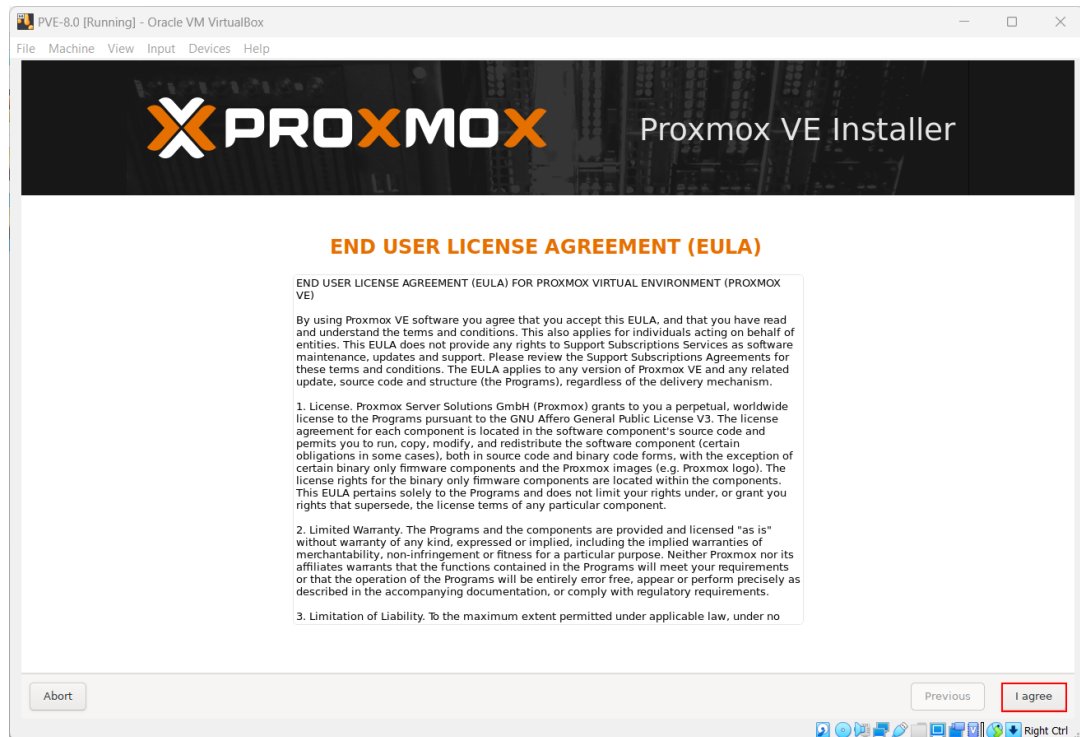


13. Tampil kotak dialog **PVE-8.0 [Running] – Oracle VM VirtualBox** dan didalamnya menampilkan menu awal instalasi berupa *Welcome to Proxmox Virtual Environment* yang digunakan untuk menentukan jenis instalasi yang akan dilakukan, seperti terlihat pada gambar berikut:



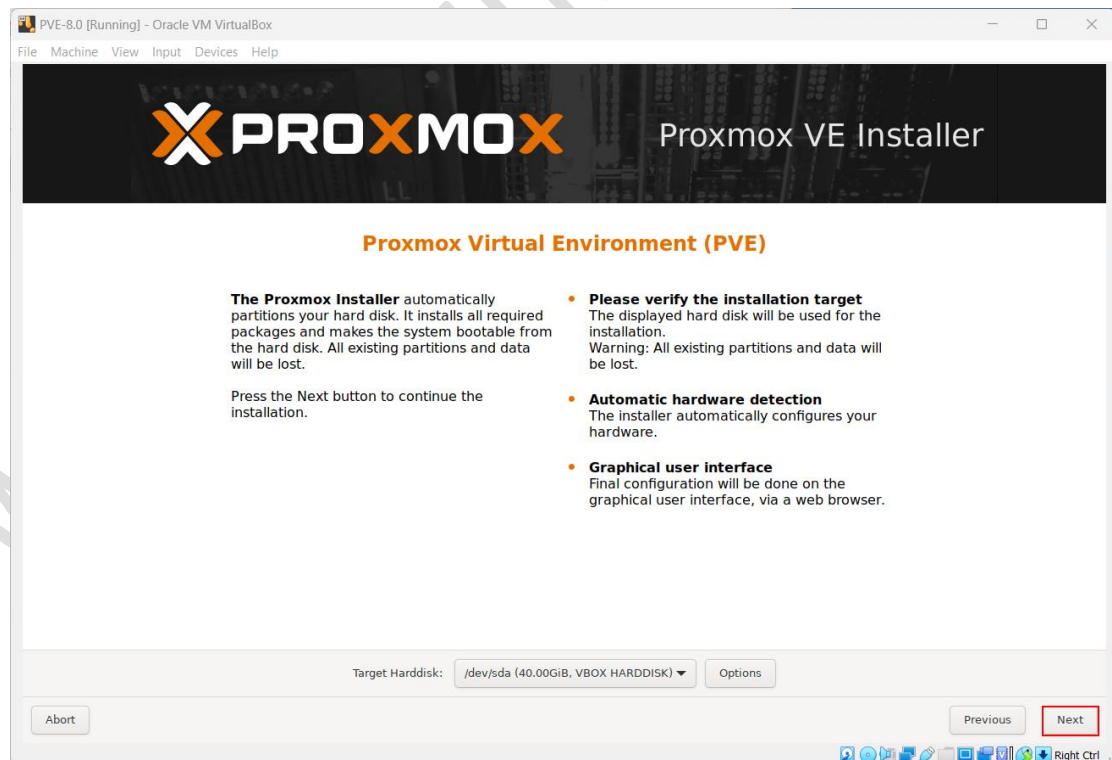
Terdapat beberapa pilihan yang tampil yaitu *Install Proxmox VE (Graphical)* untuk menginstalasi secara normal berbasis *Graphical User Interface (GUI)*, *Install Proxmox VE (Console)* untuk menginstalasi secara normal dengan antarmuka berbasis teks, *Advanced Options* untuk menampilkan pilihan mode instalasi lebih lanjut yang mendukung mode *debug*. Ketika mode debug akan membuka *shell console* pada beberapa tahapan instalasi yang membantu melakukan *debug* jika terjadi kesalahan dimana umumnya digunakan oleh developer, *Rescue Boot* (untuk memperbaiki sistem Proxmox yang telah terinstalasi ketika tidak dapat melakukan *booting* dengan normal), *Test Memory* (untuk melakukan pengujian pada RAM yang terpasang pada komputer apakah berfungsi dan bebas dari kesalahan atau *error*). Secara default telah terpilih **Install Proxmox VE (Graphical)**. Tekan tombol **Enter** untuk melanjutkan instalasi pada mode tersebut.

14. Tampil kotak dialog persetujuan lisensi “**GNU Affero General Public License**”, seperti terlihat pada gambar berikut:



Klik tombol **I Agree** untuk menyetujui lisensi dan melanjutkan instalasi.

15. Tampil kotak dialog **Proxmox Virtualization Environment (PVE)** untuk memilih **Target hardisk** sebagai lokasi instalasi, seperti terlihat pada gambar berikut:

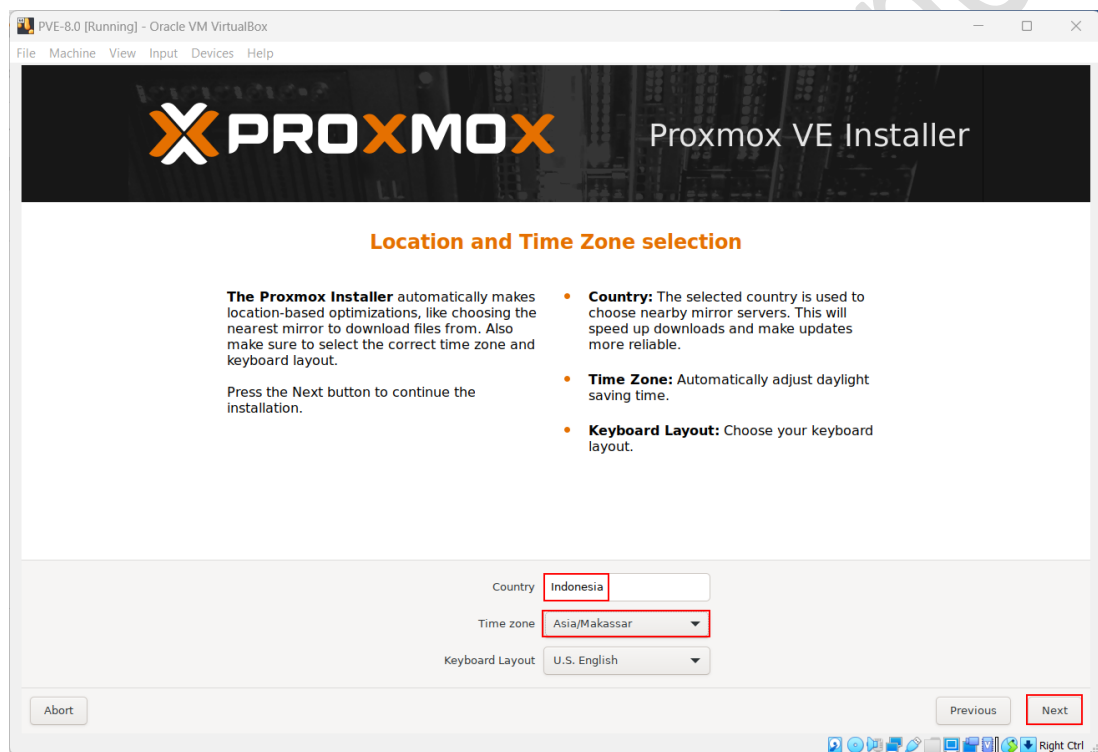


Terlihat **Target Hardisk** yang telah terpilih adalah **/dev/sda** dengan kapasitas **40GB**. *Installer Proxmox* akan secara otomatis membuat partisi pada hardisk dan

menginstalasi paket-paket yang dibutuhkan serta membuat sistem dapat di boot dari hardisk. **Perhatian:** keseluruhan partisi dan data akan hilang. *Installer* akan menggunakan *Logical Volume Manager (LVM)* apabila file system yang dipilih adalah **ext3**, **ext4** atau **xfs**. Secara default telah terpilih **ext4**. Jika diperlukan dapat pula dilakukan pengaturan jenis *file system* dan parameter LVM lainnya dengan menekan tombol **Options**.

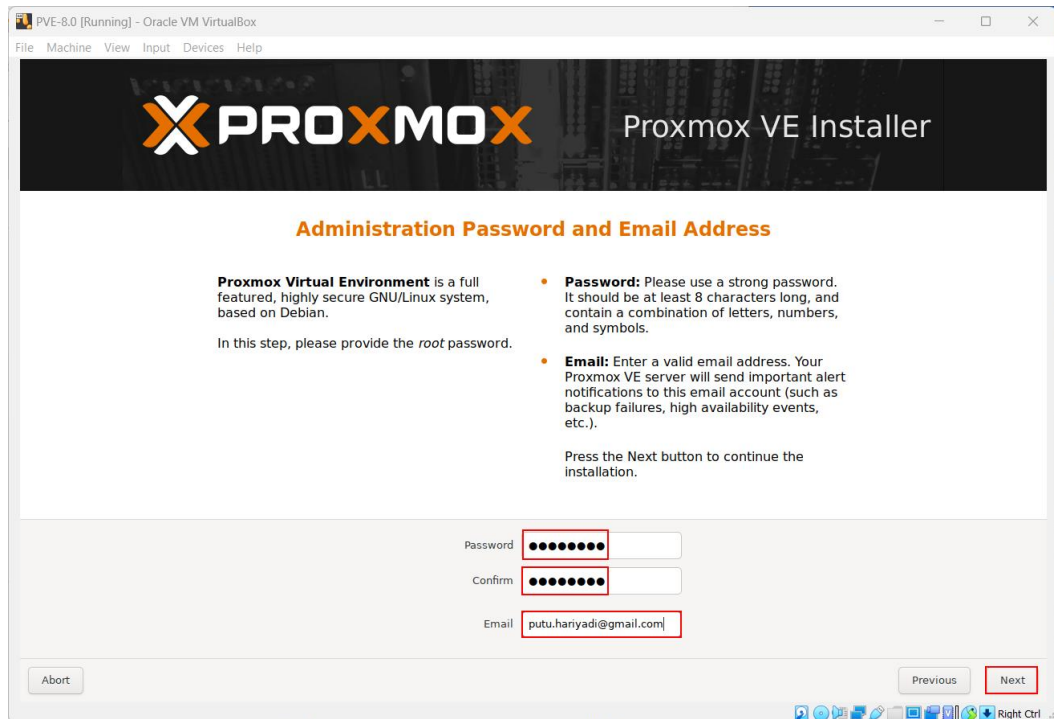
Klik tombol **Next** untuk melanjutkan instalasi.

16. Tampil kotak dialog “**Location and Time Zone selection**” untuk mengatur *Country*, *Time zone* dan *Keyboard Layout*, seperti terlihat pada gambar berikut:



Pada isian **Country** masukkan **Indonesia**. Sedangkan pengaturan zone waktu dapat dilakukan dengan memilih menu *dropdown* dari parameter **Time zone**. Untuk Waktu Indonesia Barat (WIB) pilih *Asia/Jakarta*, untuk Waktu Indonesia Tengah (WITA) pilih *Asia/Makassar*, sedangkan Wilayah Indonesia Timur (WIT) pilih *Asia/Jayapura*. Pilih **Asia/Makassar**. Klik tombol **Next** untuk melanjutkan.

17. Tampil kotak dialog **Administration Password and E-mail Address** untuk mengatur *Password* dari user “*root*” dan *E-mail*, seperti terlihat pada gambar berikut:

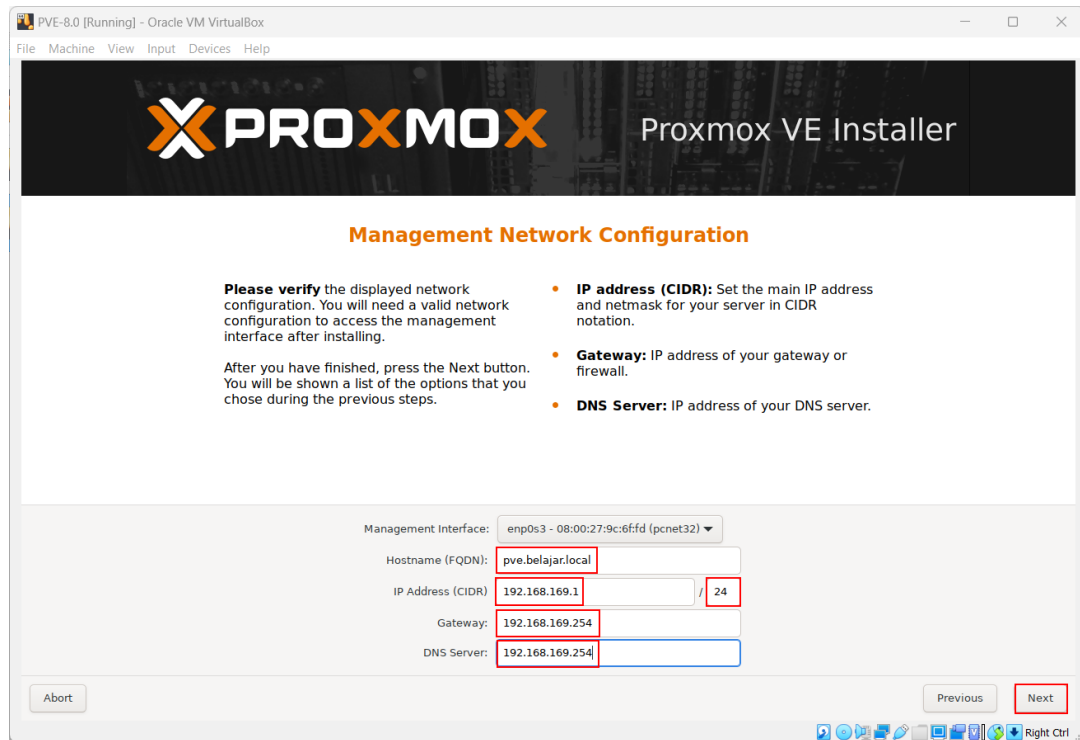


Pada isian **Password** dan **Confirm**, masukkan sandi login yang akan digunakan oleh user “**root**”, sebagai contoh “**12345678**”. Sedangkan pada isian **E-mail**, masukkan alamat untuk yang akan digunakan oleh Proxmox untuk mengirimkan notifikasi terkait kegagalan *backup*, *high availability events*, dan lainnya, sebagai contoh **putu.hariyadi@gmail.com**. Tekan tombol **Next** untuk melanjutkan instalasi.

18. Tampil kotak dialog **Management Network Configuration** untuk mengatur konfigurasi jaringan. Lengkapi isian dari masing-masing parameter berikut:

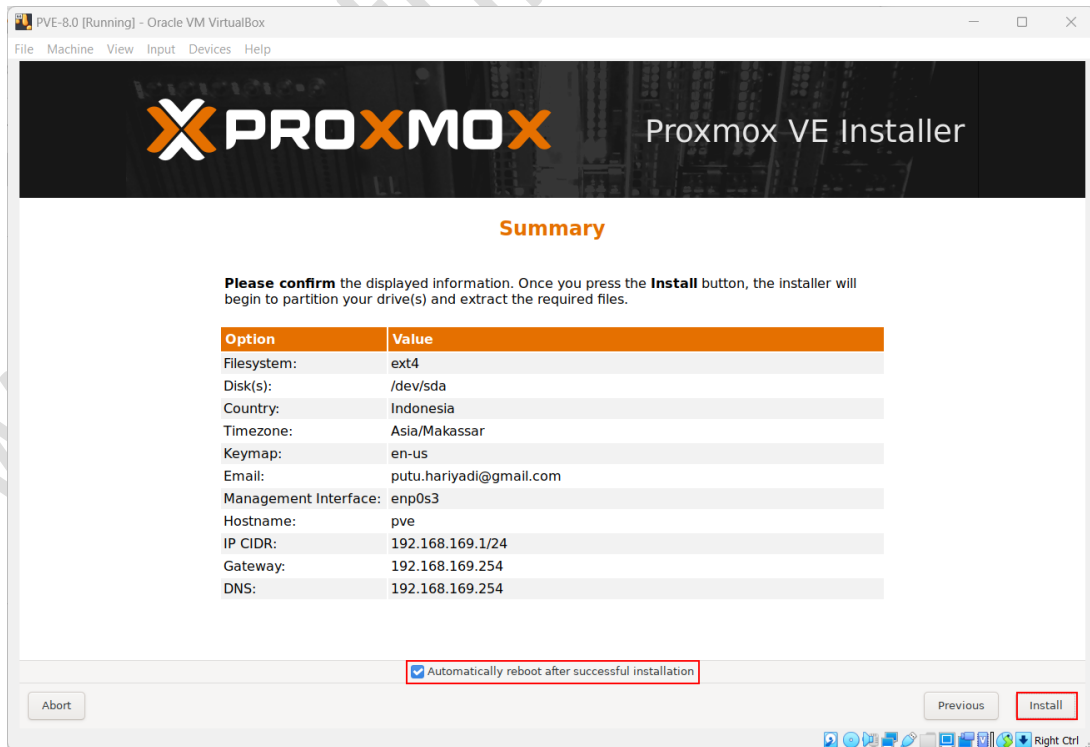
- Hostname (FQDN)**, masukkan nama komputer dengan format *Fully Qualified Domain Name*, sebagai contoh **pve.belajar.local**.
- IP Address (CIDR)**, masukkan alamat IP yang digunakan oleh Proxmox yaitu **192.168.169.1/24** sesuai dengan rancangan jaringan ujicoba.
- Gateway**, masukkan alamat *gateway* untuk komunikasi ke beda jaringan atau ke *Internet*, sebagai contoh **192.168.169.254**.
- DNS Server**, masukkan alamat *server Domain Name System (DNS)* untuk mentranslasikan nama domain ke alamat IP dan sebaliknya, sebagai contoh **192.168.169.254**.

seperti terlihat pada gambar berikut:



Tekan tombol **Next** untuk melanjutkan instalasi.

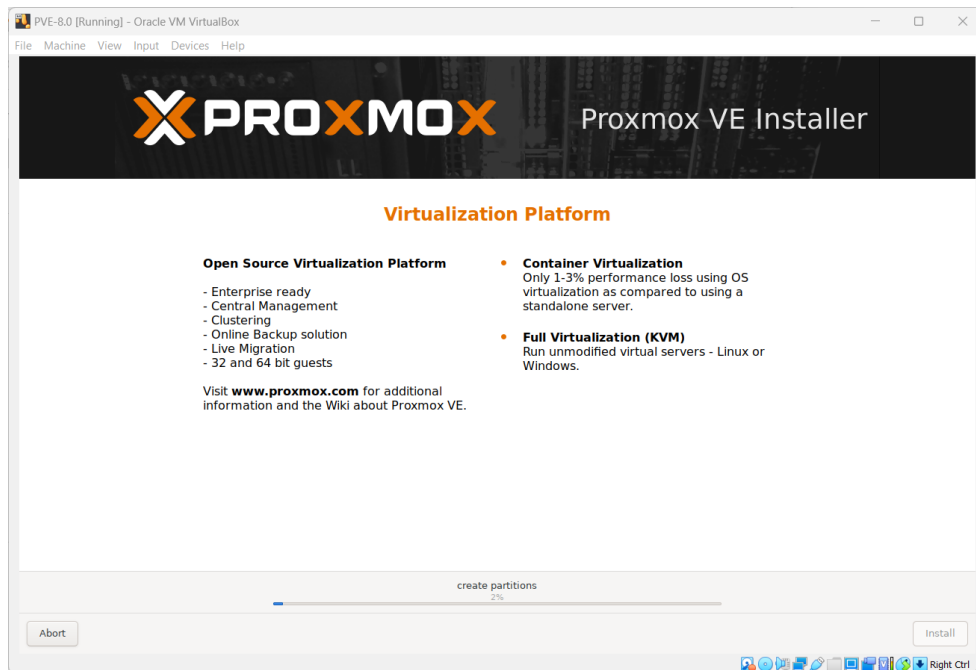
19. Tampil kotak **Summary** yang menampilkan rangkuman informasi pengaturan yang telah dilakukan pada langkah-langkah sebelumnya, seperti terlihat pada gambar berikut:



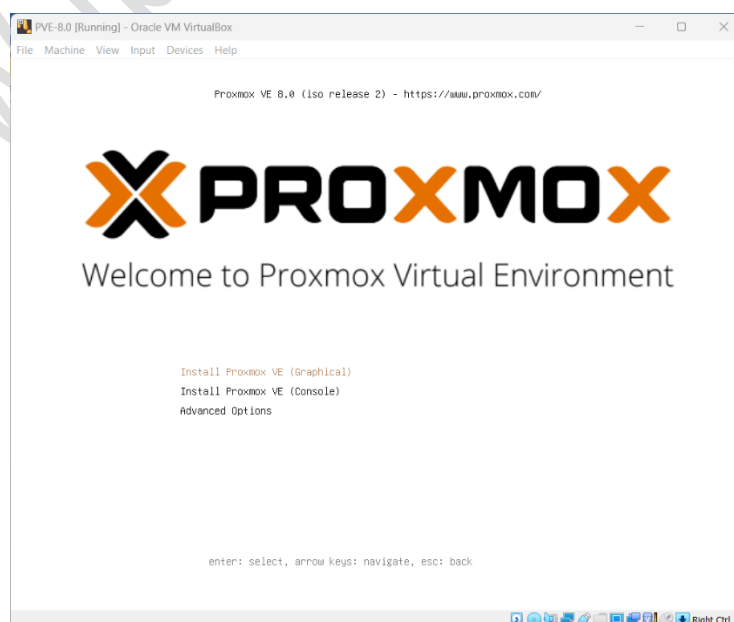
Pada bagian bawah dari kotak dialog ini juga terdapat *checkbox* pengaturan “*Automatically reboot after successful installation*” yang telah tercentang sehingga setelah instalasi sukses dilakukan akan melakukan *reboot* secara otomatis.

Tekan tombol **Install** untuk memulai proses instalasi.


20. Tampil kotak dialog yang menampilkan proses pembuatan partisi, format hardisk dan penyalinan paket-paket ke target hardisk, seperti terlihat pada gambar berikut:

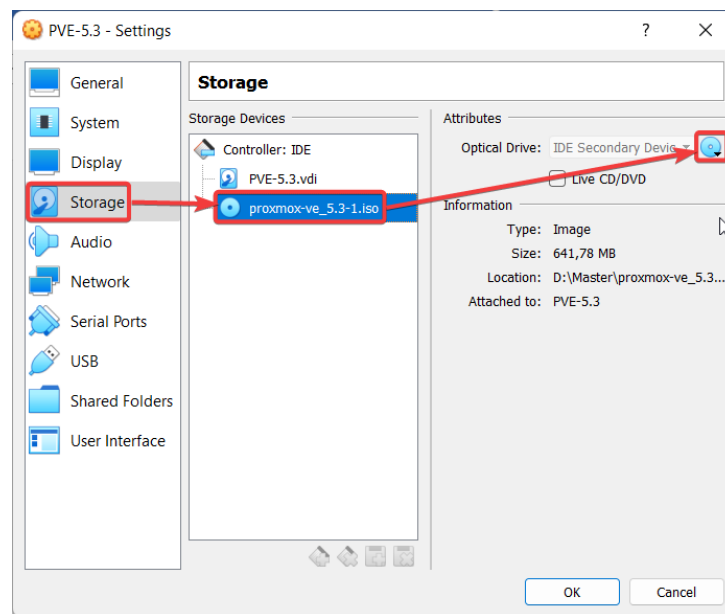


Tunggu hingga proses instalasi selesai dan pada kotak dialog **PVE-8.0 [Running] – Oracle VM VirtualBox** menampilkan kembali menu awal instalasi berupa *Welcome to Proxmox Virtual Environment*, seperti terlihat pada gambar berikut:

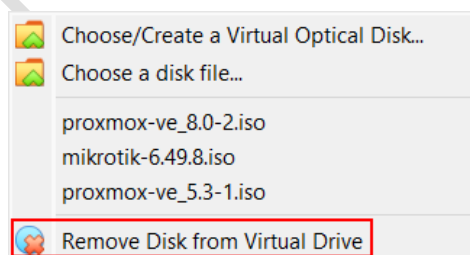


Hal ini terjadi VM melakukan boot dari CD yang mengarah ke **file ISO Proxmox**. Untuk itu diperlukan penghapusan *disk* dari *virtual drive* dengan cara memilih menu **Machine > Settings** maka akan tampil kotak dialog **PVE-8.0 Settings**.

Pada panel sebelah kiri dari **PVE-8.0 Settings**, pilih **Storage** dan pada panel detail sebelah kanan yaitu di bagian **Storage Devices**, pilih **proxmox-ve_8.0-2.iso** yang ditandai dengan **icon CD**. Selanjutnya di bagian **Attributes**, klik pada **icon CD dengan tanda panah bawah**  dari pilihan **Optical Drive**, seperti yang ditunjukkan pada gambar berikut:

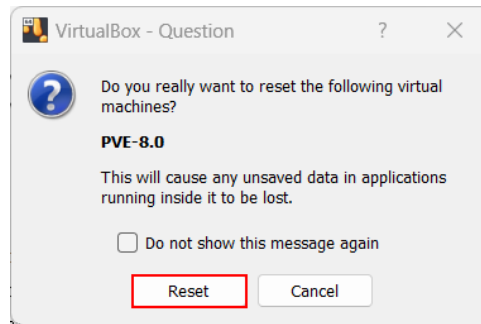


Pada *dropdown* yang tampil, pilih **Remove Disk from Virtual Drive**, seperti terlihat pada gambar berikut:



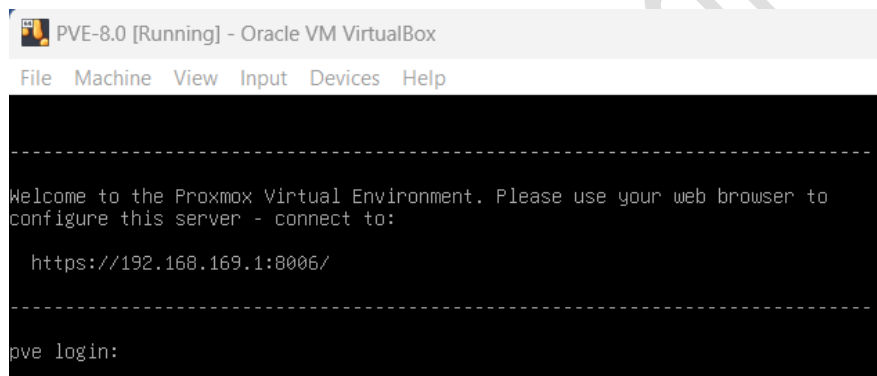
CD di panel detail bagian **Storage Devices** telah berubah menjadi **Empty**. Tekan tombol **OK** untuk menyimpan perubahan.

Selanjutnya lakukan **reboot VM** dengan cara memilih menu **Machine > Reset** maka akan tampil kotak dialog **VirtualBox – Question** dengan pesan “**Do you really want to reset the following virtual machine?**” yang mengkonfirmasi apakah ingin melakukan *reset virtual machine?*, seperti terlihat pada gambar berikut:



Tekan tombol **Reset** untuk melanjutkan proses tersebut maka VM akan melakukan *reboot*.

21. Tunggu hingga proses *reboot* selesai dilakukan. Setelah proses *reboot* selesai dilakukan maka akan tampak prompt login untuk otentikasi sebelum dapat mengakses sistem *Proxmox*, seperti terlihat pada gambar berikut:

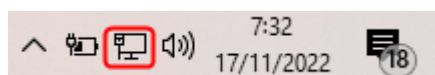


Konfigurasi selanjutnya dapat dilakukan melalui antarmuka web dari *Proxmox* yang dapat diakses pada alamat **http://192.168.169.1:8006**.

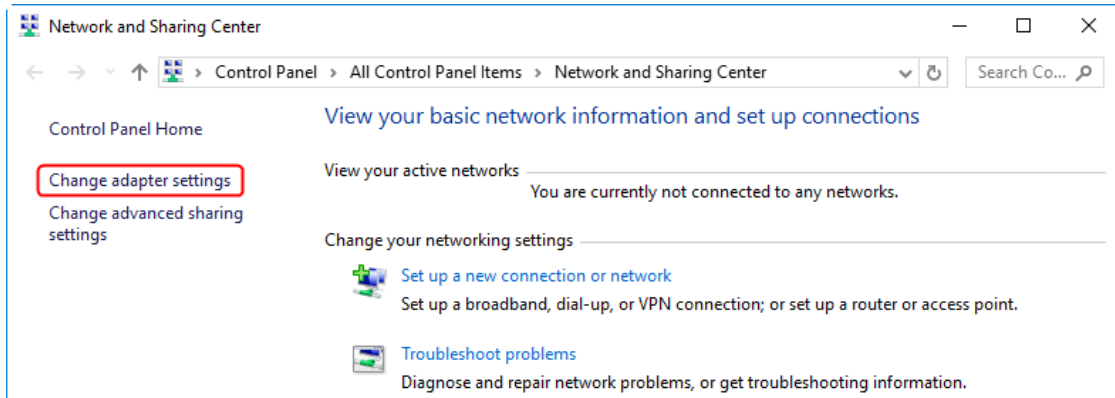
C. Konfigurasi Client Windows 10

Adapun langkah-langkah konfigurasi yang dilakukan pada *Client Windows 10* adalah sebagai berikut:

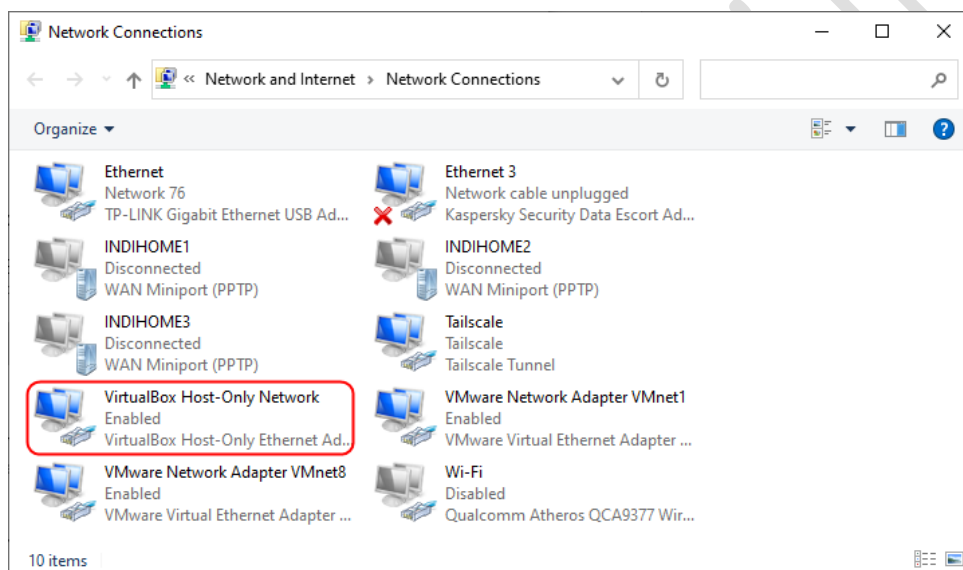
1. Mengatur pengalamanan IP dan parameter TCP/IP lainnya melalui **taskbar bagian pojok kanan bawah** dengan cara **klik kanan** pada icon **Network** dan pilih **Open Network & Sharing Center**, seperti terlihat pada gambar berikut:



2. Tampil kotak dialog **Network and Sharing Center**. Pilih **Change Adapter Settings**, seperti terlihat pada gambar berikut:

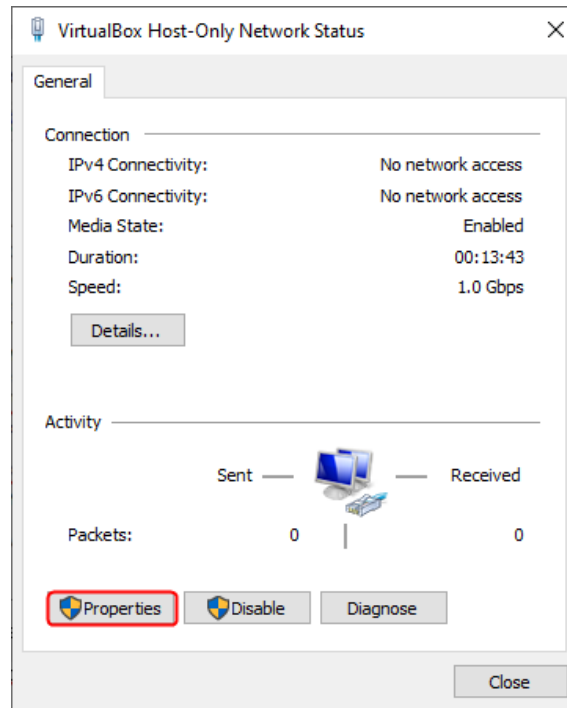


3. Tampil kotak dialog **Network Connections**. **Klik dua kali pada VirtualBox Host-Only Network**, seperti terlihat pada gambar berikut:

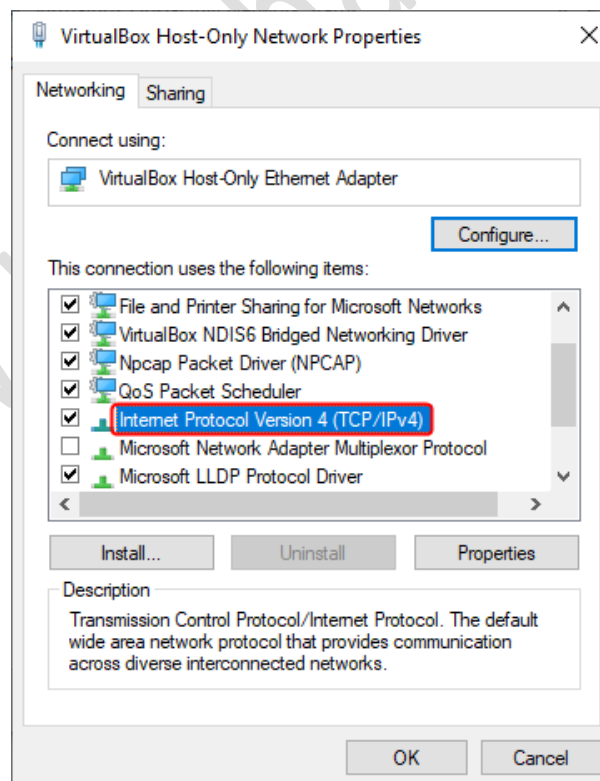


4. Tampil kotak dialog **VirtualBox Host-Only Network Status**. Klik tombol **Properties**, seperti terlihat pada gambar berikut:

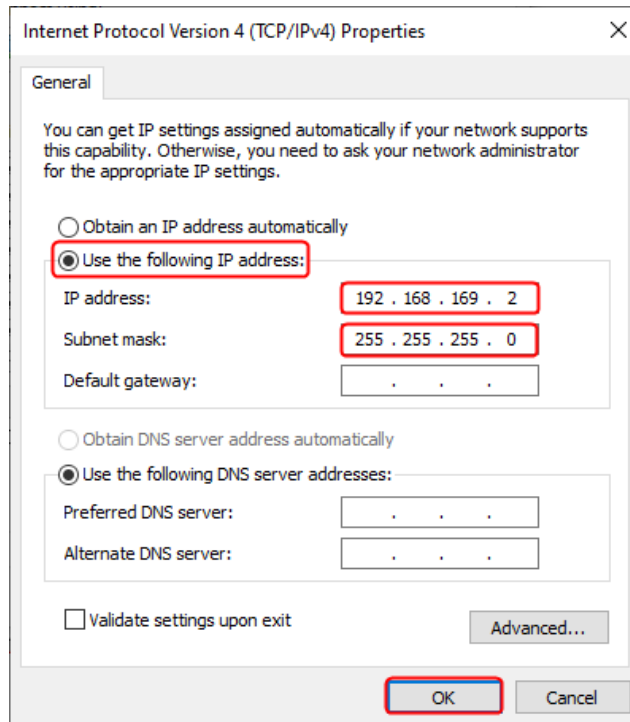
WWW.IPUTUHARIYADI.NET



5. Tampil kotak dialog **VirtualBox Host-Only Network Properties**. Pada bagian “**This connection uses the following items:**”, klik dua kali pada pilihan **Internet Protocol Version 4 (TCP/IPv4)**, seperti terlihat pada gambar berikut:

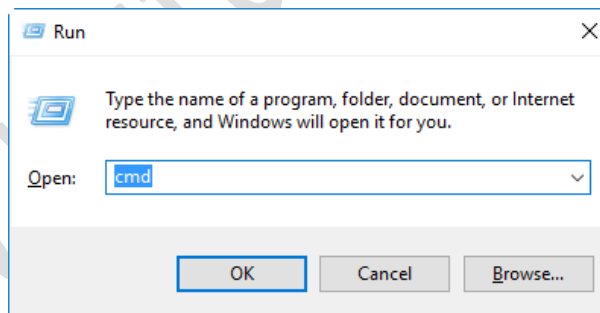


6. Tampil kotak dialog **Internet Protocol Version 4 (TCP/IPv4) Properties**. Pilih *Use the following IP Address*, seperti terlihat pada gambar berikut:



Pada isian **IP address:**, masukkan **192.168.169.2**. Sedangkan pada isian **Subnet mask:**, masukkan **255.255.255.0**. Klik tombol **OK > OK > Close**. Tutup kotak dialog **Network and Sharing Center**.

7. Buka **Command Prompt Windows** dengan menekan tombol **Windows+R**. Pada inputan form yang tampil, ketik "**cmd**" dan tekan tombol **Enter**.



8. Pada **Command Prompt** masukkan perintah "**ipconfig/all | more**" untuk memverifikasi pengalaman IP yang telah diatur, seperti terlihat pada gambar berikut:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.
C:\Users\ASUS>ipconfig/all | more
```

Tekan tombol **spasi** untuk menampilkan layar berikutnya. Pastikan adapter **VirtualBox Host-Only Network Adapter** telah menggunakan alamat IP dan subnetmask yang telah diatur pada langkah sebelumnya, seperti terlihat pada gambar berikut:

```

C:\WINDOWS\system32\cmd.exe
Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-11
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4dfa:b20:5f58:ed4a%17(Preferred)
IPv4 Address. . . . . : 192.168.169.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 1074397223
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-C8-8F-1C-50-3E-AA-B5-C3-12
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled

```

Tekan tombol **q** untuk keluar.

9. Verifikasi koneksi dari *client Windows 10* ke *VM Proxmox* menggunakan perintah “**ping 192.168.169.1**” pada **Command Prompt Windows**, seperti terlihat pada gambar berikut:

```

C:\WINDOWS\system32\cmd.exe

C:\Users\ASUS>ping 192.168.169.1

Pinging 192.168.169.1 with 32 bytes of data:
Reply from 192.168.169.1: bytes=32 time<1ms TTL=64
Reply from 192.168.169.1: bytes=32 time=1ms TTL=64
Reply from 192.168.169.1: bytes=32 time<1ms TTL=64
Reply from 192.168.169.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.169.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

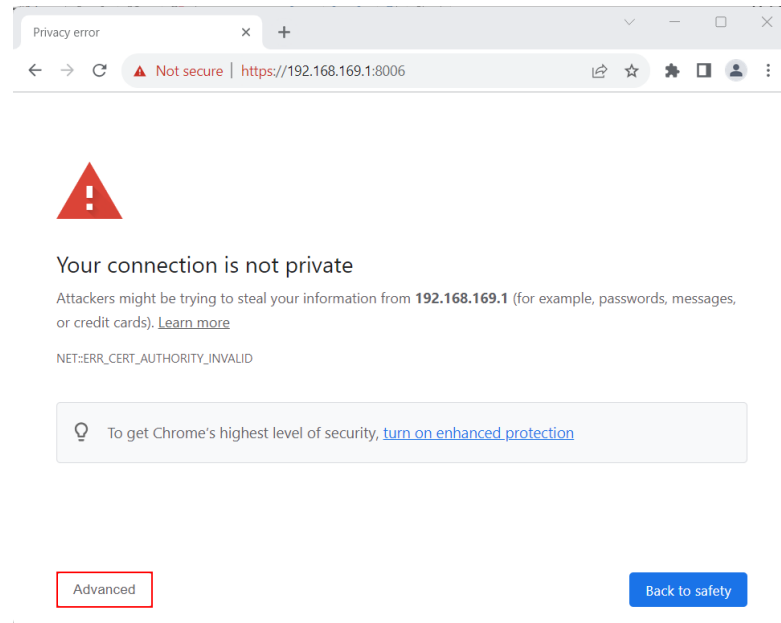
```

Terlihat koneksi ke *VM Proxmox* telah berhasil dilakukan.

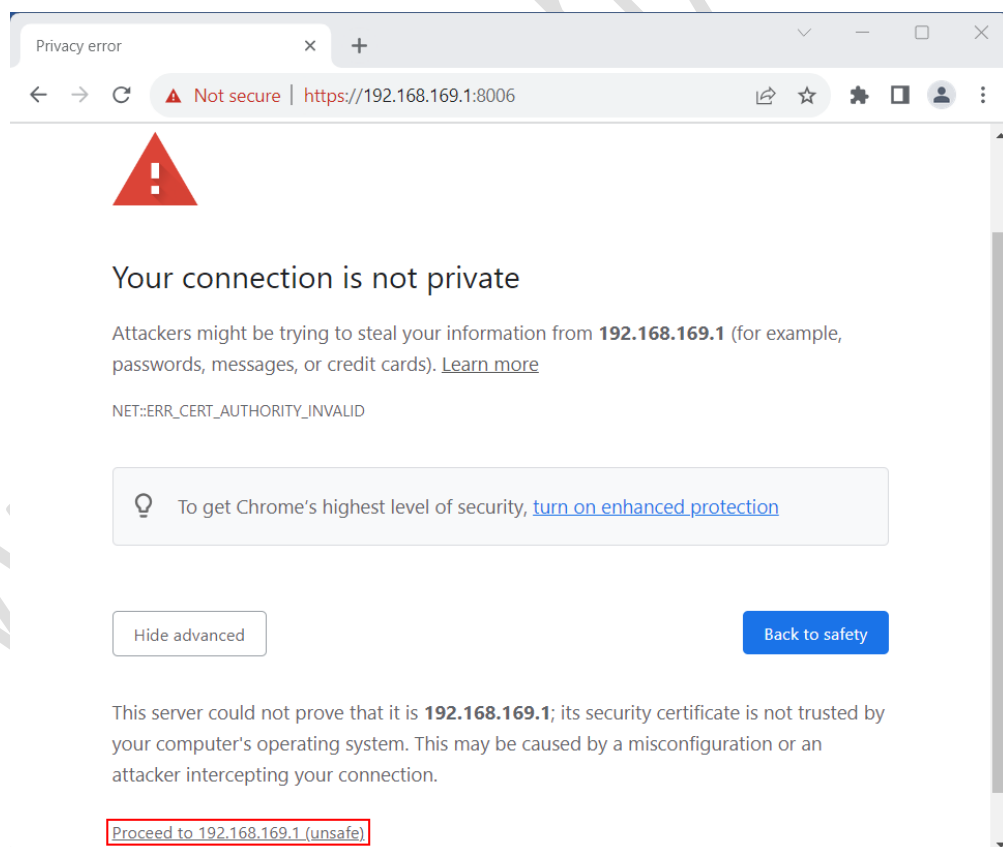
D. Konfigurasi Proxmox VE 8.0

Adapun langkah-langkah untuk mengkonfigurasi Proxmox VE 8.0 melalui antarmuka berbasis web adalah sebagai berikut:

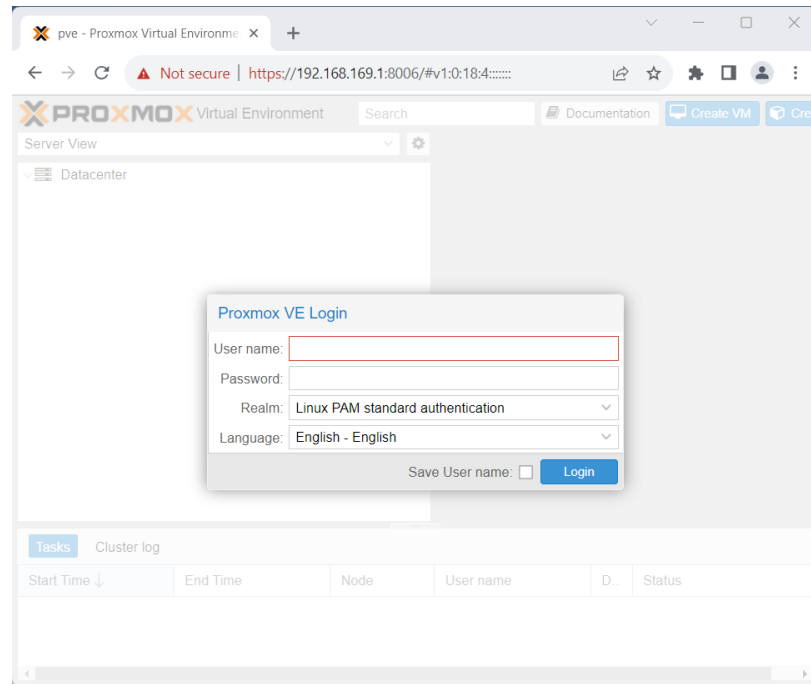
1. Buka *browser* sebagai contoh menggunakan **Chrome**. Pada address bar dari browser, masukkan URL <https://192.168.169.1:8006>. Hasil pengaksesan, seperti terlihat pada gambar berikut:



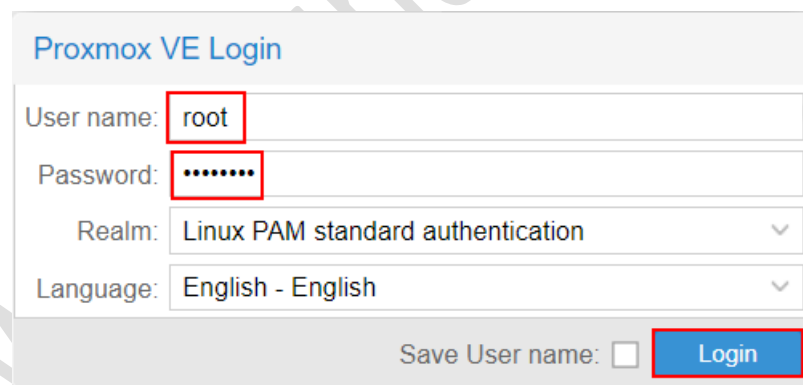
Tampil pesan peringatan **“Your connection is not private”**. Klik **Advanced** untuk melanjutkan pengaksesan dan klik link **“Proceed to 192.168.169.1 (unsafe)”**, seperti terlihat pada gambar berikut:



Maka *web interface* dari konfigurasi *Proxmox* berhasil diakses, seperti terlihat pada gambar berikut:

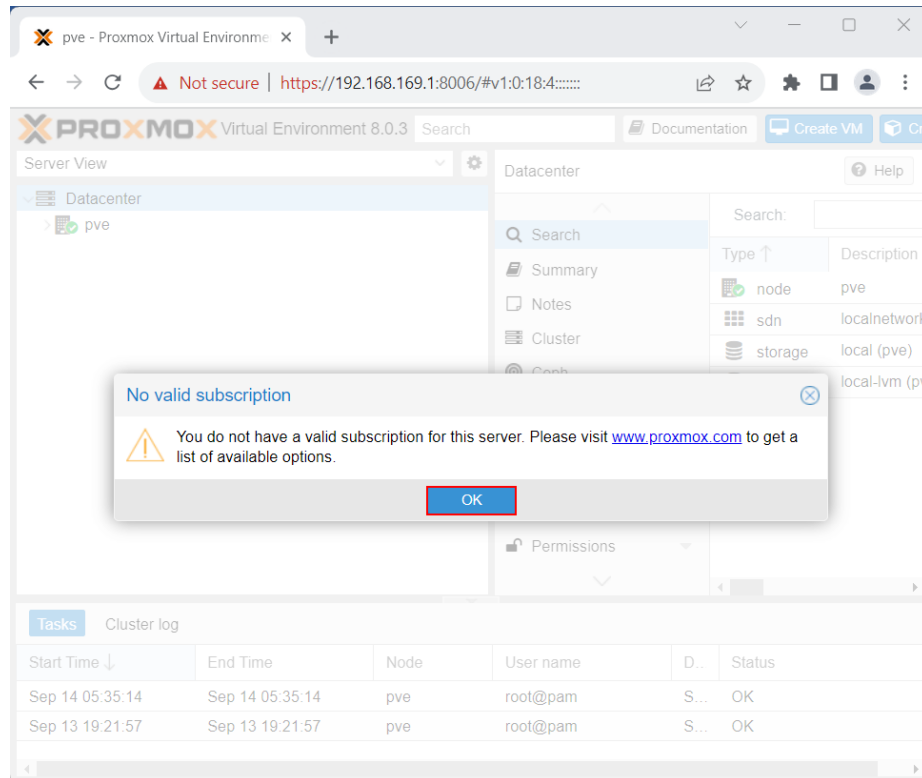


2. Pada kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**, seperti terlihat pada gambar berikut:



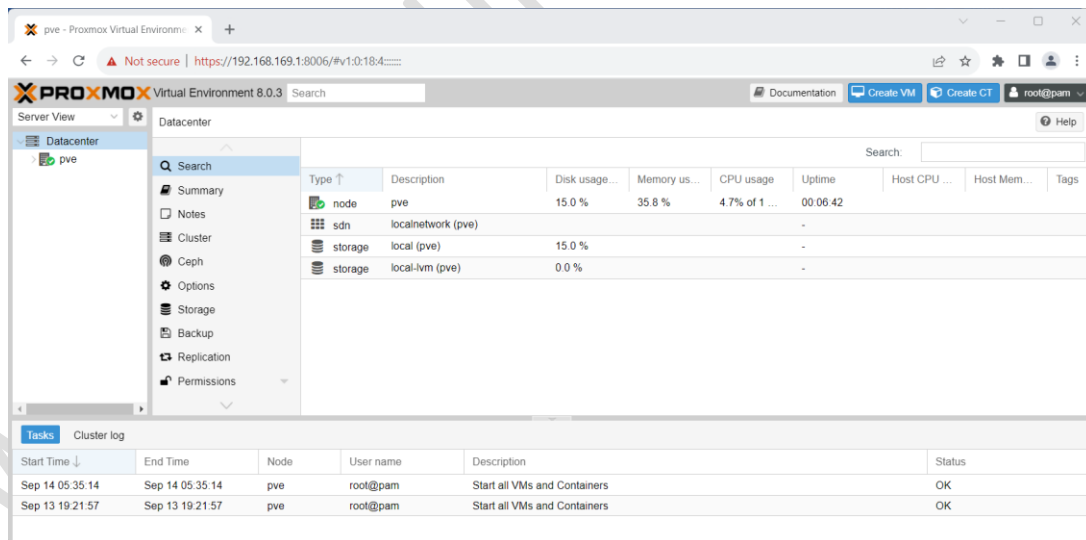
Klik tombol **Login**.

3. Tampil kotak dialog “**No valid subscription**” yang menginformasikan bahwa Anda tidak memiliki *subscription* yang valid untuk server ini, seperti terlihat pada gambar berikut:



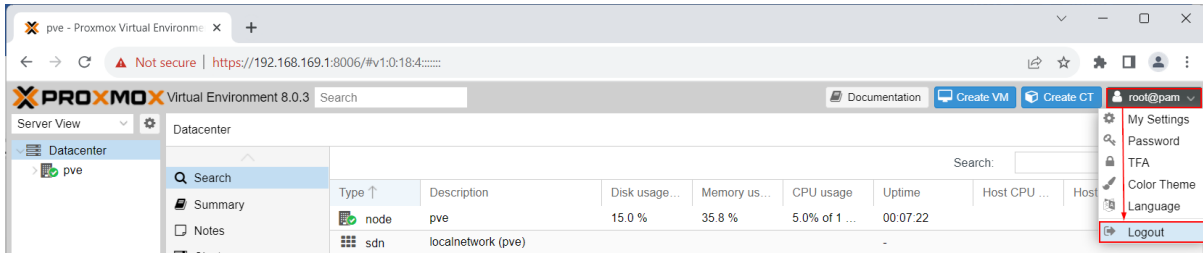
Pilihan jenis *subscription* dapat diakses lebih lanjut pada situs Proxmox di alamat www.proxmox.com. Klik tombol **OK**.

4. Tampil halaman *Server View* dari *Proxmox*, seperti terlihat pada gambar berikut:



Selanjutnya Anda dapat melakukan aktivitas manajemen Proxmox seperti mengunggah file *image Template Linux Container* atau file *ISO image*, pembuatan *Virtual Machine (Create VM)* atau *Container (Create CT)* dan lain sebagainya.

5. Untuk keluar dari *web interface* konfigurasi *Proxmox* maka klik pada *dropdown* menu **root@pam** di sebelah pojok kanan atas dan pilih **Logout**, seperti terlihat pada gambar berikut:



www.iputuhariyadi.net

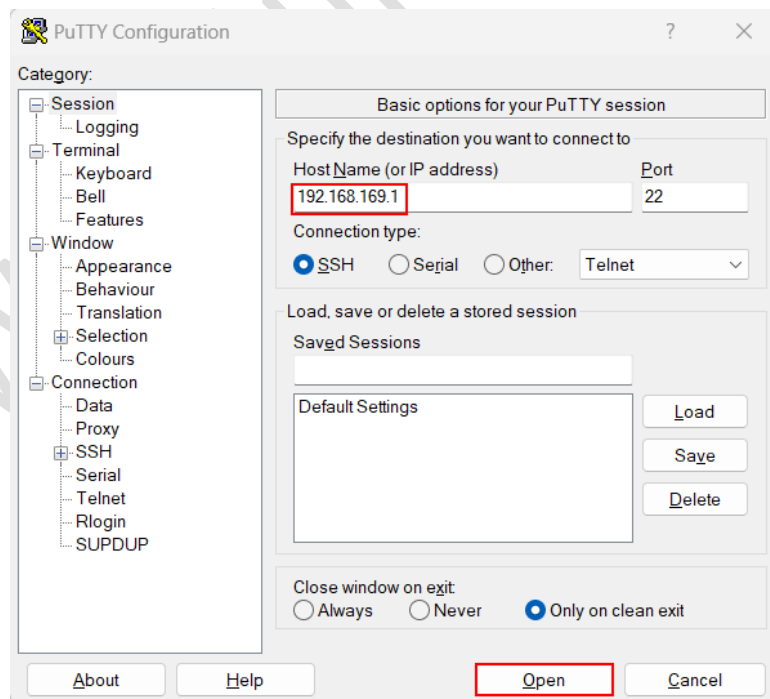
BAB II

MENONAKTIFKAN PESAN NOTIFIKASI “NO VALID
SUBSCRIPTION” PADA PROXMOX VE 8.0

Setelah berhasil melakukan “Instalasi dan Konfigurasi Proxmox VE 8.0 pada Oracle VirtualBox” di bab sebelumnya maka selanjutnya akan dilakukan penonaktifan pesan notifikasi “No Valid Subscription”. Pesan notifikasi ini akan selalu tampil ketika pengguna telah berhasil melalui proses otentikasi login pada *web interface Proxmox*. Proses penonaktifan pesan notifikasi tersebut memerlukan akses *console* atau *remote access* melalui *Secure Shell (SSH)*.

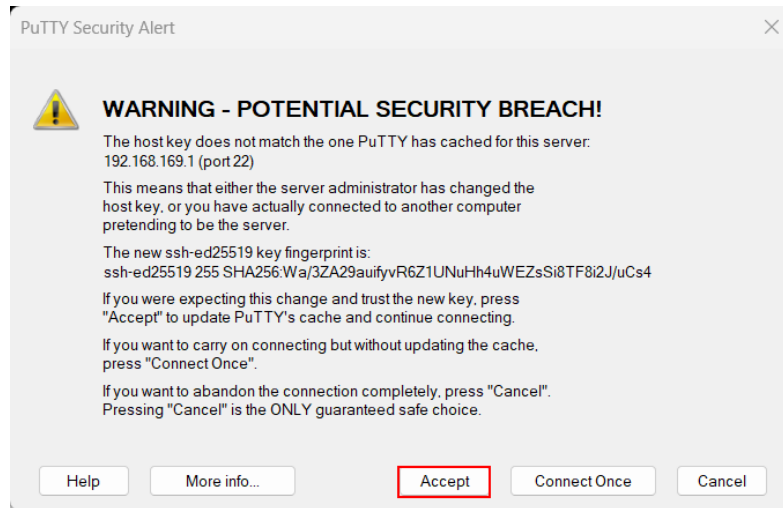
Adapun langkah-langkah penonaktifan pesan notifikasi tersebut melalui *SSH* adalah sebagai berikut:

1. Jalankan aplikasi *SSH Client*, sebagai contoh menggunakan *Putty*. Tampil kotak dialog *Putty Configuration*. Pada isian **Host Name (or IP Address)**, masukkan alamat IP dari *Server Proxmox* yaitu **192.168.169.1**, seperti terlihat pada gambar berikut:



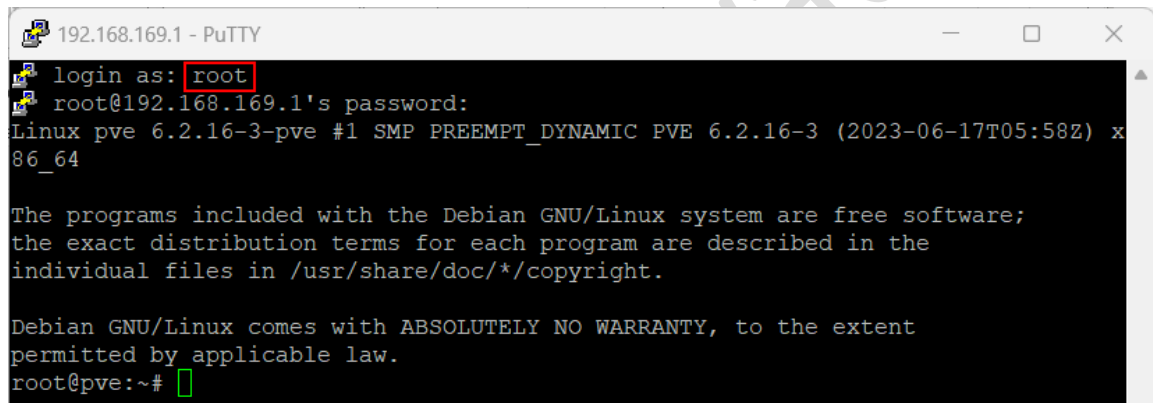
Klik tombol **Open**.

2. Tampil kotak dialog **Putty Security Alert** yang menampilkan pesan peringatan terkait potensi pelanggaran keamanan, seperti terlihat pada gambar berikut:



Klik tombol **Accept** untuk melanjutkan.

3. Tampil kotak dialog *PuTTY* yang meminta pengguna untuk melakukan proses otentikasi login ke *Server Proxmox*, seperti terlihat pada gambar berikut:



Pada inputan **login as:**, masukkan “**root**” dan tekan tombol **Enter**. Selanjutnya tampil inputan **password:**, masukkan “**12345678**” dan tekan tombol **Enter**. Apabila proses otentikasi berhasil dilakukan maka akan tampil *shell prompt #*.

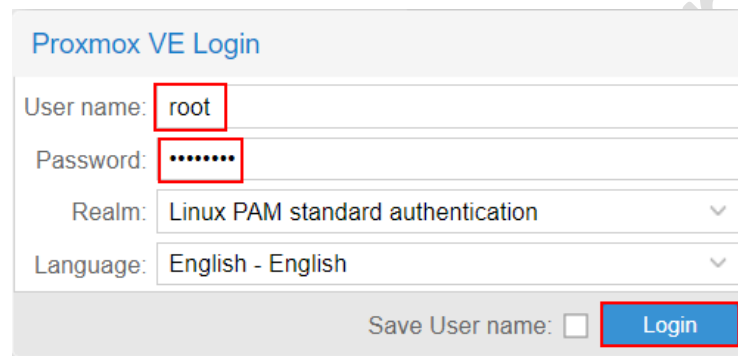
4. Mengubah parameter pada file `"/usr/share/javascript/proxmox-widget-toolkit/proxmoxlib.js"` yaitu: `Ext.Msg.show({ title: gettext('No valid sub menjadi void({ //Ext.Msg.show({` pada baris 549 dari file tersebut. Selain itu juga sekaligus membuat *file backup* dengan nama “**proxmoxlib.js.bak**” dan melakukan *restart service pveproxy.service* untuk mengaktifkan perubahan yaitu dengan mengeksekusi perintah berikut:

```
# sed -Ezi.bak "s/(Ext.Msg.show\(\{\s+title: gettext\('No
valid sub)/void\(\{\ \\/\1/g" /usr/share/javascript/proxmox-
widget-toolkit/proxmoxlib.js && systemctl restart
pveproxy.service
```

- Keluar dari SSH.

```
# exit
```

- Memverifikasi hasil penonaktifkan pesan notifikasi dengan mengakses *web interface* dari *Proxmox*. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
- Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**, seperti terlihat pada gambar berikut:



Proxmox VE Login

User name:

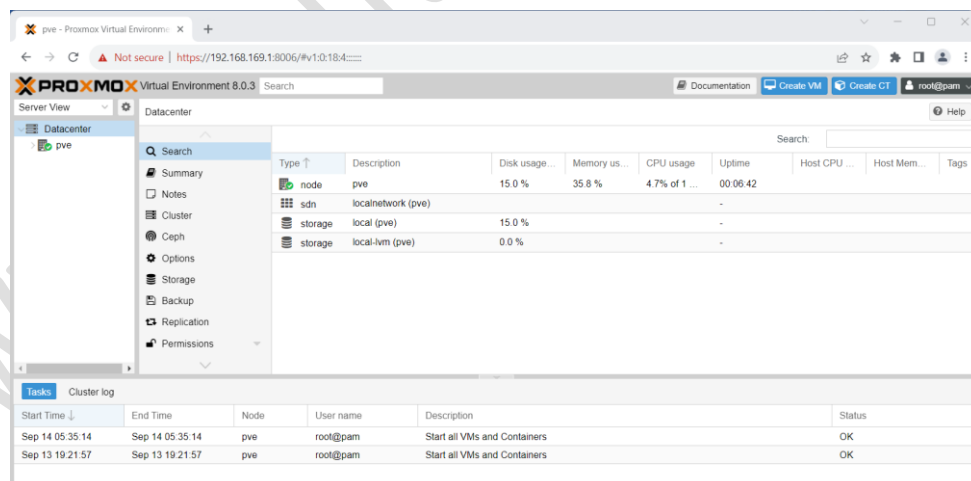
Password:

Realm:

Language:

Save User name:

Klik tombol **Login**. Pesan notifikasi “**No Valid Subscription**” tidak tampil. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*, seperti pada gambar berikut:

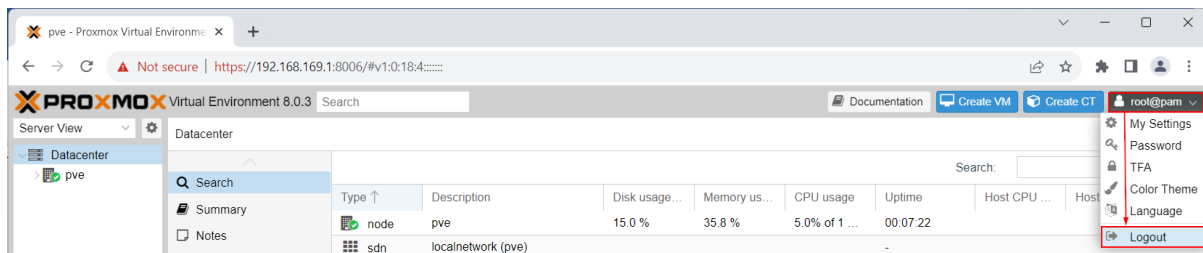


Type	Description	Disk usage...	Memory us...	CPU usage	Uptime	Host CPU ...	Host Mem...	Tags
node	pve	15.0 %	35.8 %	4.7% of 1 ...	00:06:42			
sdn	localnetwork (pve)							
storage	local (pve)	15.0 %						
storage	local-lvm (pve)	0.0 %						

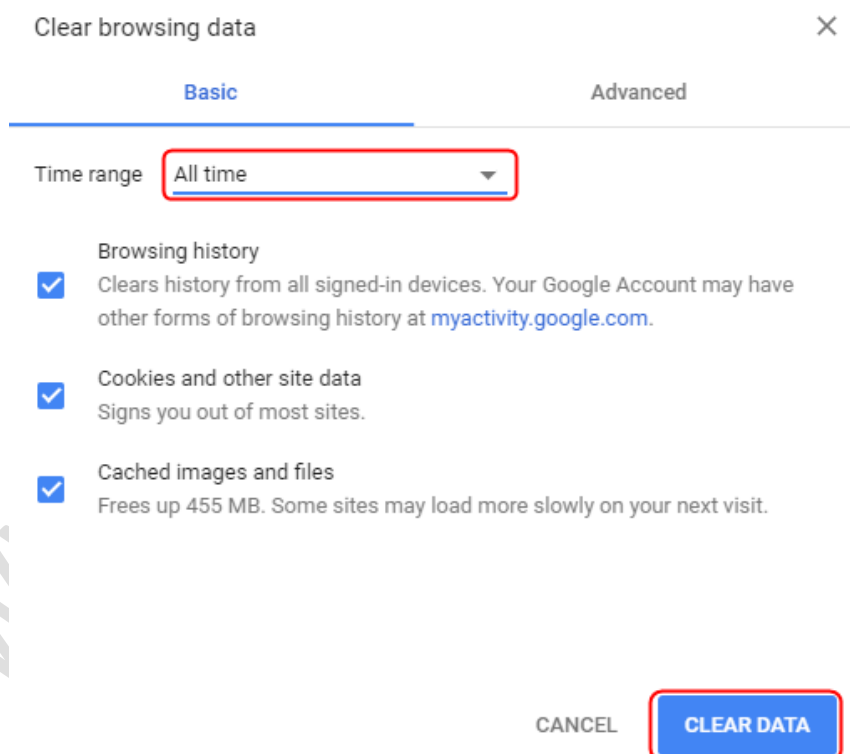
Start Time	End Time	Node	User name	Description	Status
Sep 14 05:35:14	Sep 14 05:35:14	pve	root@pam	Start all VMs and Containers	OK
Sep 13 19:21:57	Sep 13 19:21:57	pve	root@pam	Start all VMs and Containers	OK

Selamat Anda telah berhasil menonaktifkan pesan notifikasi “**No Valid Subscription**” pada *Proxmox VE 8.0*.

8. Untuk keluar dari *web interface* konfigurasi *Proxmox* maka klik pada *dropdown* menu **root@pam** di sebelah pojok kanan atas dan pilih **Logout**, seperti terlihat pada gambar berikut:



Apabila pesan notifikasi masih tampil, maka lakukan penghapusan **Cookies** dari *browser* dengan menekan tombol **CTRL+SHIFT+DEL**. Tampil kotak dialog, **Clear browsing data**. Pada pilihan **Time range**, pilih **All time**, dan tekan tombol **CLEAR DATA**, seperti terlihat pada gambar berikut:



Selanjutnya lakukan percobaan pengaksesan kembali ke *web interface* dari *Proxmox* pada alamat **https://192.168.169.1:8006**.

BAB III

MANAJEMEN REPOSITORY PADA PROXMOX VE 8.0

Menurut *Wiki* dari *Proxmox*, *repository* merupakan kumpulan paket perangkat lunak yang dapat digunakan untuk menginstalasi perangkat lunak baru dan memperoleh pembaharuan terkait paket perangkat lunak yang telah terinstalasi. Secara *default* *PVE Enterprise Repository* dan *Ceph Enterprise Repository Subscription* telah aktif serta direkomendasikan untuk tetap digunakan bagi pengguna PVE yang melakukan *subscription* karena memuat paket yang paling stabil sehingga sangat cocok digunakan untuk *production*. Untuk dapat memanfaatkan *repository* ini maka diperlukan *subscription key* yang **BERBAYAR**. Detail informasi pembiayaan terkait *PVE subscription* dapat dilihat pada alamat <https://www.proxmox.com/en/proxmox-ve/pricing>. *File* yang memuat pengaturan *PVE Enterprise Repository Subscription* adalah `/etc/apt/sources.list.d/pve-enterprise.list`, dengan konten seperti berikut:

```
deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise
```

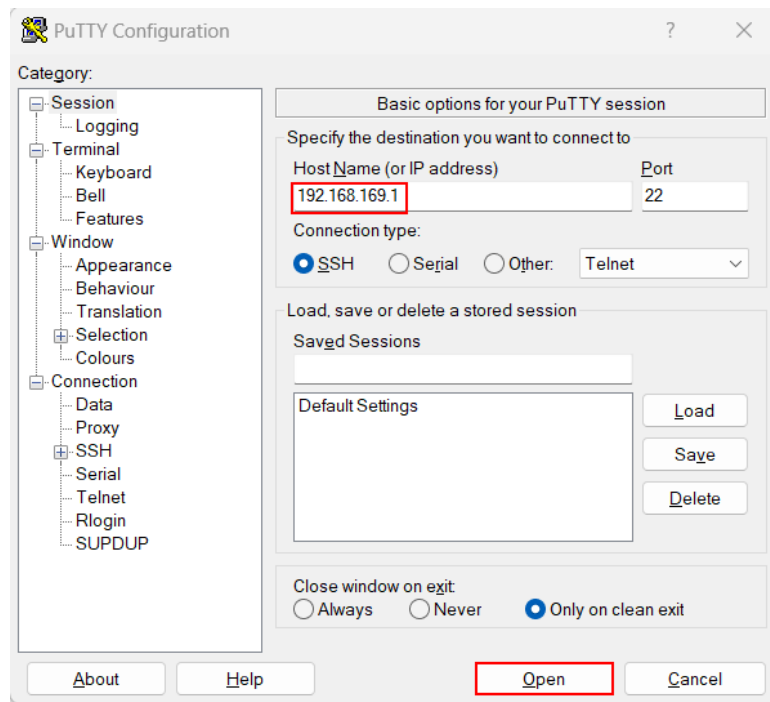
Sedangkan *file* yang memuat pengaturan *Ceph Enterprise Repository Subscription* adalah `/etc/apt/sources.list.d/ceph.list`, dengan konten seperti berikut:

```
deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise
```

Penonaktifan *PVE Enterprise Repository* dan *Ceph Enterprise Repository* diperlukan apabila tidak memiliki *subscription key* sehingga tidak memunculkan pesan kesalahan. Bagi pengguna PVE yang tidak memiliki *subscription key* dapat memanfaatkan *PVE No-Subscription Repository* dan *Ceph No-Subscription Repository*.

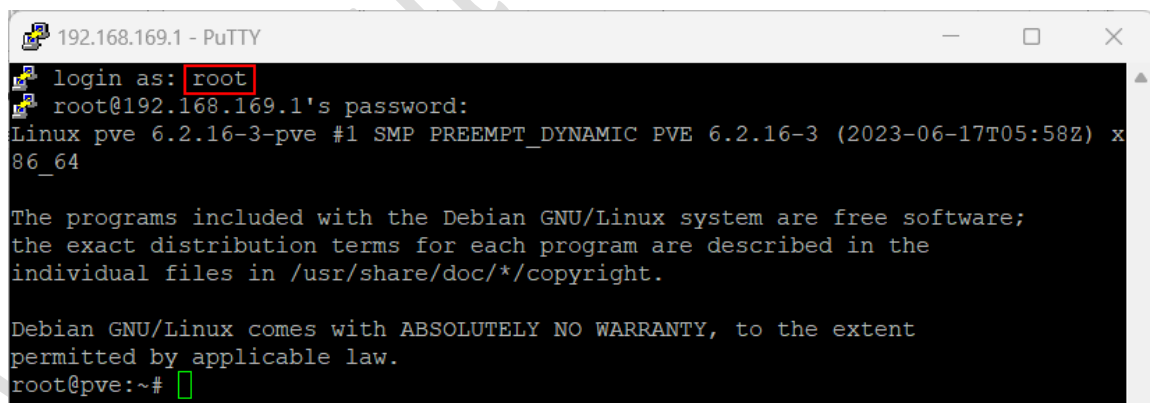
Adapun langkah-langkah untuk menonaktifkan *PVE Enterprise* dan *Ceph Enterprise Repository* serta mengaktifkan baik *PVE No-Subscription* dan *Ceph No-Subscription* melalui *SSH* adalah sebagai berikut:

1. Jalankan aplikasi *SSH Client*, sebagai contoh menggunakan *Putty*. Tampil kotak dialog *Putty Configuration*. Pada isian **Host Name (or IP Address)**, masukkan alamat IP dari *Server Proxmox* yaitu **192.168.169.1**, seperti terlihat pada gambar berikut:



Klik tombol **Open**.

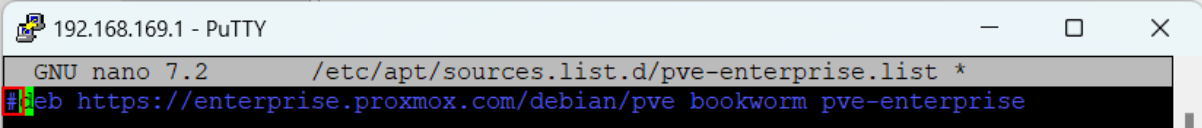
2. Tampil kotak dialog *Putty* yang meminta pengguna untuk melakukan proses otentikasi login ke *Server Proxmox*, seperti terlihat pada gambar berikut:



Pada inputan **login as:**, masukkan “**root**” dan tekan tombol **Enter**. Selanjutnya tampil inputan **password:**, masukkan “**12345678**” dan tekan tombol **Enter**. Apabila proses otentikasi berhasil dilakukan maka akan tampil *shell prompt #*.

3. Menonaktifkan *PVE Enterprise Repository* dengan cara menambahkan tanda # diawal baris dari konten pada file `/etc/apt/sources.list.d/pve-enterprise.list` menggunakan editor *nano*.

```
# nano /etc/apt/sources.list.d/pve-enterprise.list
```



```
192.168.169.1 - PuTTY
GNU nano 7.2 /etc/apt/sources.list.d/pve-enterprise.list *
#deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise
```

Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

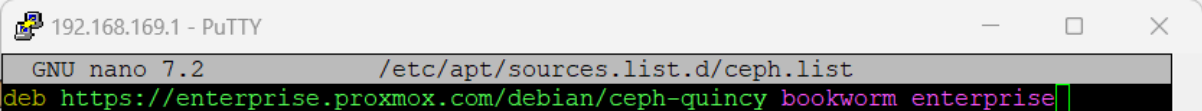
- Memverifikasi hasil penonaktifan *PVE Enterprise Repository* menggunakan perintah “`cat /etc/apt/sources.list.d/pve-enterprise.list`”.

```
root@pve:~# cat /etc/apt/sources.list.d/pve-enterprise.list
#deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise
```

Terlihat pada awal baris dari *file pve-enterprise.list* telah terdapat tanda **#** yang berfungsi sebagai komentar.

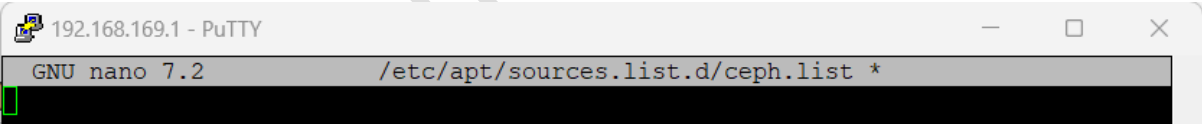
- Menonaktifkan *Ceph Enterprise Repository* dan mengaktifkan *Ceph No-Subscription Repository* pada *file /etc/apt/sources.list* menggunakan editor *nano*.

```
# nano /etc/apt/sources.list.d/ceph.list
```



```
192.168.169.1 - PuTTY
GNU nano 7.2 /etc/apt/sources.list.d/ceph.list
deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise
```

Lakukan penghapusan konten pada baris di posisi kursor saat ini berada dengan menekan tombol **CTRL+K**, sehingga hasilnya, seperti terlihat pada gambar berikut:

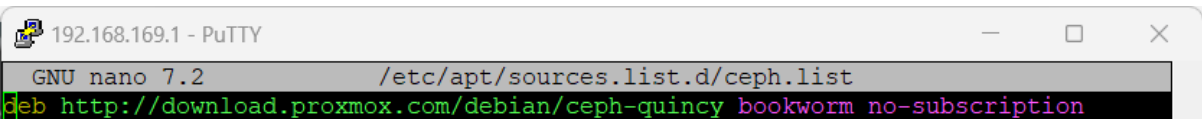


```
192.168.169.1 - PuTTY
GNU nano 7.2 /etc/apt/sources.list.d/ceph.list *
```

Lakukan penambahan parameter dengan nilai berikut sebagai konten dari *file* tersebut dan pastikan tercantum dalam satu baris:

```
deb http://download.proxmox.com/debian/ceph-quincy bookworm
no-subscription
```


Sehingga terlihat seperti gambar berikut:



```
192.168.169.1 - PuTTY
GNU nano 7.2 /etc/apt/sources.list.d/ceph.list
deb http://download.proxmox.com/debian/ceph-quincy bookworm no-subscription
```

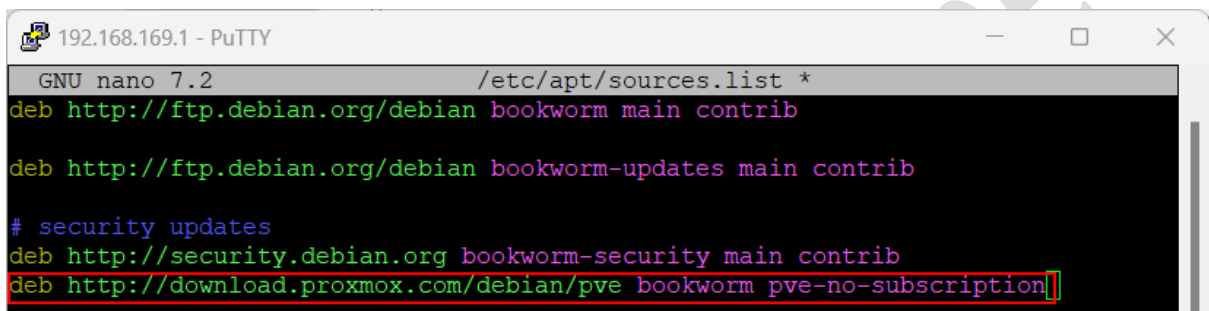
Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

- Memverifikasi hasil penonaktifan *Ceph Enterprise Repository* menggunakan perintah “`cat /etc/apt/sources.list.d/ceph.list`”.



```
192.168.169.1 - PuTTY
root@pve:~# cat /etc/apt/sources.list.d/ceph.list
deb http://download.proxmox.com/debian/ceph-quincy bookworm no-subscription
```

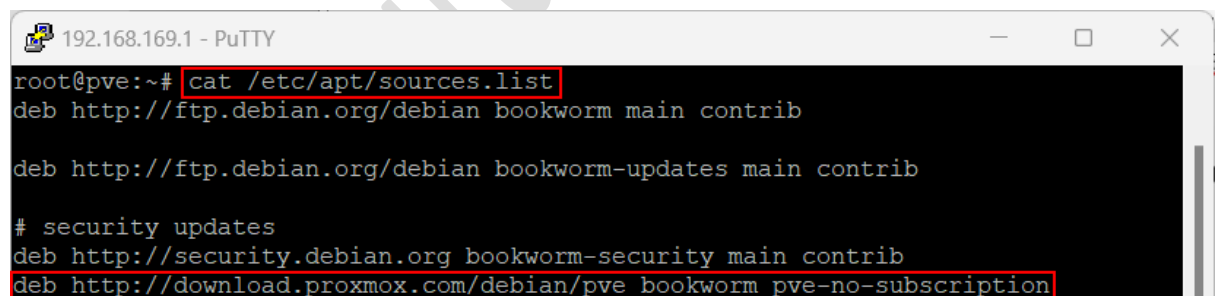
- Mengaktifkan *PVE No-Subscription* dengan cara menambahkan parameter “`deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription`” pada file `/etc/apt/sources.list` menggunakan editor *nano*.
`nano /etc/apt/sources.list`



```
192.168.169.1 - PuTTY
GNU nano 7.2 /etc/apt/sources.list *
deb http://ftp.debian.org/debian bookworm main contrib
deb http://ftp.debian.org/debian bookworm-updates main contrib
# security updates
deb http://security.debian.org bookworm-security main contrib
deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription
```

Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

- Memverifikasi hasil pengaturan *PVE No-Subscription Repository* menggunakan perintah “`cat /etc/apt/sources.list`”.

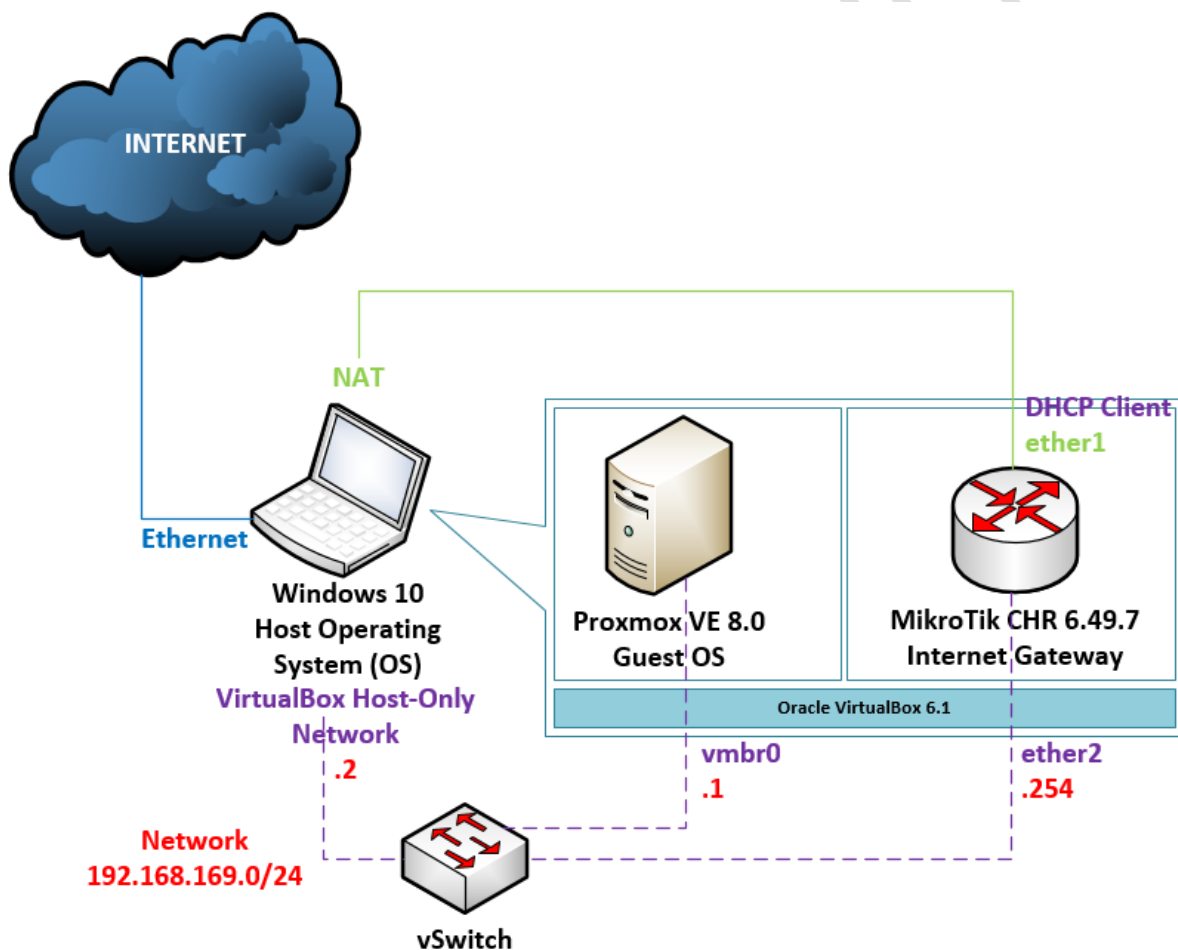


```
192.168.169.1 - PuTTY
root@pve:~# cat /etc/apt/sources.list
deb http://ftp.debian.org/debian bookworm main contrib
deb http://ftp.debian.org/debian bookworm-updates main contrib
# security updates
deb http://security.debian.org bookworm-security main contrib
deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription
```

BAB IV

INSTALASI DAN KONFIGURASI MIKROTIK CHR SEBAGAI INTERNET GATEWAY PADA ORACLE VIRTUALBOX

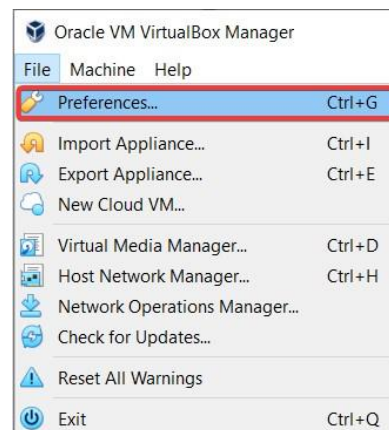
Untuk menjembatani kebutuhan akses *Internet* dari *Proxmox VE 8.0* maka pada *Oracle VirtualBox* akan diinstalasi **Mikrotik CHR 6.49.7** sebagai *Virtual Machine (VM)* dan dikonfigurasi sebagai *gateway* untuk berbagi pakai koneksi *Internet*, seperti terlihat pada gambar berikut:



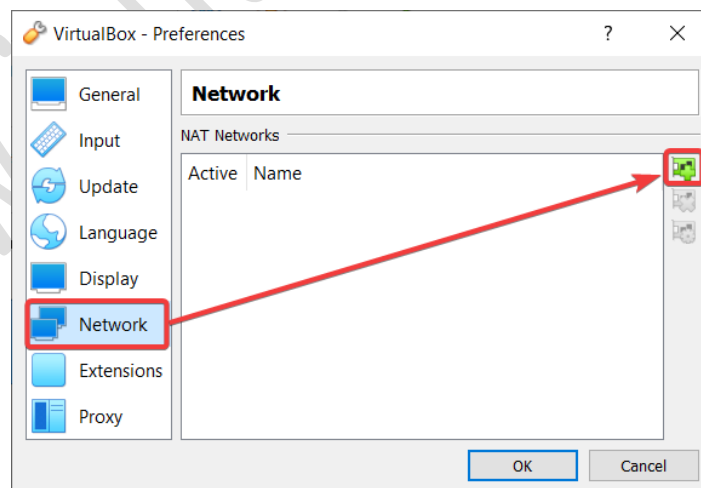
MikroTik CHR memiliki 2 (dua) *interface* yaitu **ether1** dengan jenis koneksi *NAT* dan **ether2** dengan jenis koneksi *host-only*. *Interface ether2* menggunakan alamat IP **192.168.169.254/24**. Sedangkan *interface ether1* dialokasi secara dinamis sehingga bertindak sebagai **DHCP Client**.

Adapun langkah-langkah instalasi dan konfigurasi *MikroTik CHR* sebagai *gateway Internet* pada *Oracle VirtualBox* adalah sebagai berikut:

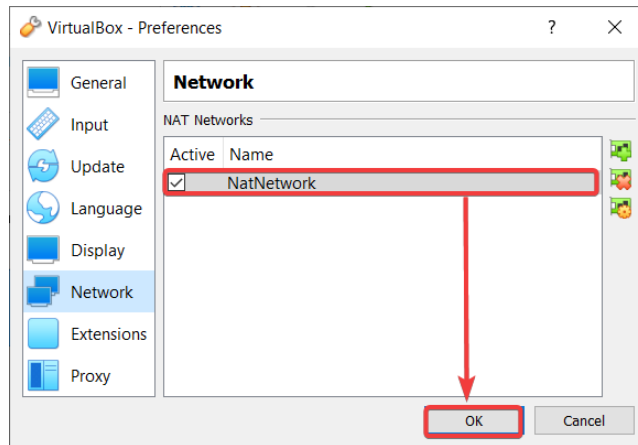
1. Jalankan aplikasi *Oracle VirtualBox* melalui **Start > Oracle VM VirtualBox > Oracle VM VirtualBox**.
2. Tampil aplikasi *Oracle VM VirtualBox Manager* dan lakukan penambahan **Network Address Translation (NAT) Network** dengan mengakses menu **File > Preferences** pada **Oracle VM VirtualBox Manager**, seperti yang ditunjukkan pada gambar berikut:



Tampil kotak dialog **VirtualBox – Preferences** dan pada panel menu sebelah kiri pilih **Network**. Pada panel detail dari *Network* di sebelah kanan, pilih *icon Adds new NAT Network*, seperti yang ditunjukkan pada gambar berikut:

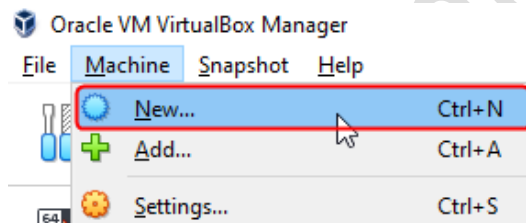


Terbentuk “**NatNetwork**” yang telah aktif, seperti terlihat pada gambar berikut:

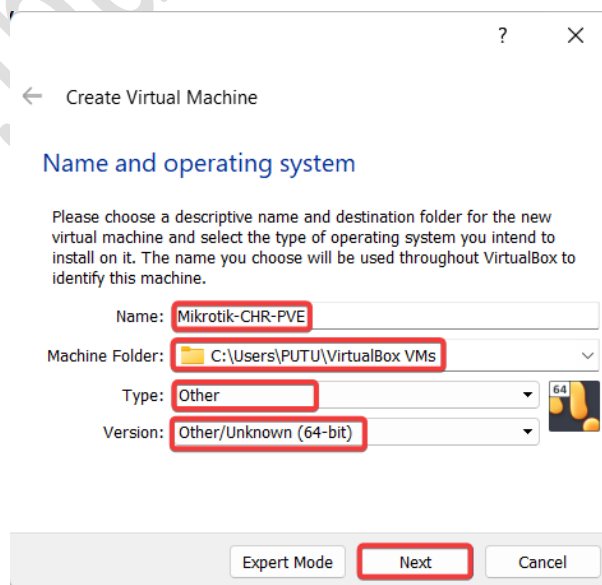


Klik tombol **OK** untuk menutup kotak dialog *VirtualBox - Preferences*.

3. Pada kotak dialog *Oracle VM VirtualBox Manager*, pilih menu **Machine > New** ...Untuk membuat *virtual machine* baru, seperti terlihat pada gambar berikut:



4. Tampil kotak dialog *Create Virtual Machine* untuk menentukan nama pengenalan, lokasi penyimpanan dan jenis serta versi dari sistem operasi yang ingin dibuat pada *virtual machine*, seperti terlihat pada gambar berikut:

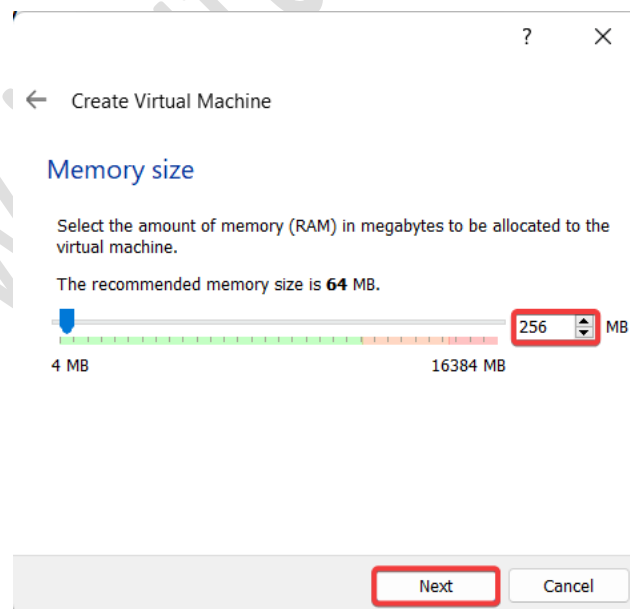


Lengkapi isian beberapa parameter berikut:

- a. **Name:** dengan nama pengenal dari *virtual machine*, sebagai contoh **Mikrotik-CHR-PVE**.
- b. **Machine Folder** digunakan untuk menentukan lokasi penyimpanan *file virtual machine* yang dibuat yaitu secara *default* disimpan di **C:\Users\NamaLogin\VirtualBox VMs**. **NamaLogin** merupakan nama login pengguna yang digunakan untuk akses ke sistem *Windows*, sebagai contoh **PUTU** sehingga nilai pada *dropdown Machine Folder* adalah **C:\Users\PUTU\VirtualBox VMs**. Apabila ingin menyimpan di lokasi lain maka pilih **Other...** pada *dropdown Machine Folder* tersebut dan arahkan ke lokasi direktori penyimpanan baru yang diinginkan.
- c. **Type** digunakan untuk menentukan jenis sistem operasi yang akan diinstalasi pada *virtual machine* yaitu **Other**.
- d. **Version** digunakan untuk menentukan versi dari sistem operasi yang akan diinstalasi pada *virtual machine* yaitu **Other/Unknown (64 bit)**.


Klik tombol **Next** untuk melanjutkan.

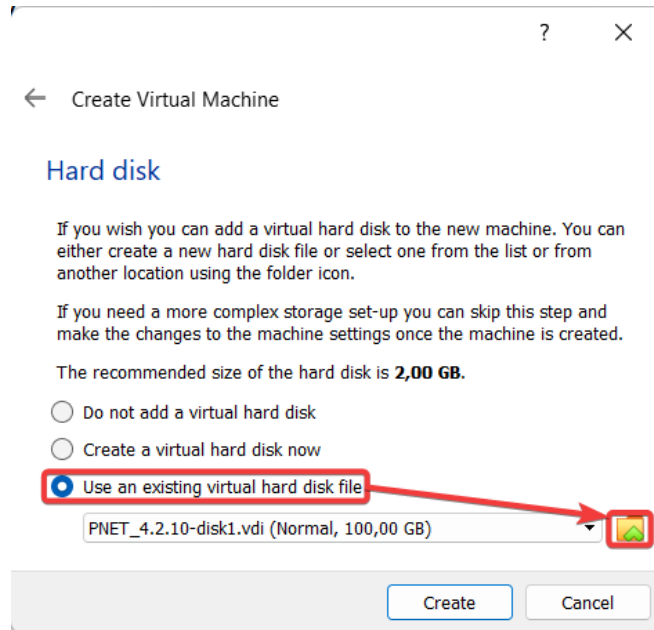
5. Tampil kotak dialog *Memory size* untuk menentukan ukuran memori yang dialokasikan bagi *virtual machine* yang dibuat. Sebagai contoh dialokasikan **256 MB**, seperti terlihat pada gambar berikut:



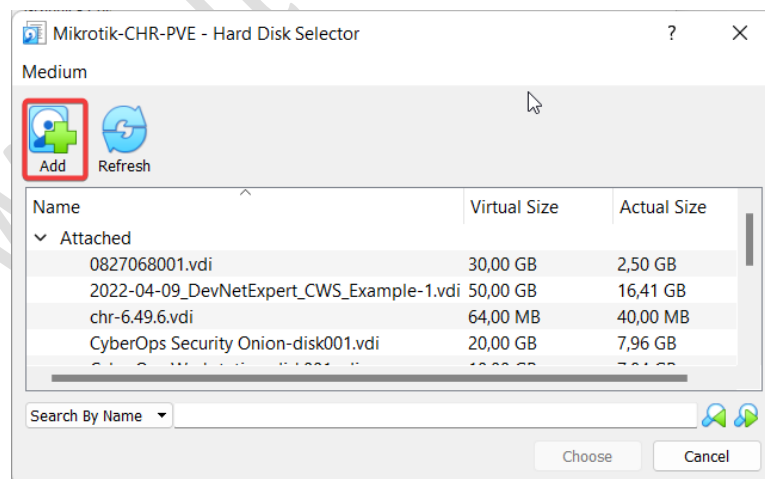
Klik tombol **Next** > untuk melanjutkan.

6. Tampil kotak dialog *Hard disk* untuk menentukan *virtual hardisk* yang digunakan oleh *virtual machine* yang dibuat. Secara default telah terpilih **Create a virtual hard disk**

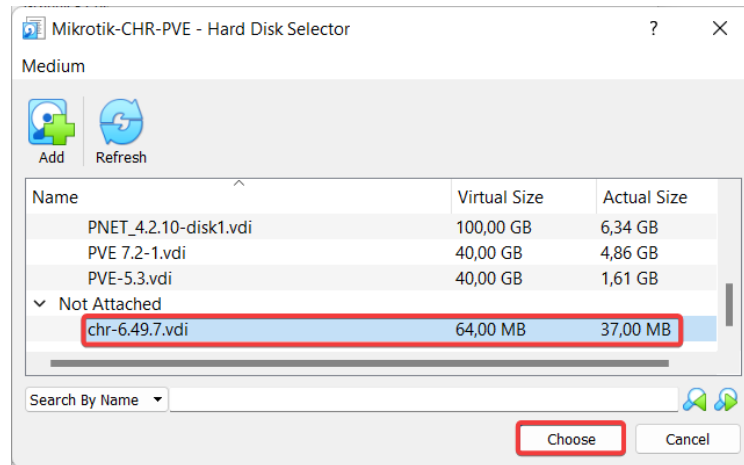
now untuk membuat *virtual hard disk* bagi *virtual machine* baru yang dibuat. Namun lakukan penyesuaian dengan memilih “Use an existing virtual hard disk now” untuk menggunakan *virtual hard disk* yang telah ada dan klik tombol  **Choose a virtual hard disk file** untuk memilih file *virtual hard disk* yang akan digunakan, seperti terlihat pada gambar berikut:



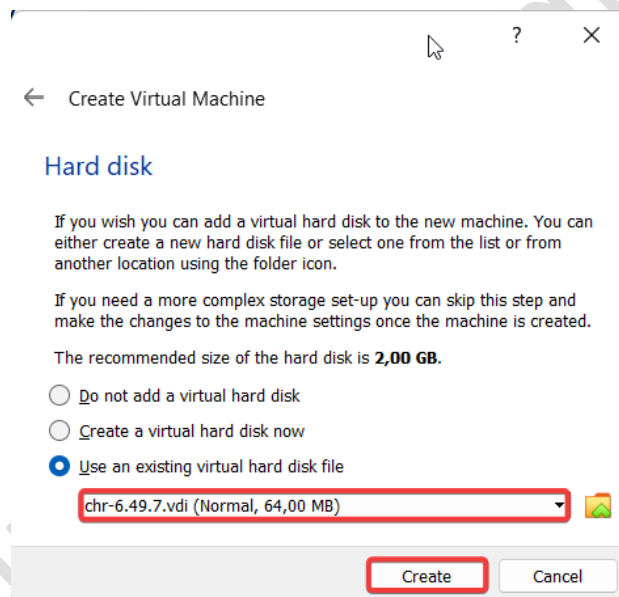
Tampil kotak dialog Mikrotik-CHR-PVE-Hard Disk Selector dan klik tombol Add untuk melakukan penambahan *virtual hard disk*, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Please choose a virtual hard disk file**. Arahkan ke lokasi direktori yang menyimpan file **chr-6.49.7.vdi**, sebagai contoh di **D:\Master\chr-6.49.7.vdi**. **Silakan menyesuaikan lokasi direktori yang memuat file tersebut di computer masing-masing**. Pilih file **chr-6.49.7.vdi** yang terdapat pada direktori tersebut dan klik tombol **Open** maka hasil penambahannya akan terlihat seperti pada gambar berikut:

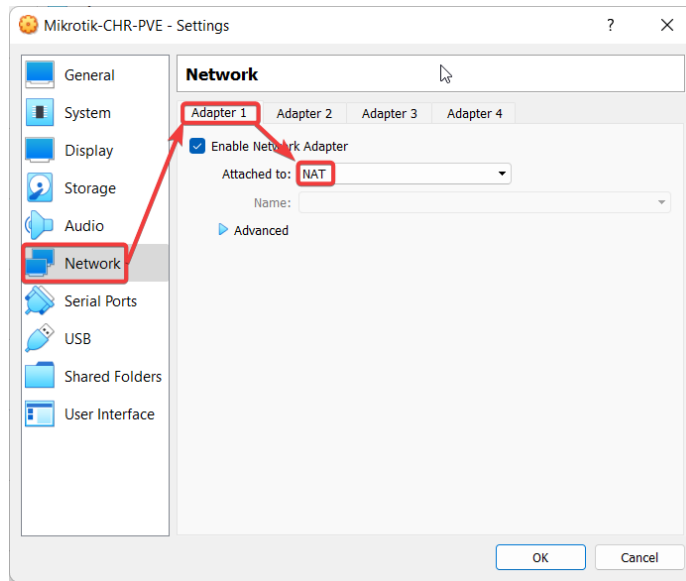


Klik tombol **Choose** untuk memilih file **chr-6.49-7.vdi** sehingga dapat digunakan oleh *virtual machine* maka hasilnya akan terlihat seperti pada gambar berikut:

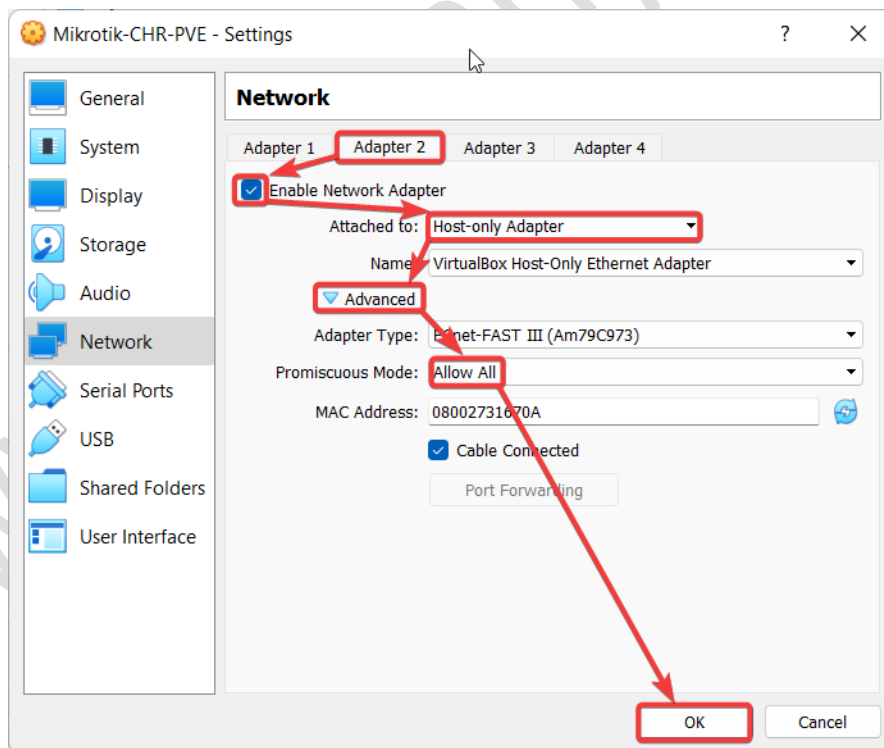


Klik tombol **Create** untuk melanjutkan. *Virtual machine* telah selesai dibuat.

- Menambah dan mengubah pengaturan **network adapter** terkait jenis dan **promiscuous mode**. Pilih VM **MIKROTIK-CHR-PVE** pada daftar dari *Oracle VirtualBox Manager* dan klik **Settings** pada *toolbar*. Pada panel sebelah kiri dari **MIKROTIK-CHR-PVE Settings** yang tampil, pilih **Network** dan pada panel detail sebelah kanan yaitu di tab **Adapter 1**, pastikan pilihan jenis koneksi jaringan pada *dropdown Attached to* adalah **NAT**, seperti terlihat pada gambar berikut:



Selanjutnya pindah ke tab **Adapter 2** dan centang (✓) pada **Enable Network Adapter** untuk mengaktifkan *network adapter* tersebut serta pilih **Host-only Adapter** sebagai jenis koneksi jaringan pada *dropdown Attached to*, seperti terlihat pada gambar berikut:

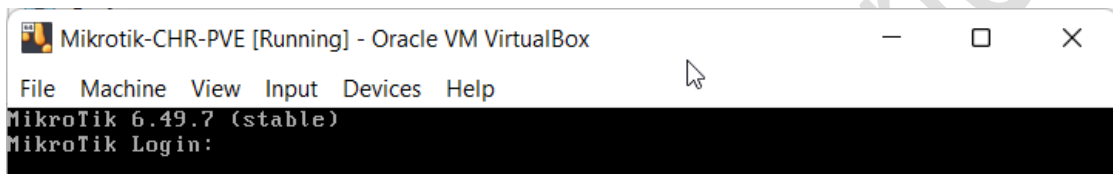


Selanjutnya klik bagian **Advanced** dan pada *dropdown Promiscuous Mode*, pilih **Allow All**. Klik tombol **OK** untuk menyimpan pengaturan.

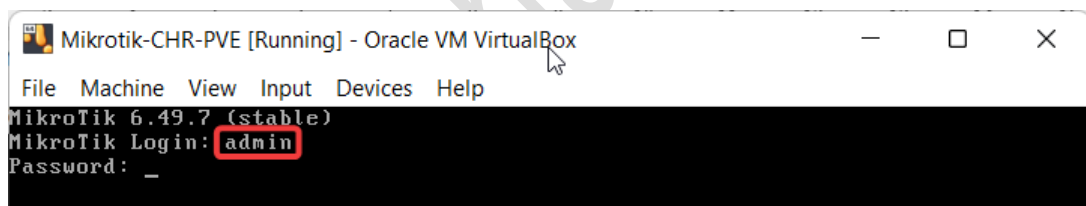
8. Menjalankan **VM** dengan memilih **Mikrotik-CHR-PVE** pada daftar dari *Oracle VM VirtualBox Manager* dan memilih **Start** pada *toolbar*, seperti yang ditunjukkan pada gambar berikut:



9. Tampil kotak dialog **Mikrotik-CHR-PVE [Running] – Oracle VM VirtualBox** dan tunggu hingga menampilkan *prompt MikroTik Login*.

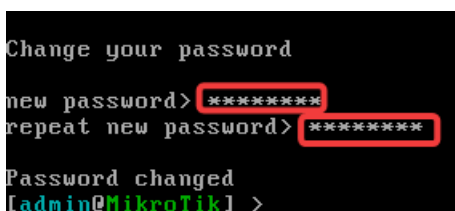


Secara *default* akun otentikasi *login* ke MikroTik menggunakan **username “admin”** dengan **password** kosong (**blank**). Pada *input MikroTik Login*, masukkan “**admin**” dan tekan tombol **Enter**. Sedangkan pada *input Password*, tekan tombol **Enter**, seperti terlihat pada gambar berikut:



Tampil pesan konfirmasi **Do you want to see the software license? [Y/n]**. Ketik **n** untuk tidak melihat lisensi perangkat lunak.

Selanjutnya tampil pesan **Change your password** untuk mengubah sandi dari *user* “**admin**”. Sebagai contoh *password* yang ingin digunakan adalah “**12345678**” sehingga pada *input new password>* yang tampil, masukkan “**12345678**” dan tekan tombol **Enter**. Tampil *input repeat new password>*, untuk memasukkan kembali sandi baru yaitu “**admin**” dan tekan tombol **Enter**, seperti terlihat pada gambar berikut:



Terlihat *prompt CLI* dari *Mikrotik*, seperti gambar berikut:

```
[admin@MikroTik] >
```

10. Menampilkan informasi *interface* yang dimiliki oleh *router* Mikrotik.

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#   NAME      TYPE      ACTUAL-MTU  L2MTU
0   R ether1    ether      1500
1   R ether2    ether      1500
```

Terlihat terdapat 2 (dua) *interface* yaitu **ether1** dan **ether2**.

11. Menampilkan informasi *interface* dengan pengaturan *DHCP Client*.

```
[admin@MikroTik] > ip dhcp-client print
Flags: X - disabled, I - invalid, D - dynamic
#   INTERFACE  USE ADD-DEFAULT-ROUTE  STATUS  ADDRESS
0   ether1      yes yes                 bound   10.0.2.15/24
```

Terlihat terdapat satu *interface* yaitu **ether1**.

12. Mengatur pengalamatan IP pada **interface ether2** secara static menggunakan **192.168.169.254/24**.

```
[admin@MikroTik] > ip address add address=192.168.169.254/24 interface=ether2
```

13. Memverifikasi pengalamatan IP yang telah diatur pada *interface*.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS      NETWORK      INTERFACE
0   D 10.0.2.15/24  10.0.2.0     ether1
1   192.168.169.254/24  192.168.169.0 ether2
```

14. Menampilkan informasi tabel *routing*.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS  PREF-SRC  GATEWAY      DISTANCE
0   ADS  0.0.0.0/0    10.0.2.2     1
1   ADC  10.0.2.0/24  10.0.2.15    0
2   ADC  192.168.169.0/24  192.168.169.254 ether2 0
```

15. Memverifikasi koneksi ke default *gateway* menggunakan perintah *ping*.

```
[admin@MikroTik] > ping 10.0.2.2
SEQ HOST      SIZE TTL TIME  STATUS
0 10.0.2.2    56 255 0ms
1 10.0.2.2    56 255 0ms
sent=2 received=2 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Tekan **CTRL+C** untuk menghentikan *ping*.

16. Mengatur agar Mikrotik bertindak sebagai *Server DNS*.

```
[admin@MikroTik] > ip dns set allow-remote-requests=yes
```

17. Memverifikasi pengaturan *Server DNS*.

```
[admin@MikroTik] > ip dns print
servers:
dynamic-servers: 192.168.184.215
use-doh-server:
verify-doh-cert: no
allow-remote-requests: yes
max-udp-packet-size: 4096
query-server-timeout: 2s
query-total-timeout: 10s
max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 24KiB
```

18. Mengatur *Internet Connection Sharing (ICS)* menggunakan *Network Address Translation (NAT)*.

```
[admin@MikroTik] > ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

19. Memverifikasi hasil pengaturan NAT.

```
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade out-interface=ether1
```

20. Memverifikasi koneksi **Internet** menggunakan perintah ping ke salah satu situs di *Internet*, sebagai contoh ke **detik.com**.

```
[admin@MikroTik] > ping detik.com
SEQ HOST                SIZE TTL TIME  STATUS
0 203.190.242.211      56 128 46ms
1 203.190.242.211      56 128 78ms
2 203.190.242.211      56 128 47ms
sent=3 received=3 packet-loss=0% min-rtt=46ms avg-rtt=57ms max-rtt=78ms
```

Tekan **CTRL+C** untuk menghentikan *ping*.

BAB V

INSTALASI DAN KONFIGURASI MIKROTIK

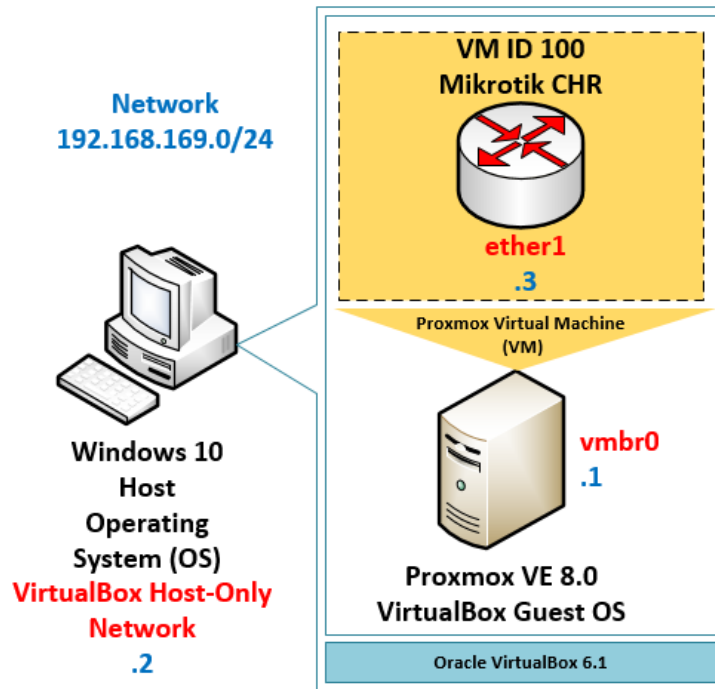
CLOUD HOSTED ROUTER (CHR) PADA PROXMOX VE 8.0

Menurut [wiki Mikrotik](#), *Cloud Hosted Router (CHR)* merupakan versi *RouterOS* yang ditujukan untuk dijalankan sebagai *virtual machine*. CHR mendukung arsitektur x86 64-bit dan dapat digunakan pada berbagai *hypervisor*, termasuk *Proxmox*. CHR memiliki fitur lengkap dari *RouterOS* yang telah diaktifkan secara *default* namun memiliki beberapa model lisensi berbeda dari versi *RouterOS* lainnya. Kebutuhan sistem minimum untuk menjalankan CHR adalah CPU 64 bit dengan dukungan virtualisasi, memori 128 MB atau lebih untuk instance CHR, hardisk 128 MB untuk *virtual drive CHR*, ukuran sistem *disk image* yang didukung adalah 16 GB.

Pembahasan pada bab ini ini terdiri dari 2 (dua) bagian yaitu (a) Instalasi *Mikrotik CHR* pada *Proxmox VE 8.0* dan (b) Verifikasi dan konfigurasi *Mikrotik CHR* pada *Web Interface Proxmox*. **Sebelum mengikuti tutorial ini, pastikan *Server Proxmox* telah dapat terkoneksi ke *Internet* karena proses instalasi membutuhkan paket *unzip* yang akan diunduh dari *Internet*. Selain itu *image* dari *Mikrotik CHR* yang diinstalasi akan diunduh pula secara langsung dari situs [Mikrotik](#).**

A. RANCANGAN JARINGAN UJICOBA

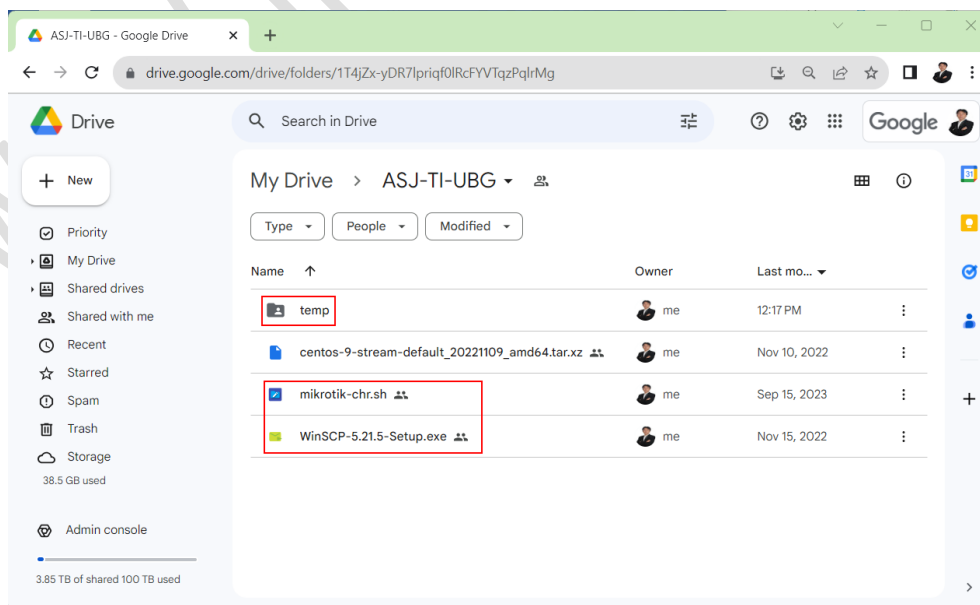
Rancangan jaringan ujicoba yang digunakan masih sama seperti pada materi sebelumnya. Namun pada *Server Proxmox VE 8.0* dilakukan pembuatan *Virtual Machine (VM)* dengan jenis *Kernel-based Virtual Machine (KVM)* menggunakan sistem operasi *Mikrotik CHR* versi **6.49.7**. *VM Mikrotik CHR* akan menggunakan ID **100** dengan alamat IP **192.168.169.3/24**, seperti terlihat pada gambar berikut:



B. INSTALASI MIKROTIK CHR PADA PROXMOX VE 8.0

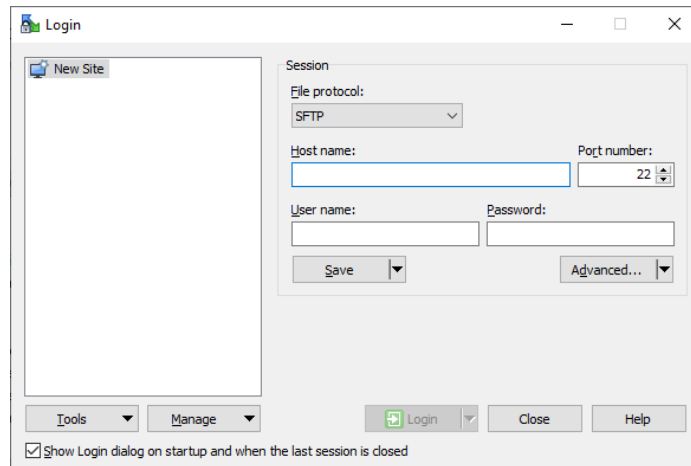
Adapun langkah-langkah instalasi dan konfigurasi *Mikrotik CHR* pada *Proxmox VE 8.0* adalah sebagai berikut:

1. Pastikan telah mengunduh folder “**temp**” yang didalamnya memuat *image MikroTik CHR* versi **6.49.7** dengan nama *file “chr-6.49.7.img”* dan *file “mikrotik-chr.sh”* serta program **WinSCP** dengan nama *file “WinSCP-5.21.5-Setup.exe”* untuk memfasilitasi *file transfer* dari **Windows** ke **Proxmox** melalui <http://bit.ly/asj-ti-ubg>, seperti terlihat pada gambar berikut:



Setelah proses unduh *file-file* tersebut selesai maka lakukan instalasi program **WinSCP** secara mandiri.

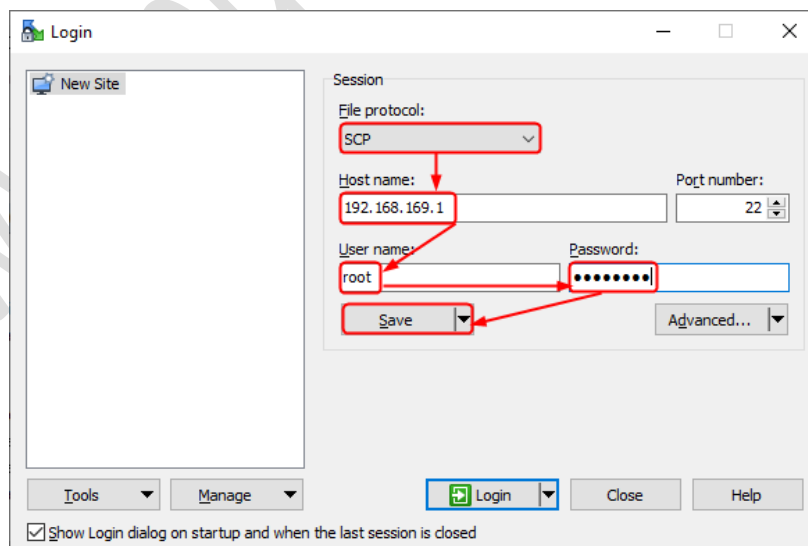
2. Jalankan aplikasi *WinSCP* untuk melakukan pengunggahan *folder* “**temp**” dan *file* “**mikrotik-chr.sh**” dari **Windows** ke **server Proxmox** maka akan tampil kotak dialog **Login**, seperti terlihat pada gambar berikut:



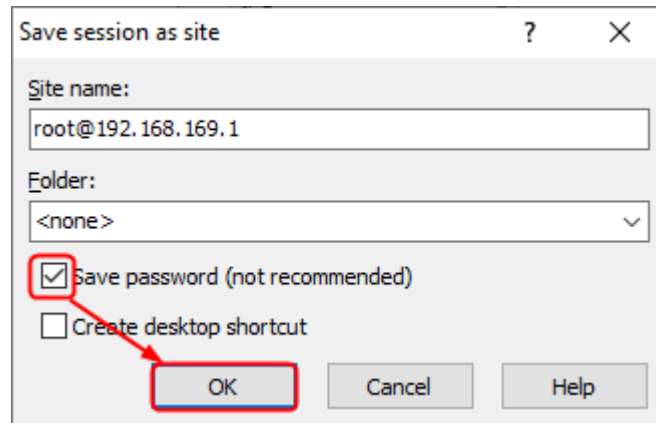
Lakukan pengaturan pada beberapa parameter berikut:

- a. **File protocol:**, menentukan jenis dari file protocol. Pilih **SCP**.
- b. **Hostname:**, masukkan alamat IP dari server Proxmox yaitu **192.168.169.1**.
- c. **User name:**, masukkan “**root**”.
- d. **Password:**, masukkan sandi dari *user* “**root**”, sebagai contoh “**12345678**”.

Sehingga hasil akhirnya akan terlihat seperti ditunjukkan pada gambar berikut:

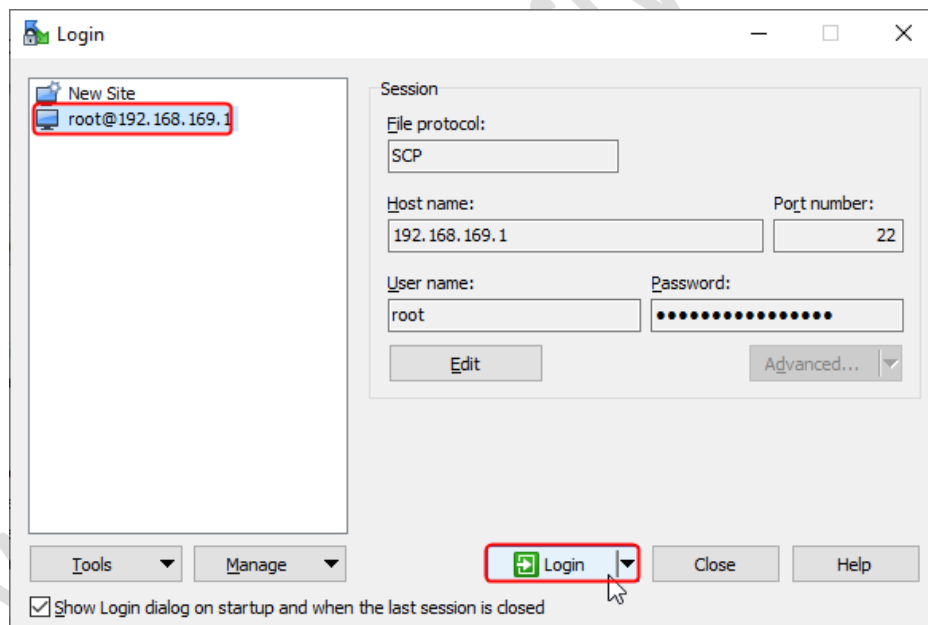


Klik tombol **Save** untuk menyimpan pengaturan maka akan tampil kotak **dialog Save session as site**, seperti terlihat pada gambar berikut:



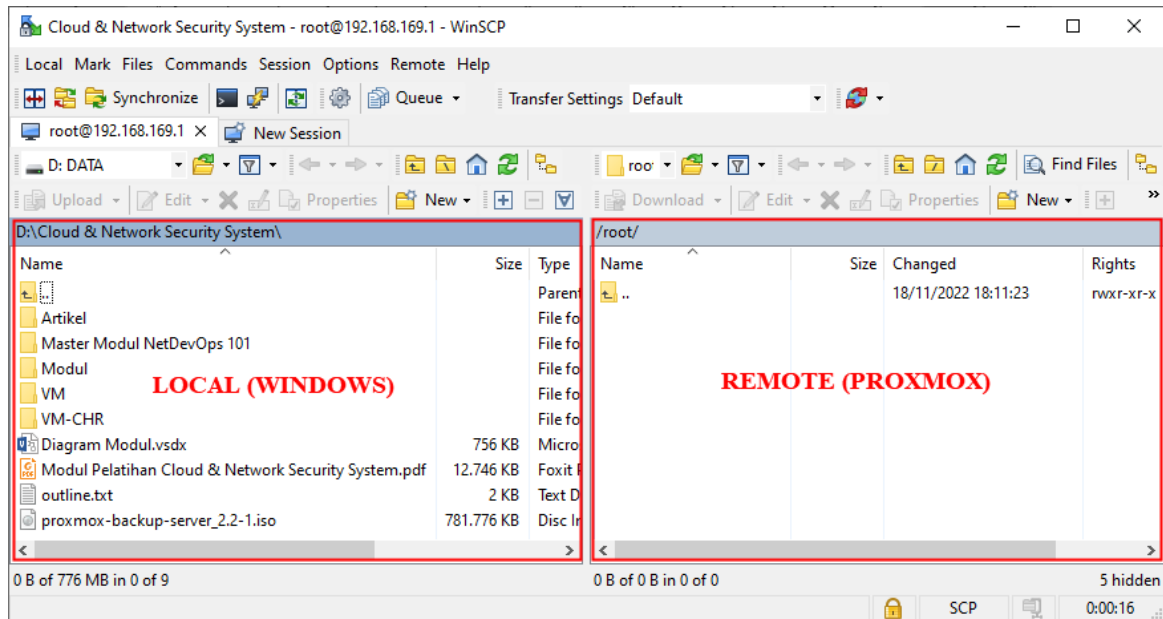
Centang (✓) pada parameter **Save password (not recommended)** untuk menyimpan sandi dari user “**root**”. Hal ini bertujuan agar pada penggunaan **WinSCP** untuk melakukan *file transfer* ke server **Proxmox** berikutnya, pengguna tidak akan diminta kembali memasukkan sandi dari user “**root**”.

Klik tombol **OK** untuk menyimpan perubahan maka hasilnya akan terlihat seperti pada gambar berikut:

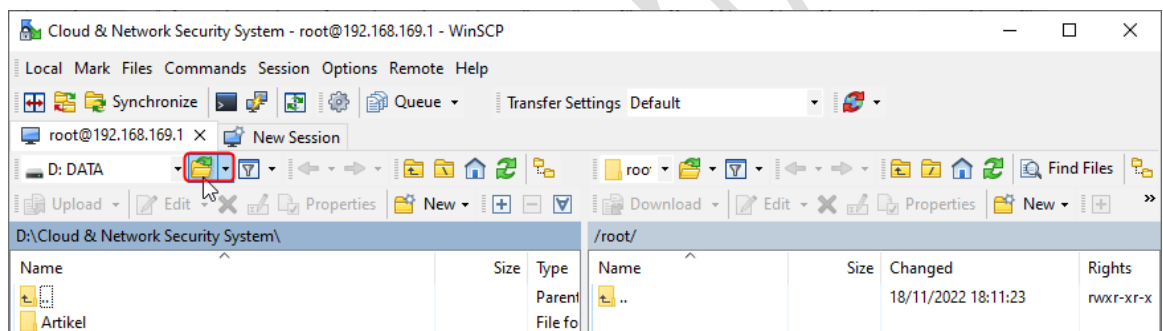


Klik tombol **Login** untuk melakukan koneksi ke server **Proxmox**.

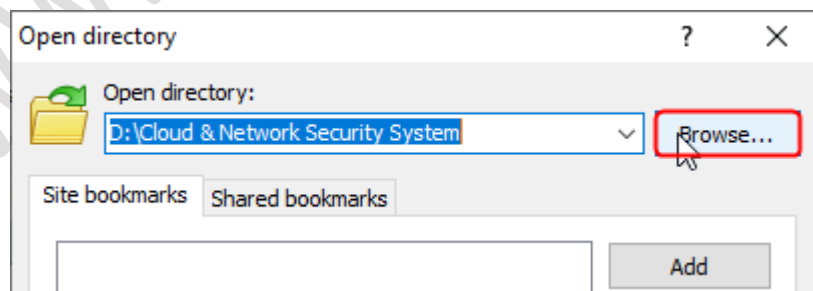
Apabila proses otentikasi *login* berhasil dilakukan maka akan tampil kotak dialog WinSCP dengan antarmuka menyerupai **file manager**. *File manager* tersebut terbagi menjadi dua bagian yaitu panel sebelah kiri **Local (Windows)** yang memperlihatkan *file-file* di komputer lokal *Windows* dan panel sebelah kanan **Remote (Proxmox)** yang memperlihatkan *file-file* di komputer server **Proxmox** dimana secara *default* mengarah ke *home directory* dari user “**root**” yaitu di **/root**, seperti terlihat pada gambar berikut:



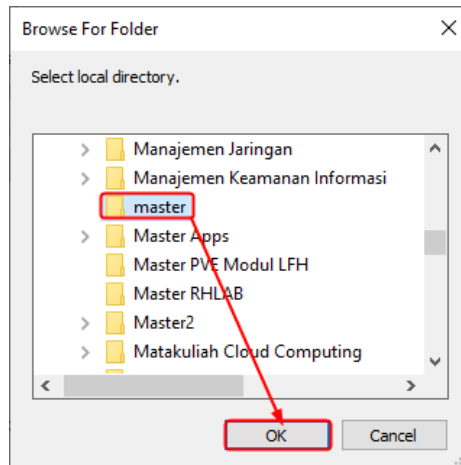
Klik icon **Open Directory** di bagian *toolbar* dari **Local (Windows)**, seperti terlihat pada gambar berikut untuk mengarahkan ke lokasi penyimpanan folder “**temp**” dan *file* “**mikrotik-chr.sh**” yang akan diunggah.



Tampil kotak dialog **Open directory** dan klik tombol **Browse...**, seperti terlihat pada gambar berikut:

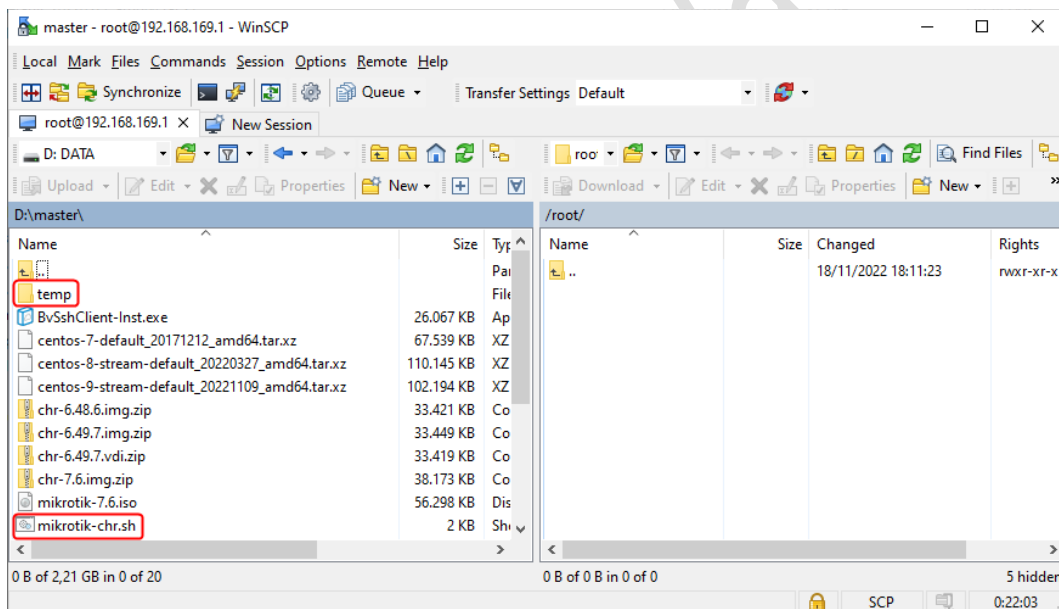


Selanjutnya akan tampil kotak dialog **Browse For Folder** dan arahkan ke lokasi penyimpanan dari folder “**temp**” dan *file* “**mikrotik-chr.sh**”, sebagai contoh di **D:\Master**, seperti terlihat pada gambar berikut:

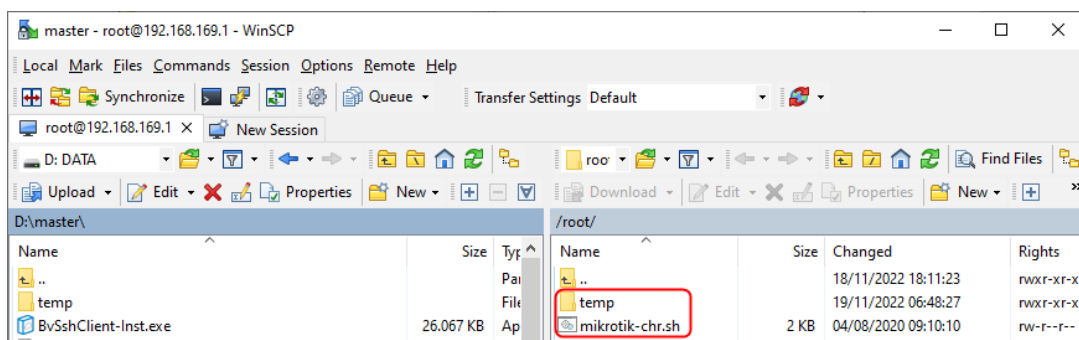


Silakan menyesuaikan dengan lokasi penyimpanan di komputer masing-masing.

Klik tombol **OK > OK** untuk menyimpan perubahan maka hasilnya pada panel sebelah kiri **Local (Windows)** akan menampilkan isi dari direktori **D:\Master**, seperti terlihat pada gambar berikut:

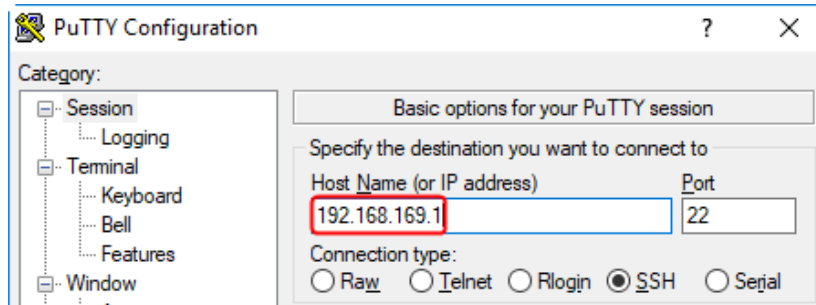


Lakukan **drag and drop** folder “temp” dan file “mikrotik-chr.sh” dari panel sebelah kiri **Local (Windows)** ke **Remote (Proxmox)** sehingga terunggah ke server Proxmox maka hasilnya akan terlihat seperti pada gambar berikut:



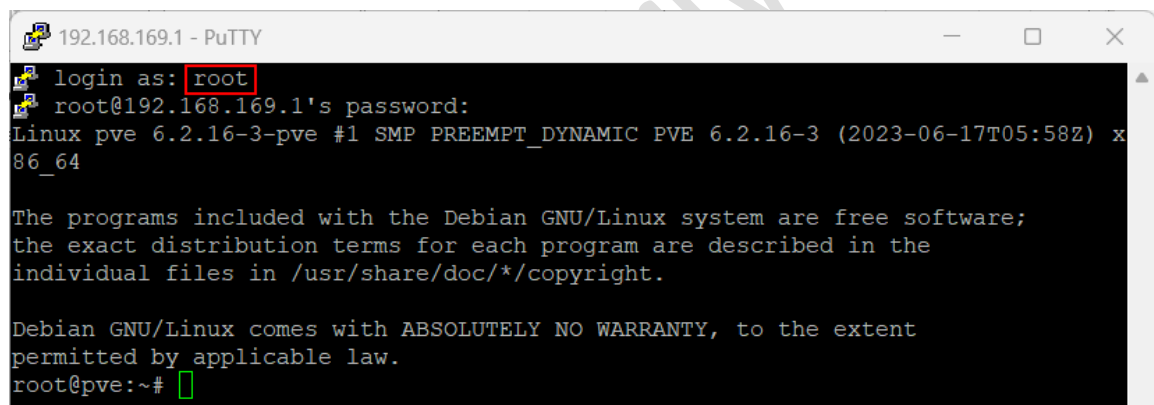
Tutup kotak dialog aplikasi *WinSCP*. Klik tombol **Yes** pada kotak dialog **Terminate session** yang tampil.

3. Jalankan aplikasi *SSH Client*, sebagai contoh menggunakan *Putty*. Tampil kotak dialog *Putty Configuration*. Pada isian **Host Name (or IP Address)**, masukkan alamat IP dari *Server Proxmox* yaitu **192.168.169.1**, seperti terlihat pada gambar berikut:



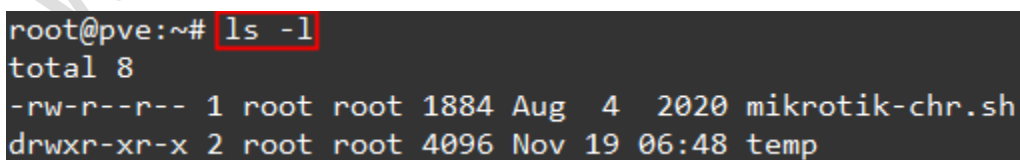
Klik tombol **Open**.

4. Tampil kotak dialog *Putty* yang meminta pengguna untuk melakukan proses otentikasi login ke *Server Proxmox*, seperti terlihat pada gambar berikut:



Pada inputan **login as:**, masukkan “**root**” dan tekan tombol **Enter**. Selanjutnya tampil inputan **password:**, masukkan “**12345678**” dan tekan tombol **Enter**. Apabila proses otentikasi berhasil dilakukan maka akan tampil *shell prompt #*.

5. Menampilkan informasi isi dari direktori saat ini berada dengan mengeksekusi perintah “**ls -l**”.



6. Memperbaharui informasi terkait daftar paket dari *repository* perangkat lunak sistem *Proxmox* dengan mengeksekusi perintah:

```
# apt update
```

7. Menginstalasi paket aplikasi **unzip** dan **jq** yang diperlukan ketika mengeksekusi *shell script mikrotik-chr.sh* dengan mengeksekusi perintah berikut:

```
# apt -y install unzip jq
```

8. Mengubah ijin akses file “**mikrotik-chr.sh**” agar memiliki hak *executable*.

```
root@pve:~# chmod +x mikrotik-chr.sh
```

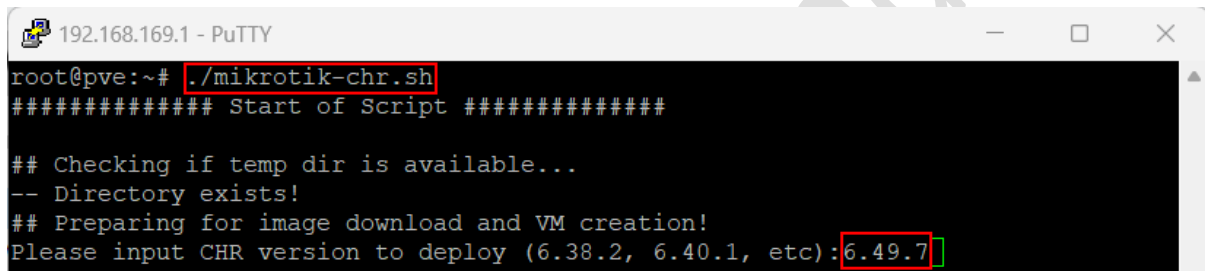
9. Memverifikasi hasil perubahan ijin akses pada file “**mikrotik-chr.sh**”.

```
root@pve:~# ls -l mikrotik-chr.sh
-rwxr-xr-x 1 root root 1884 Aug 4 2020 mikrotik-chr.sh
```

10. Mengeksekusi *file bash script* “**mikrotik-chr.sh**”.

```
root@pve:~# ./mikrotik-chr.sh
```

Tampil inputan untuk memasukkan versi CHR yang akan diunduh, seperti terlihat pada gambar berikut:



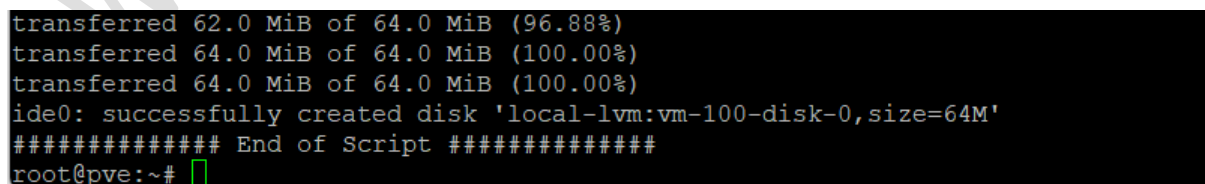
```
192.168.169.1 - PuTTY
root@pve:~# ./mikrotik-chr.sh
##### Start of Script #####
## Checking if temp dir is available...
-- Directory exists!
## Preparing for image download and VM creation!
Please input CHR version to deploy (6.38.2, 6.40.1, etc): 6.49.7
```

Masukkan “**6.49.7**” dan tekan **Enter**.

Tampil inputan untuk memasukkan **VM ID** yang akan digunakan oleh *Mikrotik CHR*. *Output* dari “**Printing list of VM’s and CT’s on this hypervisor!**” sebelum inputan ini kosong sehingga belum terdapat VM pada *Server Proxmox*. Sebaliknya pastikan **VM ID** yang dimasukkan belum digunakan oleh VM lainnya, sebagai contoh masukkan “**100**” dan tekan **Enter**, seperti terlihat pada gambar berikut:

```
Please Enter free vm ID to use: 100
```

Selanjutnya akan tampil pesan proses pembuatan *CHR VM* baru yaitu proses *import volume*, seperti terlihat pada cuplikan gambar berikut:



```
transferred 62.0 MiB of 64.0 MiB (96.88%)
transferred 64.0 MiB of 64.0 MiB (100.00%)
transferred 64.0 MiB of 64.0 MiB (100.00%)
ide0: successfully created disk 'local-lvm:vm-100-disk-0,size=64M'
##### End of Script #####
root@pve:~#
```

Instalasi *Mikrotik CHR* pada *Proxmox VE 8.0* telah selesai dilakukan.

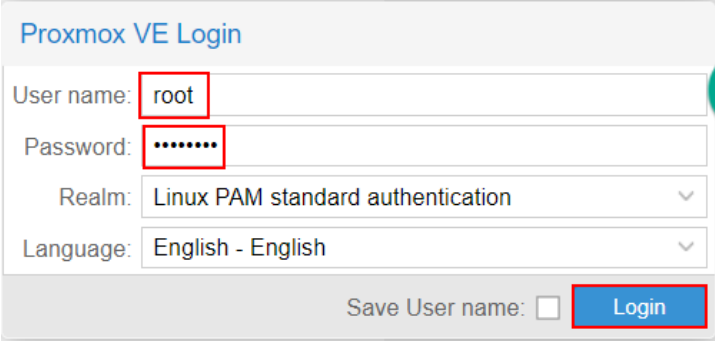
11. Keluar dari *SSH* dengan mengeksekusi perintah “**exit**”.

```
root@pve:~# exit
```

C. VERIFIKASI DAN KONFIGURASI MIKROTIK CHR PADA WEB INTERFACE PROXMOX

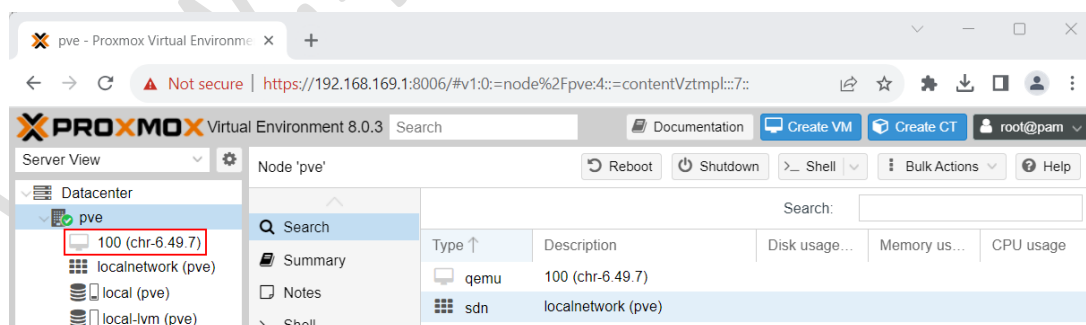
Adapun langkah-langkah verifikasi dan konfigurasi *Mikrotik CHR* pada *web interface Proxmox* adalah sebagai berikut:

1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**, seperti terlihat pada gambar berikut:



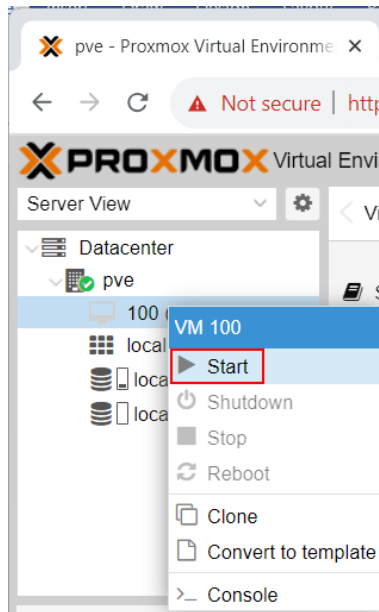
Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

3. Hasil dari instalasi *VM Mikrotik CHR* dapat diverifikasi dengan cara klik dua kali pada nama *node* yaitu “**pve**” di bawah menu **Datacenter** yang terdapat di panel sebelah kiri, seperti terlihat pada gambar berikut:



Terlihat telah terdapat VM dengan **ID 100** yaitu **chr-6.49.7**.

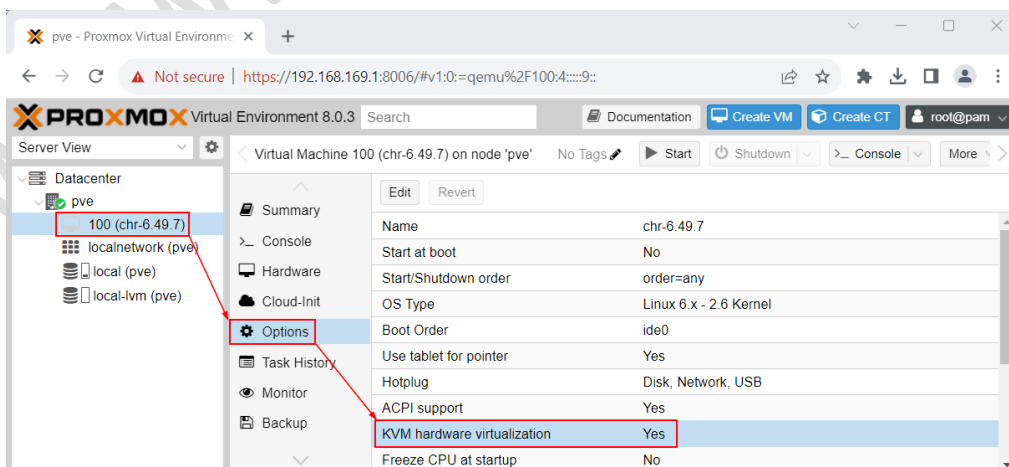
4. Untuk menjalankan *VM Mikrotik CHR*, klik kanan pada “**100 (chr-6.49.7)**” di bawah *node* “**pve**” dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:



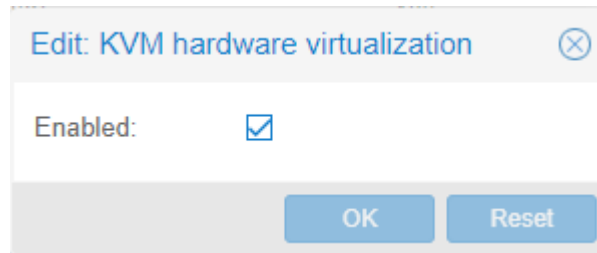
Apabila tampil pesan kesalahan berupa status “**Error: KVM virtualization configured, but not available. Either disable in VM configuration or enable in BIOS.**” terkait Tasks menjalankan VM 100 di bagian Log Panel maka fitur **KVM hardware virtualization** harus dinonaktifkan agar VM Mikrotik CHR dapat dijalankan, seperti terlihat pada gambar berikut:

Start Time ↓	End Time	Node	User name	Description	Status
Sep 15 00:00:58	Sep 15 00:00:58	pve	root@pam	VM 100 - Start	Error: KVM virtualisation con...
Sep 15 00:00:15	Sep 15 00:00:16	pve	root@pam	Start all VMs and Containers	OK

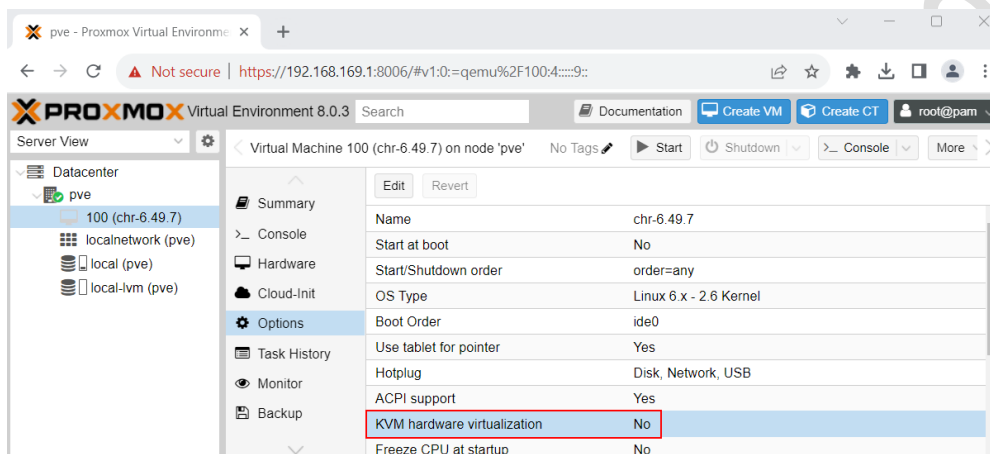
- Untuk menonaktifkan fitur **KVM hardware virtualization**, pilih menu **Options** pada panel sebelah kanan dari VM 100 (chr-6.49.7) maka akan terlihat pengaturan **KVM hardware virtualization** dengan nilai *default* Yes, seperti terlihat pada gambar berikut:



Klik dua kali pada **KVM hardware virtualization** maka akan tampil kotak dialog **Edit: KVM hardware virtualization**, seperti terlihat pada gambar berikut:

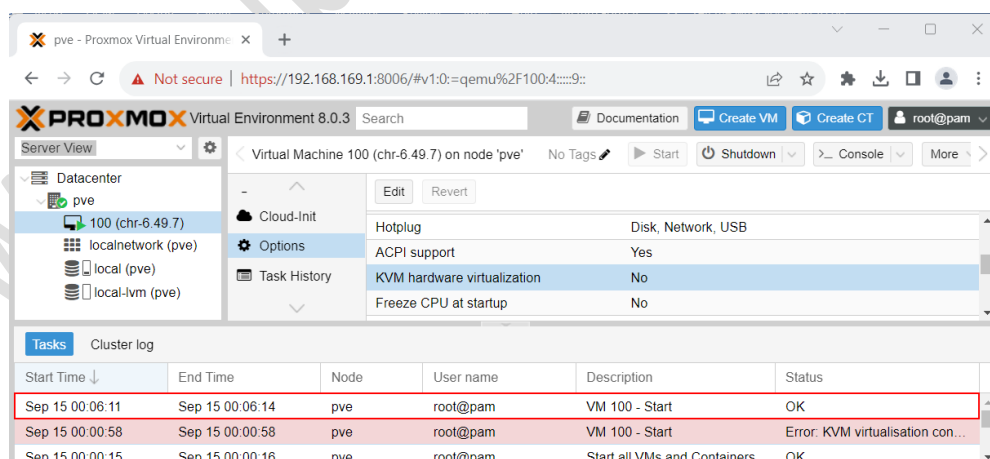


Hilangkan tanda pada cek (✓) pada parameter **Enabled** untuk menonaktifkan fitur **KVM hardware virtualization** dan tekan tombol **OK**. Hasil pengaturan akan terlihat seperti pada gambar berikut:

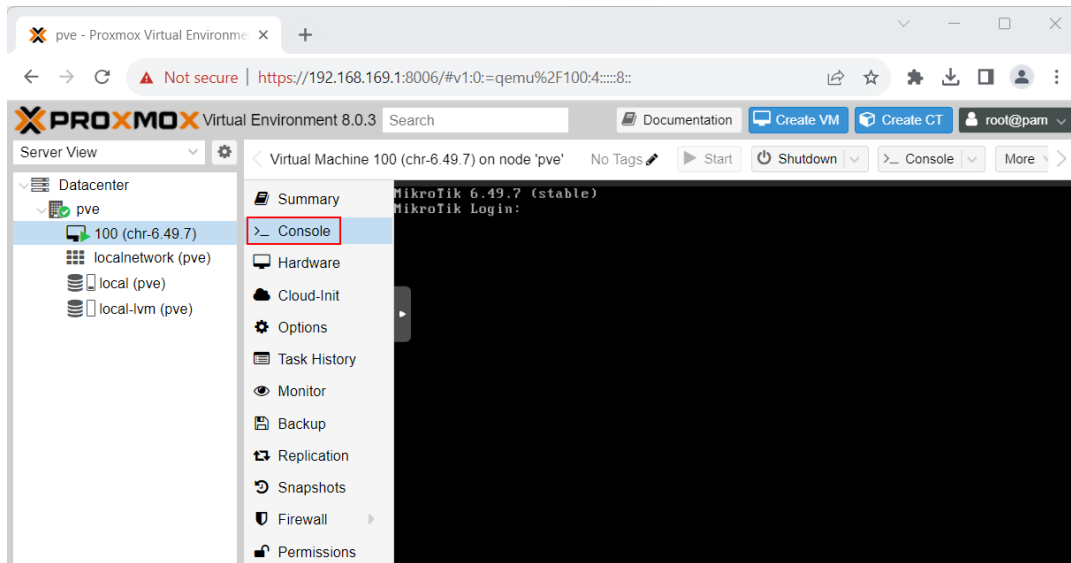


Nilai dari parameter **KVM hardware virtualization** telah diatur menjadi **No**.

6. Jalankan kembali *VM Mikrotik CHR*, seperti langkah 4 yaitu dengan cara klik kanan pada “**100 (chr-6.49.7)**” di bawah *node “pve”* dari menu **Datacenter** dan pilih **Start**. Kali ini *VM* telah berhasil dijalankan dimana ditandai dengan pesan status **OK** untuk **VM 100 - Start** pada bagian **Tasks** dari **Log Panel**, seperti terlihat pada gambar berikut:



7. Untuk mengakses tampilan dari **VM 100**, pilih **Console** pada panel sebelah kanan dari **VM 100 (chr-6.49.7)**, seperti terlihat pada gambar berikut:



Tampil inputan **Mikrotik Login** untuk proses otentikasi sebelum pengguna dapat mengakses **Command Line Interface (CLI)** dari *Mikrotik*. Masukkan nama login **“admin”** pada inputan **MikroTik Login** dan tekan tombol **Enter**.

Tampil inputan **Password:**, seperti terlihat pada gambar berikut:

```
MikroTik 6.49.7 (stable)
MikroTik Login: admin
Password: _
```

Tekan tombol **Enter** untuk melanjutkan karena *password* untuk user **“admin”** adalah **kosong (blank)**. Selanjutnya tampil pesan **“Do you want to see the software license? [Y/n]”**, tekan **“n”** untuk tidak menampilkan lisensi perangkat lunak.

Selanjutnya tampil pesan **Change your password** untuk mengubah sandi dari *user* **“admin”**. Sebagai contoh *password* yang ingin digunakan adalah **“12345678”** sehingga pada **input new password>** yang tampil, masukkan **“12345678”** dan tekan tombol **Enter**.

Tampil **input repeat new password>**, untuk memasukkan kembali sandi baru yaitu **“admin”** dan tekan tombol **Enter**, seperti terlihat pada gambar berikut:

```
Change your password
new password> *****
repeat new password> *****

Password changed
[admin@MikroTik] > _
```

Terlihat *prompt CLI* dari *Mikrotik*, seperti gambar berikut:

```
[admin@MikroTik] > _
```

Selanjutnya Anda dapat melakukan konfigurasi *Mikrotik* seperti mengatur identitas (*hostname*) dari *router*, pengalamatan IP dan lain sebagainya sesuai dengan kebutuhan.

8. Menampilkan informasi *interface* dengan pengaturan *DHCP Client*.

```
[admin@MikroTik] > ip dhcp-client print
Flags: X - disabled, I - invalid, D - dynamic
#  INTERFACE      USE ADD-DEFAULT-ROUTE  STATUS      ADDRESS
0  ether1          yes yes                 bound       192.168.56.22/24
```

Terlihat terdapat satu *interface* yaitu **ether1**.

9. Menghapus pengaturan *DHCP Client* pada *interface ether1*.

```
[admin@MikroTik] > ip dhcp-client remove 0
```

10. Mengatur pengalamatan IP pada **interface ether1** dari *Mikrotik* menggunakan alamat **192.168.169.3/24**.

```
[admin@MikroTik] > ip address add address=192.168.169.3/24 interface=ether1
```

11. Memverifikasi pengalamatan IP yang telah diatur pada *interface ether1*.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK          INTERFACE
0  192.168.169.3/24  192.168.169.0   ether1
```

12. Memverifikasi koneksi dari *Mikrotik CHR* ke *Server Proxmox* menggunakan utilitas **ping**.

```
[admin@MikroTik] > ping 192.168.169.1
SEQ HOST          SIZE TTL TIME  STATUS
0  192.168.169.1   56  64 31ms
1  192.168.169.1   56  64 7ms
sent=2 received=2 packet-loss=0% min-rtt=7ms avg-rtt=19ms max-rtt=31ms
```

Terlihat koneksi berhasil dilakukan.

13. Memverifikasi koneksi dari *Mikrotik CHR* ke *Client Windows 10* menggunakan utilitas **ping**.

```
[admin@MikroTik] > ping 192.168.169.2
SEQ HOST          SIZE TTL TIME  STATUS
0  192.168.169.2   56 128 8ms
1  192.168.169.2   56 128 7ms
sent=2 received=2 packet-loss=0% min-rtt=7ms avg-rtt=7ms max-rtt=8ms
```

Terlihat koneksi berhasil dilakukan.

14. Lakukan percobaan mengakses *Mikrotik CHR* melalui aplikasi **Winbox** yang terdapat pada **Client Windows 10**. *Winbox* merupakan aplikasi manajemen Mikrotik berbasis Graphical User Interface (GUI). Apabila Anda belum memiliki aplikasi tersebut maka dapat mengunduhnya pada alamat <https://mt.lv/winbox64>.

Klik dua kali pada *Winbox.exe*. Pada bagian tab **Neighbor** dari kotak dialog aplikasi *Winbox* yang tampil memperlihatkan *Mikrotik CHR* pada Proxmox telah terdeteksi secara otomatis, seperti ditunjukkan pada gambar berikut:

Managed Neighbors					
MAC Address	IP Address	Identity	Version	Board	
62:F6:95:98:48:E3	192.168.169.3	MikroTik	6.49.7 (stable)	CHR	

1 item (1 selected)

Untuk mengakses *Mikrotik CHR* melalui *Winbox*, terdapat beberapa parameter yang harus diatur pada *Winbox* antara lain:

- Connect to**, masukkan alamat *Media Access Control (MAC)* atau *IP* dari *Mikrotik CHR*. Isian parameter ini dapat diinputkan secara otomatis dengan cara memilih dari output Klik atau pilih pada alamat IP **192.168.169.3** yang muncul di kolom **IP Address** dari *output* tab **Neighbors** sehingga Anda tidak perlu memasukkan secara manual.
- Login**, masukkan nama user “**admin**”.
- Password**, masukkan sandi user “**12345678**”.

Hasilnya terlihat, seperti pada gambar berikut:

WinBox (64bit) v3.37 (Addresses)

File Tools

Connect To: **192.168.169.3** Keep Password

Login: **admin** Autosave Session

Password: ********* Open In New Window

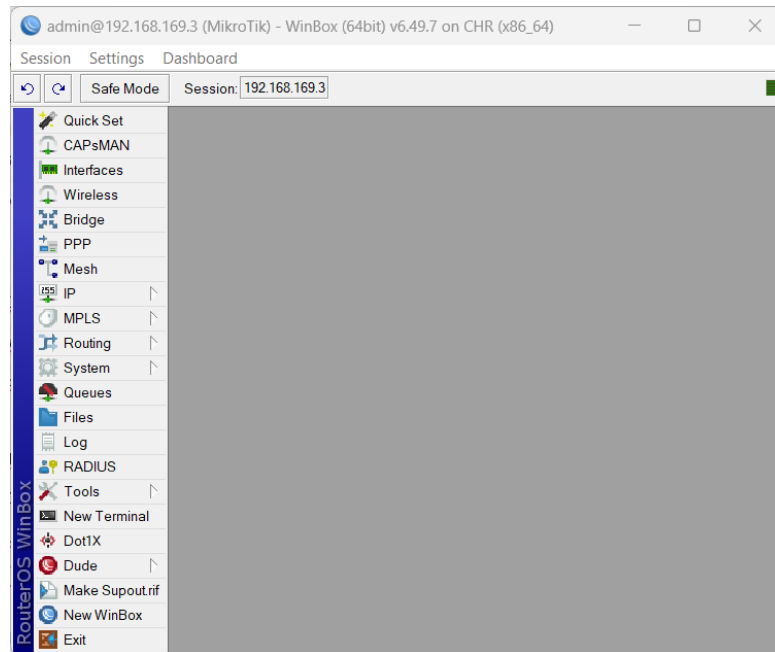
Session: <own> Auto Reconnect

Note: MikroTik

Group:

RoMON Agent:

Klik tombol **Connect** untuk menghubungkan ke *Mikrotik CHR* yang terdapat pada *Server Proxmox*. Apabila koneksi berhasil dilakukan maka akan terlihat seperti pada gambar berikut:



Tutup aplikasi *Winbox*.

15. Kembali ke **Console** dari *VM Mikrotik CHR* pada *web interface* administrasi *Proxmox*. Untuk mematikan *Mikrotik*, eksekusi perintah “**system shutdown**”, seperti terlihat pada gambar berikut:

```
[admin@MikroTik] > system shutdown
Shutdown, yes? [y/N]:
```

Pada pesan konfirmasi “**Shutdown, yes? [y/N]:**” yang tampil, tekan tombol “**y**” untuk melanjutkan proses *shutdown*. Tunggu hingga proses *shutdown* selesai dilakukan.

16. Untuk keluar dari *web interface* administrasi *Proxmox*, klik tombol **Logout** pada bagian *header* paling kanan.

D. INSTALASI DAN KONFIGURASI MIKROTIK CHR MENGGUNAKAN WIZARD MELALUI WEB GUI PROXMOX VE 8.0

Adapun langkah-langkah instalasi dan konfigurasi *MikroTik CHR* sebagai VM pada *Proxmox VE 8.0* melalui *wizard* di Web GUI adalah sebagai berikut:

1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian

“*Password*”, masukkan sandi login dari user “*root*”, seperti terlihat pada gambar berikut:

Proxmox VE Login

User name:

Password:

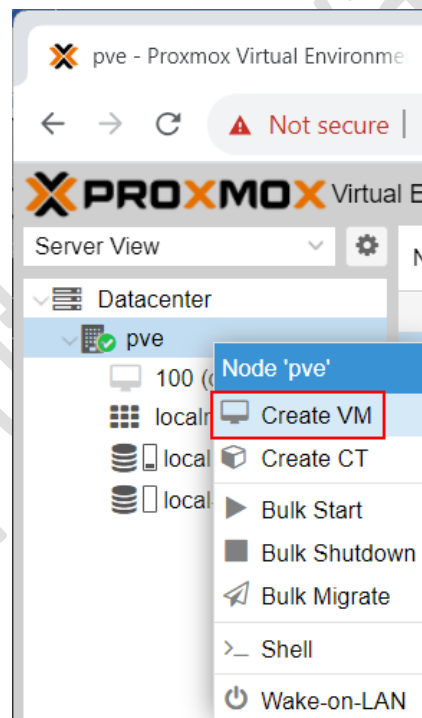
Realm: Linux PAM standard authentication

Language: English - English

Save User name:

Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

3. Membuat **VM** dengan cara klik kanan pada *node* “**pve**” dibawah menu **Datacenter** di panel sebelah kiri dan memilih **Create VM**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Create: Virtual Machine**. Terdapat beberapa parameter yang diatur di bagian **General** dari **Virtual Machine**, seperti terlihat pada gambar berikut:

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

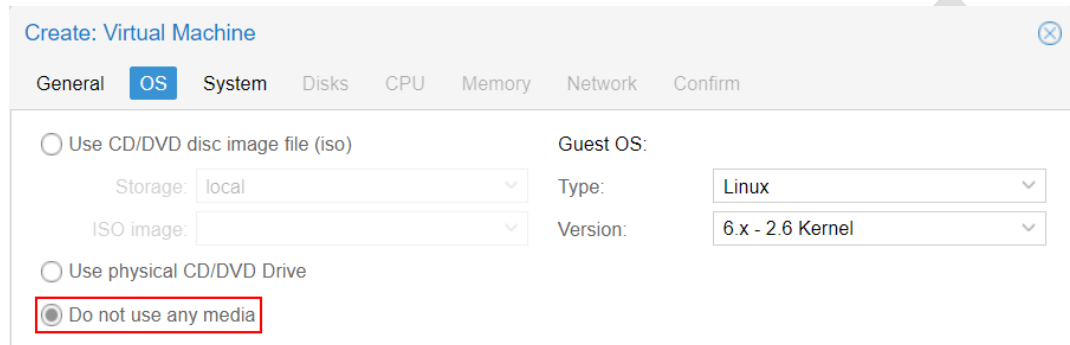
Node: Resource Pool:

VM ID:

Name:

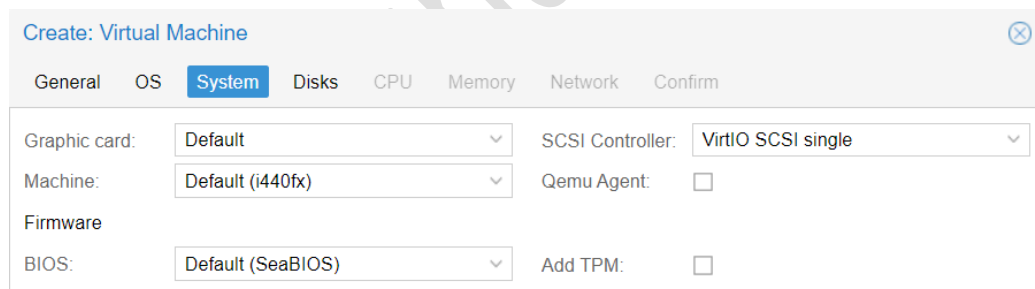
Terlihat **VM ID** telah terisi dengan nilai **200**. **Mohon untuk mengingat nilai VM ID tersebut karena akan diperlukan ketika proses *import disk images MikroTik CHR* pada tahap selanjutnya.** Pada parameter **Hostname:**, masukkan nama pengenalan dan nama domain bagi *host*, sebagai contoh “**chr200.belajar.local**”. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan bagian **OS** dari **Virtual Machine**. Pilih pada parameter **Do not use any media**, seperti terlihat pada gambar berikut:



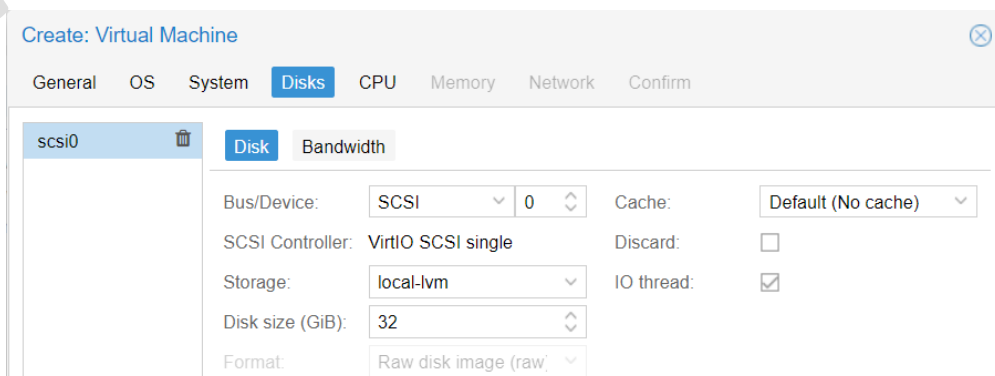
Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan bagian **System** dari **Virtual Machine**, seperti terlihat pada gambar berikut:



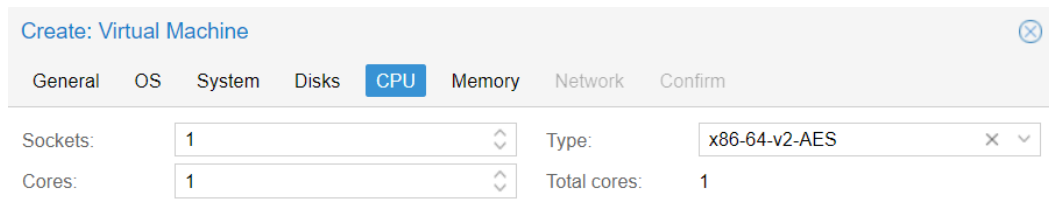
Tidak dilakukan pengaturan parameter apapun pada kotak dialog ini. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan bagian **Hard Disk** dari **Virtual Machine**, seperti terlihat pada gambar berikut:



Tidak dilakukan pengaturan parameter apapun pada kotak dialog ini karena hardisk yang terbuat pada VM tersebut nantinya akan dihapus. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan **CPU** dari **Virtual Machine**. Pada parameter **Cores**, lakukan penyesuaian jumlah *Core CPU* yang digunakan apabila diperlukan. Secara *default* bernilai 1 (satu), seperti terlihat pada gambar berikut:



Create: Virtual Machine

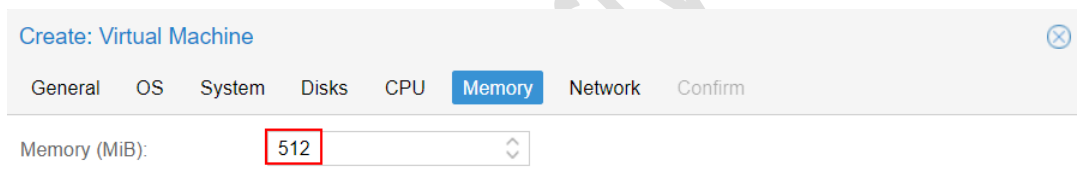
General OS System Disks **CPU** Memory Network Confirm

Sockets: 1 Type: x86-64-v2-AES

Cores: 1 Total cores: 1

Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan **Memory** dari **Virtual Machine**. Pada parameter **Memory (MiB)** lakukan penyesuaian agar kapasitas memori yang digunakan oleh VM adalah **512 MB**, seperti terlihat pada gambar berikut:



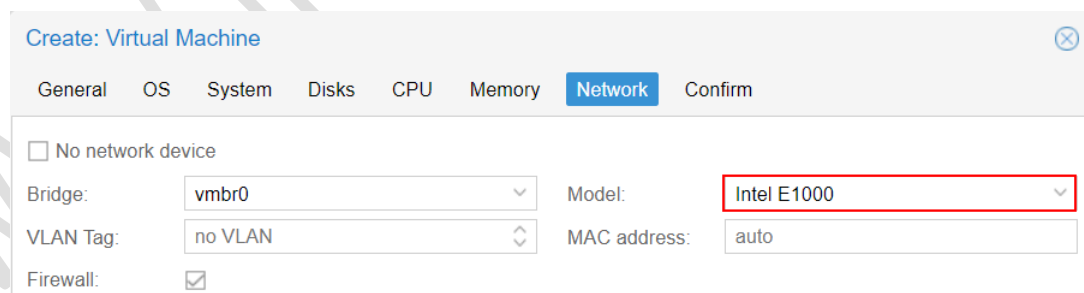
Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 512

Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan **Network** dari **Virtual Machine**. Pada parameter **Model**: lakukan penyesuaian agar model yang digunakan adalah **Intel E1000**, seperti terlihat pada gambar berikut:



Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

No network device

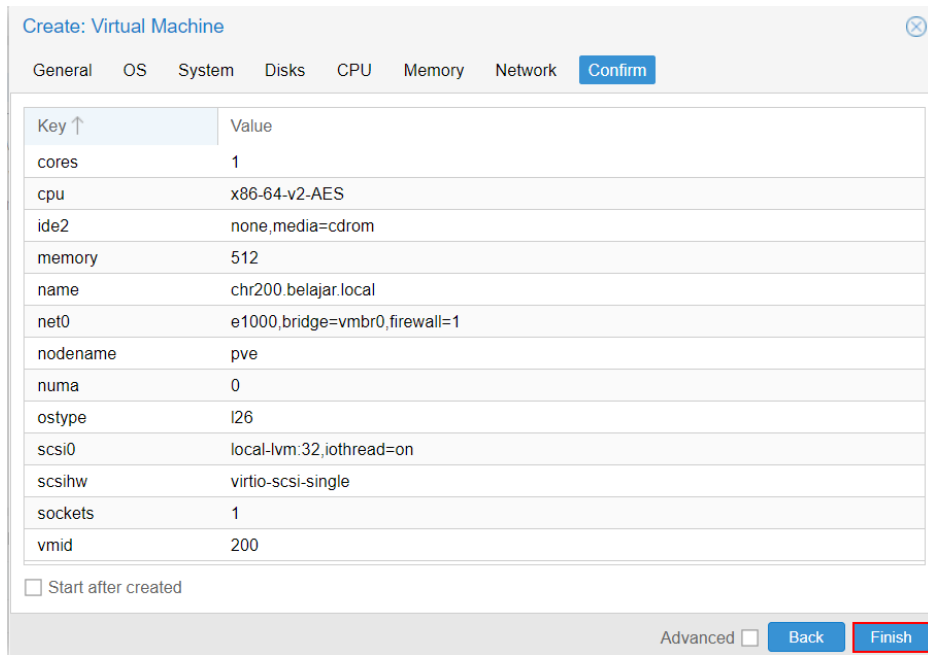
Bridge: vmbr0 Model: Intel E1000

VLAN Tag: no VLAN MAC address: auto

Firewall:

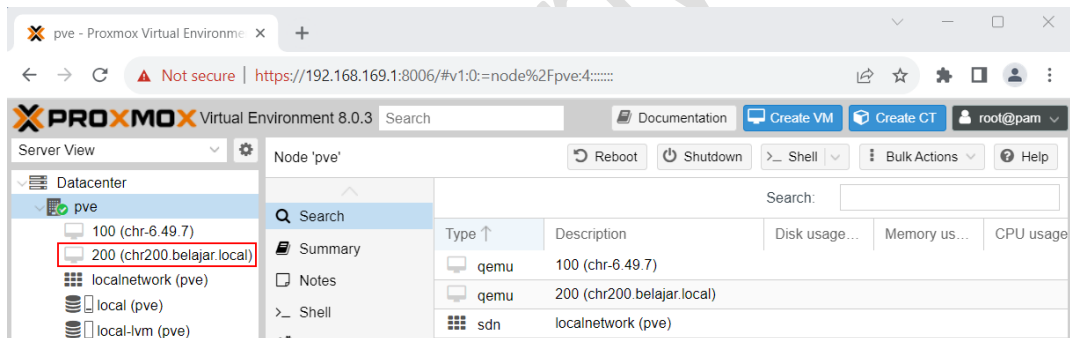
Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog **Confirm** dari **Virtual Machine** yang menampilkan ringkasan pengaturan yang telah dilakukan terkait pembuatan **Virtual Machine**, seperti terlihat pada gambar berikut:

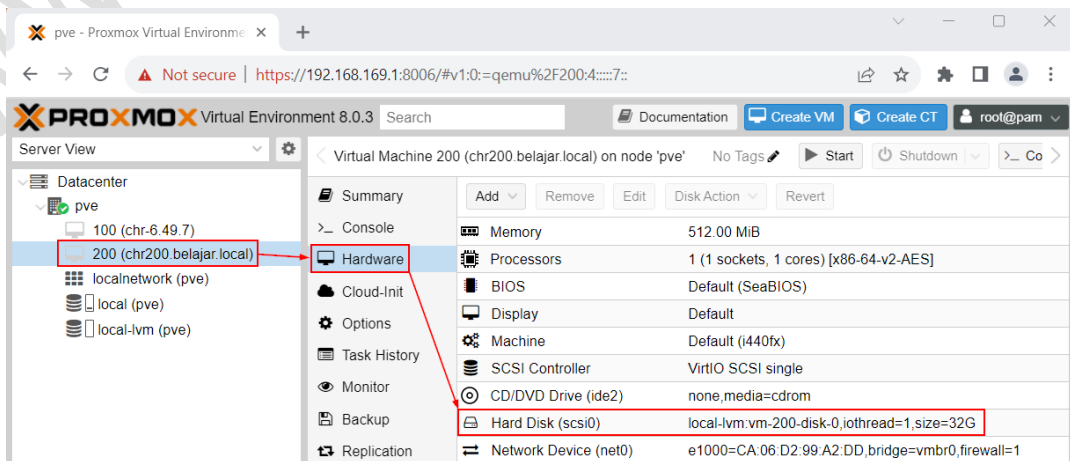


Klik tombol **Finish**.

Hasil dari pembuatan VM dengan ID 200, seperti terlihat pada gambar berikut:



- Menghapus **hard disk** pada VM ID 200 dengan cara memilih **Datacenter > pve > 200 (chr200.belajar.local)** pada panel sebelah kiri dari *Server View*. Sedangkan pada panel detail sebelah kanan pilih **Hardware** maka akan terlihat *hard disk* yang terdapat pada VM tersebut, seperti terlihat pada gambar berikut:

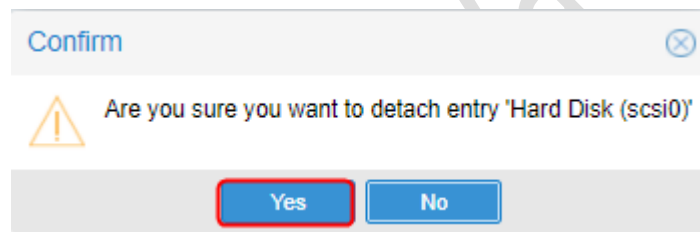


Selanjutnya pilih **Hard Disk (scsi0)** dan klik tombol **Detach**, seperti terlihat pada gambar berikut:

Virtual Machine 200 (chr200.belajar.local) on node 'pve' No Tags ▶ Start ⏻ Shutdown >_ Co

Summary	Add	Detach	Edit	Disk Action	Revert
Console	Memory	512.00 MiB			
Hardware	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]			
Cloud-Init	BIOS	Default (SeaBIOS)			
Options	Display	Default			
Task History	Machine	Default (i440fx)			
Monitor	SCSI Controller	VirtIO SCSI single			
Backup	CD/DVD Drive (ide2)	none,media=cdrom			
Replication	Hard Disk (scsi0)	local-lvm:vm-200-disk-0,iotread=1,size=32G			
	Network Device (net0)	e1000=CA:06:D2:99:A2:DD,bridge=vibr0,firewall=1			

Maka akan tampil kotak dialog **Confirm** yang mengkonfirmasi proses **detach** dari **Hard Disk (scsi0)**, seperti terlihat pada gambar berikut:

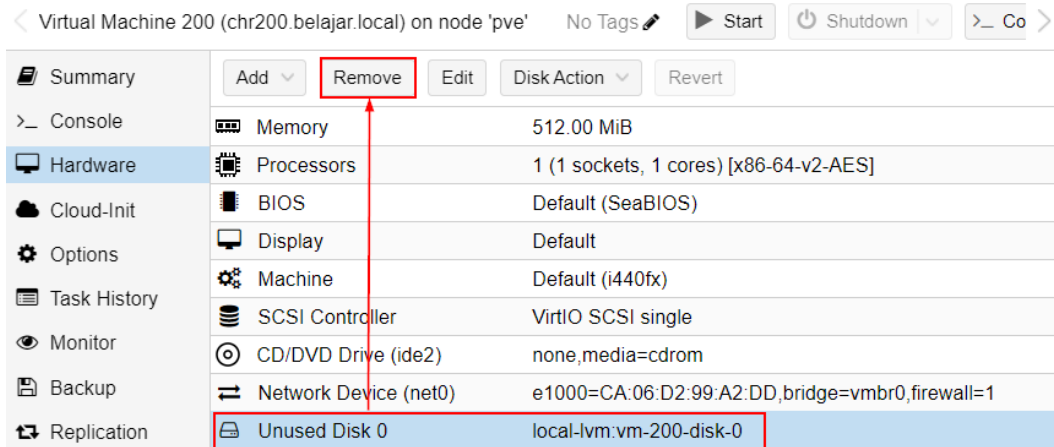


Klik tombol **Yes** maka hasilnya adalah status *disk* akan berubah menjadi **Unused Disk 0**, seperti terlihat pada gambar berikut:

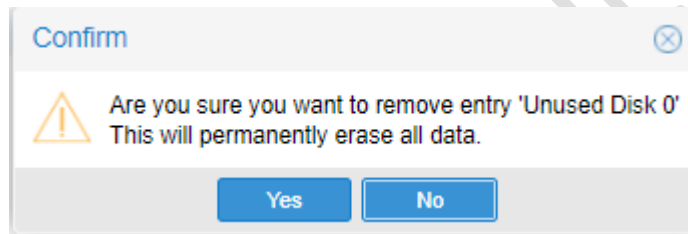
Virtual Machine 200 (chr200.belajar.local) on node 'pve' No Tags ▶ Start ⏻ Shutdown >_ Co

Summary	Add	Detach	Edit	Disk Action	Revert
Console	Memory	512.00 MiB			
Hardware	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]			
Cloud-Init	BIOS	Default (SeaBIOS)			
Options	Display	Default			
Task History	Machine	Default (i440fx)			
Monitor	SCSI Controller	VirtIO SCSI single			
Backup	CD/DVD Drive (ide2)	none,media=cdrom			
Replication	Network Device (net0)	e1000=CA:06:D2:99:A2:DD,bridge=vibr0,firewall=1			
	Unused Disk 0	local-lvm:vm-200-disk-0			

Terakhir pilih **Unused Disk 0** dan klik tombol **Remove** untuk menghapus *disk* tersebut dari VM, seperti terlihat pada gambar berikut:

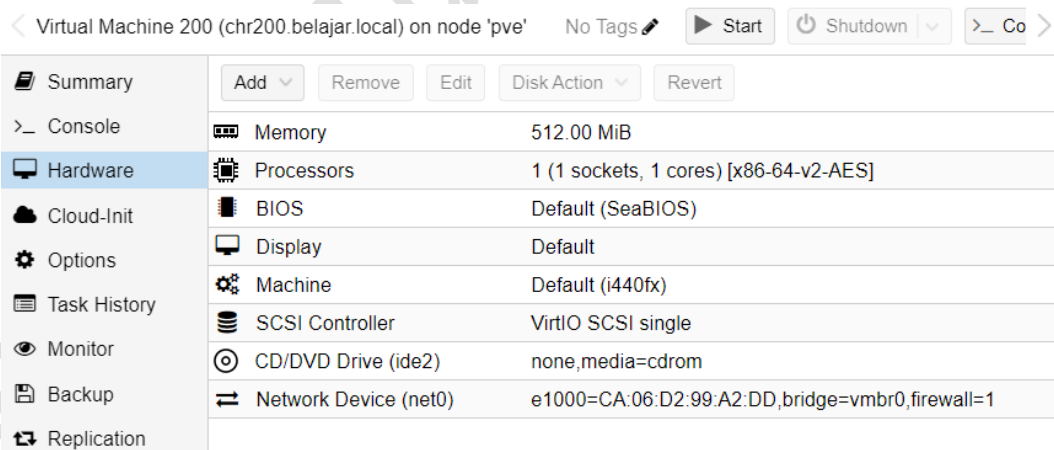


Tampil kotak dialog **Confirm** yang mengkonfirmasi proses penghapusan **Unused Disk 0**, seperti terlihat pada gambar berikut:



Proses ini akan menyebabkan semua data pada *disk* tersebut dihapus secara permanen. Klik tombol **Yes**.

Hasil akhir dari penghapusan *disk* tersebut akan terlihat seperti pada gambar berikut:



5. Meng-**import** *file raw disk image* **chr-6.49.7.img** yang terdapat didalam folder “temp” ke **VM ID 200** dan menentukan lokasi *disk* sebagai tujuan proses *import* yaitu **local-lvm** dengan mengeksekusi perintah `qm importdisk 200 temp/chr-6.49.7.img local-lvm` melalui aplikasi *Putty*. Cuplikan eksekusi perintah tersebut, seperti terlihat pada gambar berikut:

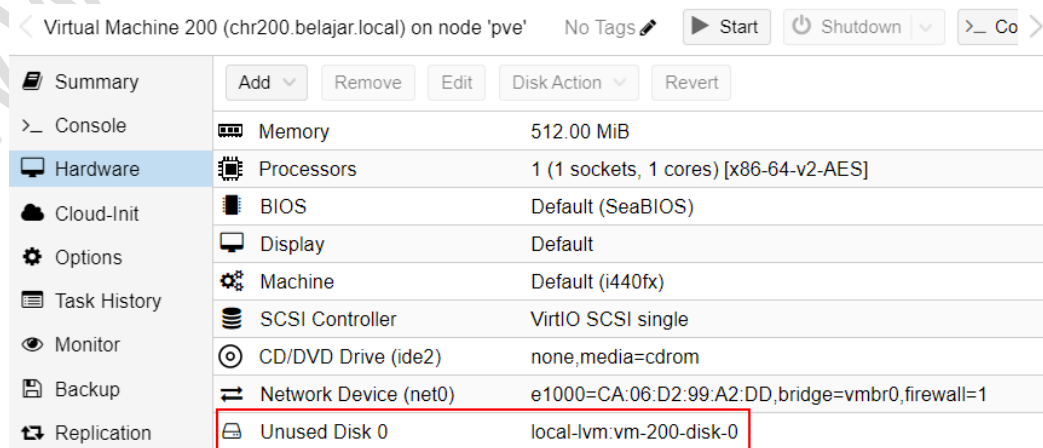

```

192.168.169.1 - PuTTY
root@pve:~# qm importdisk 200 temp/chr-6.49.7.img local-lvm
importing disk 'temp/chr-6.49.7.img' to VM 200 ...
Logical volume "vm-200-disk-0" created.
transferred 0.0 B of 64.0 MiB (0.00%)
transferred 2.0 MiB of 64.0 MiB (3.12%)
transferred 4.0 MiB of 64.0 MiB (6.25%)
transferred 6.0 MiB of 64.0 MiB (9.38%)
transferred 8.0 MiB of 64.0 MiB (12.50%)
transferred 10.0 MiB of 64.0 MiB (15.62%)
transferred 12.0 MiB of 64.0 MiB (18.75%)
transferred 14.0 MiB of 64.0 MiB (21.88%)
transferred 16.0 MiB of 64.0 MiB (25.00%)
transferred 18.0 MiB of 64.0 MiB (28.12%)
transferred 20.0 MiB of 64.0 MiB (31.25%)
transferred 22.0 MiB of 64.0 MiB (34.38%)
transferred 24.0 MiB of 64.0 MiB (37.50%)
transferred 26.0 MiB of 64.0 MiB (40.62%)
transferred 28.0 MiB of 64.0 MiB (43.75%)
transferred 30.0 MiB of 64.0 MiB (46.88%)
transferred 32.0 MiB of 64.0 MiB (50.00%)
transferred 34.0 MiB of 64.0 MiB (53.12%)
transferred 36.0 MiB of 64.0 MiB (56.25%)
transferred 38.0 MiB of 64.0 MiB (59.38%)
transferred 40.0 MiB of 64.0 MiB (62.50%)
transferred 42.0 MiB of 64.0 MiB (65.62%)
transferred 44.0 MiB of 64.0 MiB (68.75%)
transferred 46.0 MiB of 64.0 MiB (71.88%)
transferred 48.0 MiB of 64.0 MiB (75.00%)
transferred 50.0 MiB of 64.0 MiB (78.12%)
transferred 52.0 MiB of 64.0 MiB (81.25%)
transferred 54.0 MiB of 64.0 MiB (84.38%)
transferred 56.0 MiB of 64.0 MiB (87.50%)
transferred 58.0 MiB of 64.0 MiB (90.62%)
transferred 60.0 MiB of 64.0 MiB (93.75%)
transferred 62.0 MiB of 64.0 MiB (96.88%)
transferred 64.0 MiB of 64.0 MiB (100.00%)
transferred 64.0 MiB of 64.0 MiB (100.00%)
Successfully imported disk as 'unused0:local-lvm:vm-200-disk-0'
root@pve:~#

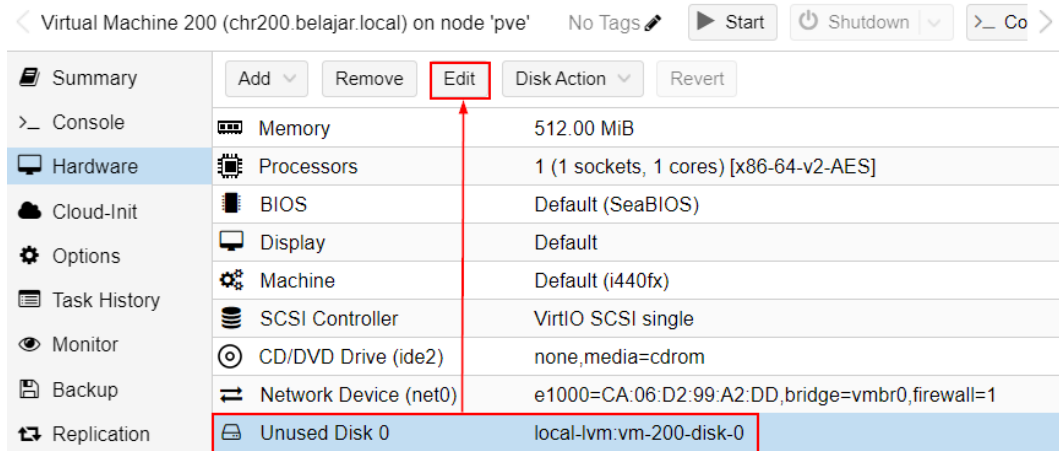
```

Tunggu hingga prosesnya selesai dilakukan dimana ditandai dengan pesan “Successfully imported disk as 'unused0:local-lvm:vm-200-disk-0'”.

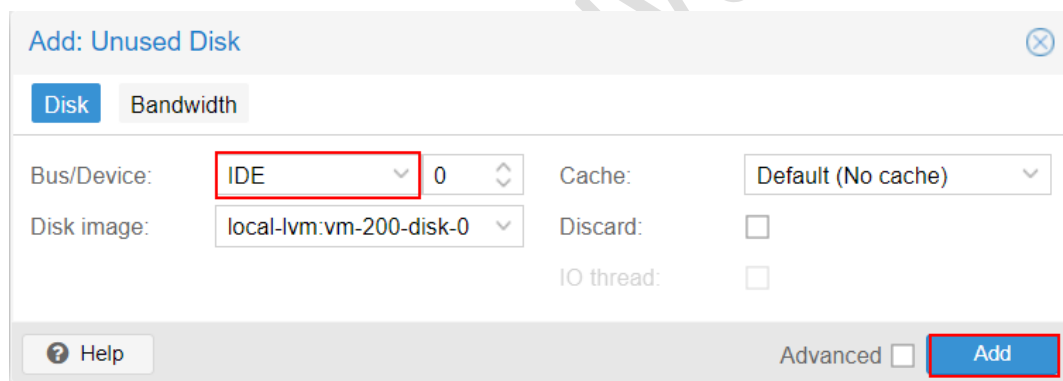
Hasil dari operasi *import file* tersebut dapat diverifikasi dengan mengakses menu **Hardware** pada **VM ID 200 (chr200.belajar.local)** dimana akan menunjukkan **Unused Disk 0**, seperti terlihat pada gambar berikut:



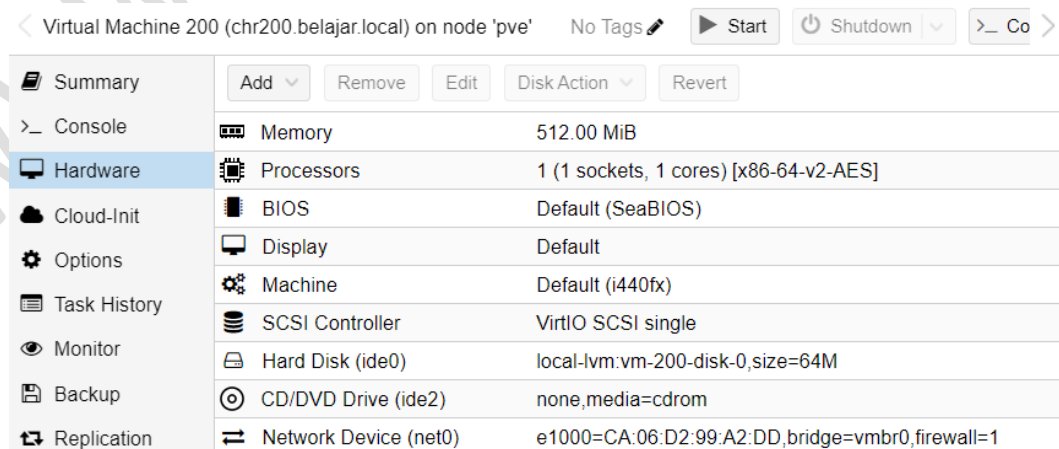
6. Menambahkan **Unused Disk 0** sehingga dapat digunakan oleh **VM ID 200** dengan cara memilih *disk* tersebut dan klik tombol **Edit**, seperti terlihat pada gambar berikut:



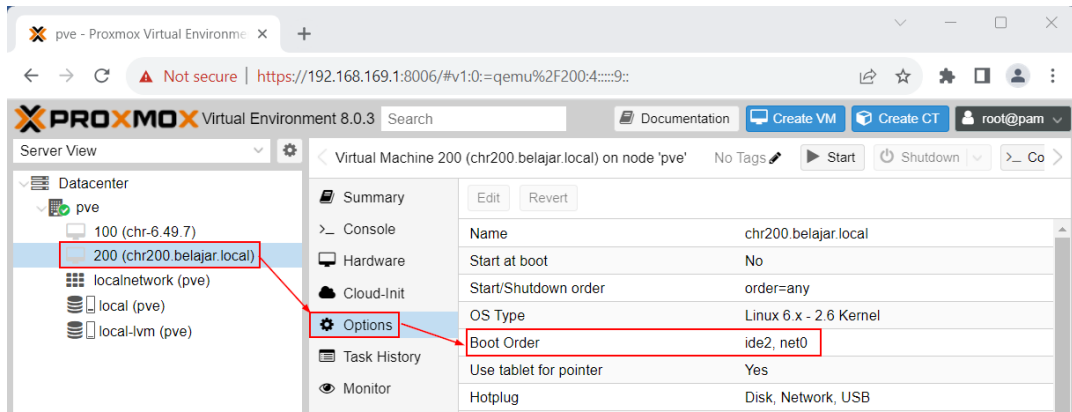
Tampil kotak dialog **Add: Unused Disk**. Lakukan pengaturan pada parameter **Bus/IDE**: agar menggunakan **IDE**, seperti terlihat pada gambar berikut:



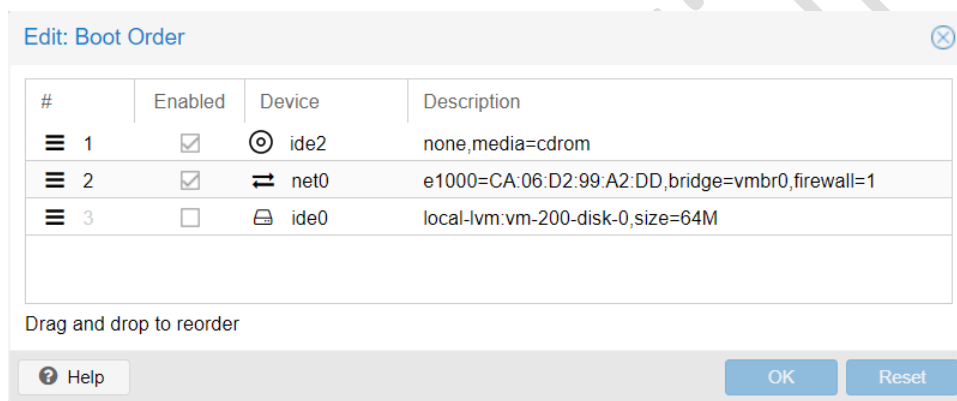
Klik tombol **Add** untuk memproses perubahan maka hasilnya akan terlihat seperti pada gambar berikut:



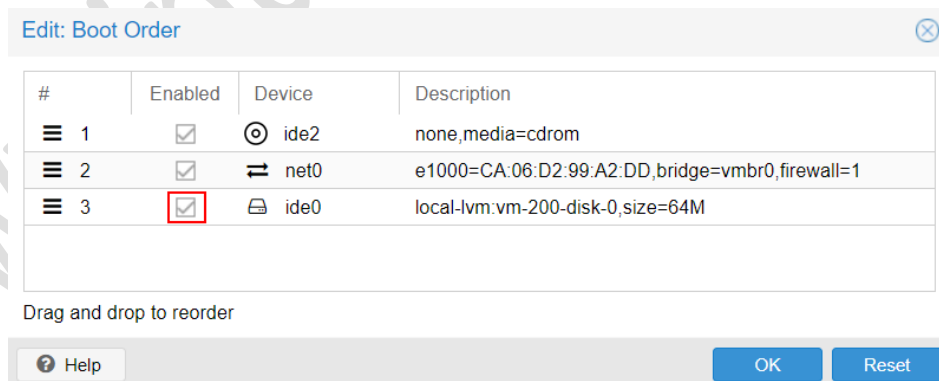
7. Mengatur **Boot Order pertama** dari **VM ID 200** agar menggunakan **ide0** dengan mengakses menu, seperti terlihat pada gambar berikut:



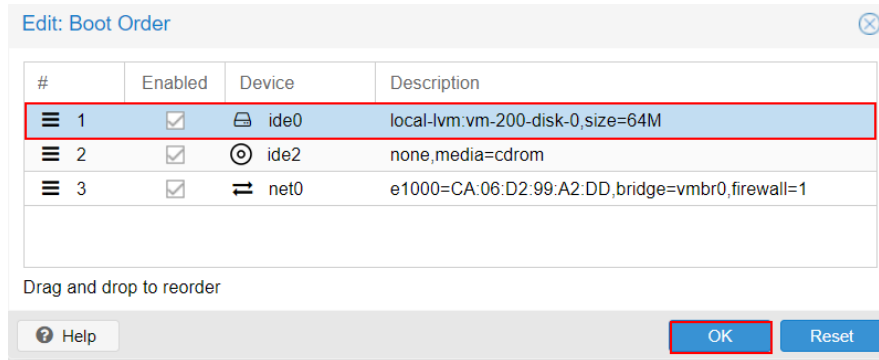
Selanjutnya pilih **Boot Order** **ide2**, **net0** dan klik tombol **Edit**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Edit: Boot Order**. Klik *checkbox* pada kolom **Enabled** dari baris pada nomor urutan pilihan 3 untuk **Device "ide0"** sehingga hasilnya seperti terlihat pada gambar berikut:

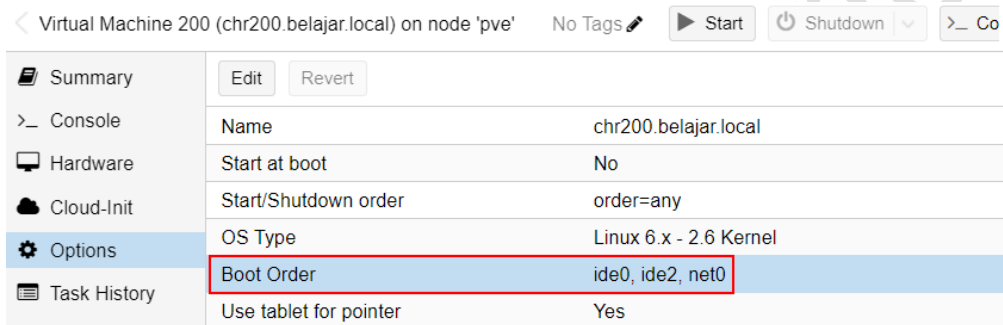


Lakukan **drag and drop** dengan memilih nilai dari baris nomor urutan pilihan 3 untuk **Device "ide0"** ke atas sehingga menjadi baris dengan nomor urutan pilihan 1, seperti terlihat pada gambar berikut:

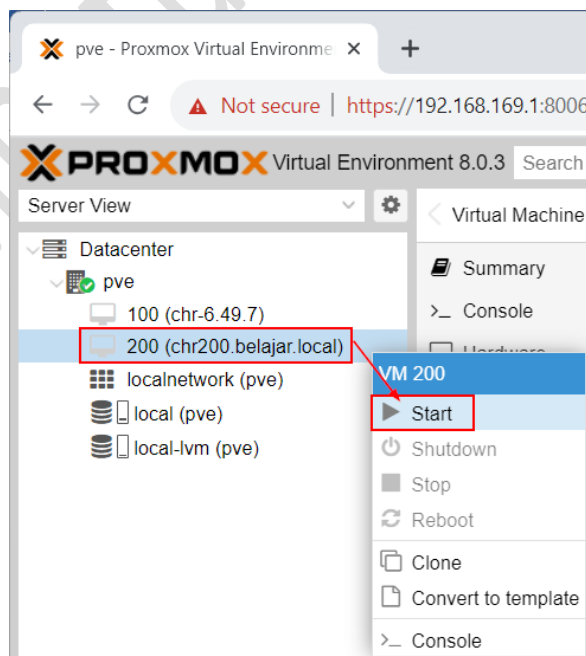


Klik tombol **OK** untuk menyimpan perubahan.

Hasilnya akhir dari penyesuaian **Boot Order** akan terlihat seperti gambar berikut:



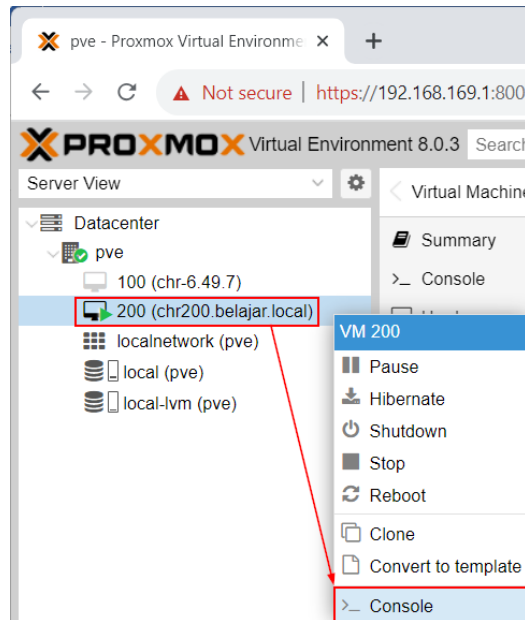
- Untuk menjalankan **VM CHR**, klik kanan pada “**200 (chr200.belajar.local)**” di bawah *node* “**pve**” dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:



VM CHR berhasil dijalankan dimana ditandai dengan pesan status **OK** untuk **CT 200 - Start** pada bagian **Tasks** dari **Log Panel**, seperti terlihat pada gambar berikut:

Start Time ↓	End Time	Node	User name	Description	Status
Sep 15 01:14:49	Sep 15 01:14:50	pve	root@pam	VM 200 - Start	OK

9. Untuk mengakses tampilan atau **Console** dari **VM ID 200**, klik kanan pada “**200 (chr200.belajar.local)**” di bawah *node* “**pve**” dari menu **Datacenter** dan pilih **Console**, seperti terlihat pada gambar berikut:

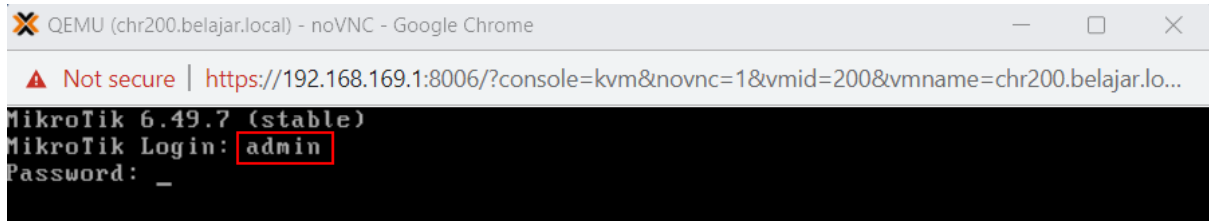


Tampil inputan **MikroTik Login:** untuk proses otentikasi sebelum pengguna dapat mengakses **Command Line Interface (CLI)** dari *Mikrotik*, seperti terlihat pada gambar berikut:



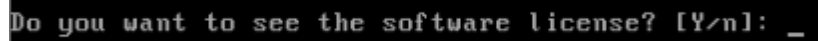
Masukkan nama login “**admin**” pada inputan **MikroTik Login** dan tekan tombol **Enter**.

Selanjutnya tampil inputan **Password:**. Tekan tombol **Enter** untuk melanjutkan karena *password* untuk user “*admin*” adalah **kosong (blank)**, seperti terlihat pada gambar berikut:



```
QEMU (chr200.belajar.local) - noVNC - Google Chrome
https://192.168.169.1:8006/?console=kvm&novnc=1&vmid=200&vmname=chr200.belajar.lo...
MikroTik 6.49.7 (stable)
MikroTik Login: admin
Password: _
```

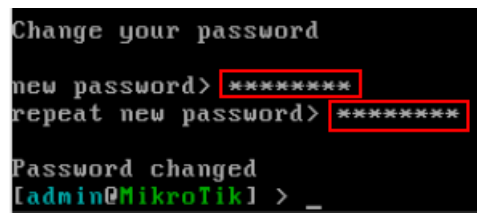
Selanjutnya tampil pesan “**Do you want to see the software license? [Y/n]**”, seperti terlihat pada gambar berikut:



```
Do you want to see the software license? [Y/n]: _
```

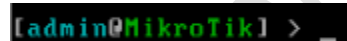
Tekan “**n**” untuk tidak menampilkan lisensi perangkat lunak.

Selanjutnya tampil pesan **Change your password** untuk mengubah sandi dari *user* “**admin**”. Sebagai contoh *password* yang ingin digunakan adalah “**12345678**” sehingga pada **input new password>** yang tampil, masukkan “**12345678**” dan tekan tombol **Enter**. Tampil **input repeat new password>**, untuk memasukkan kembali sandi baru yaitu “**admin**” dan tekan tombol **Enter**, seperti terlihat pada gambar berikut:



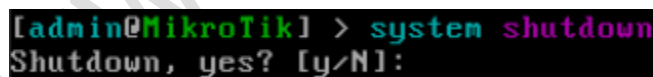
```
Change your password
new password> *****
repeat new password> *****
Password changed
[admin@MikroTik] > _
```

Terlihat *prompt CLI* dari *Mikrotik*, seperti gambar berikut:



```
[admin@MikroTik] > _
```

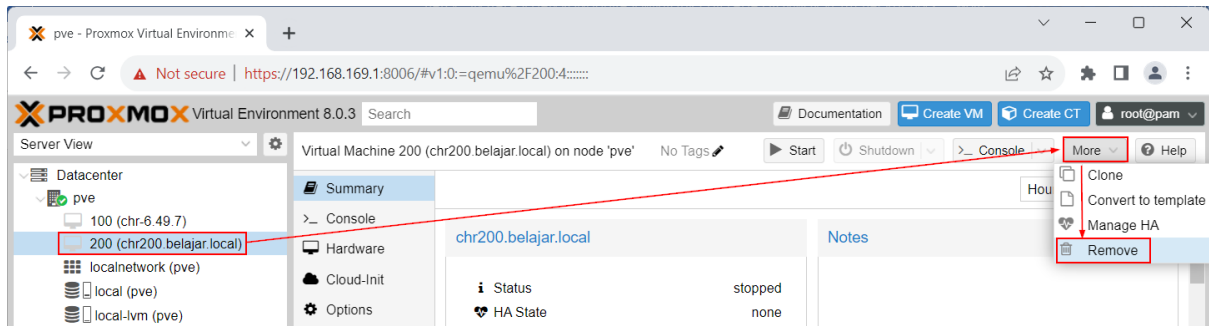
- Untuk mematikan *Mikrotik*, eksekusi perintah “**system shutdown**”, seperti terlihat pada gambar berikut:



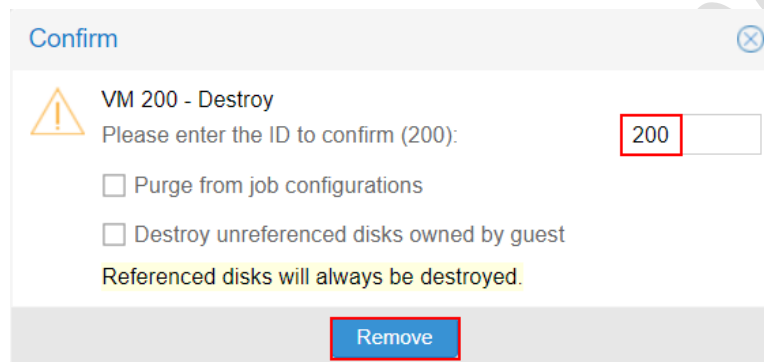
```
[admin@MikroTik] > system shutdown
Shutdown, yes? [y/N]:
```

Pada pesan konfirmasi “**Shutdown, yes? [y/N]:**” yang tampil, tekan tombol “**y**” untuk melanjutkan proses *shutdown*. Tunggu hingga proses *shutdown* selesai dilakukan. Tutup kotak dialog **console VM 200** (‘**chr200.belajar.local**’).

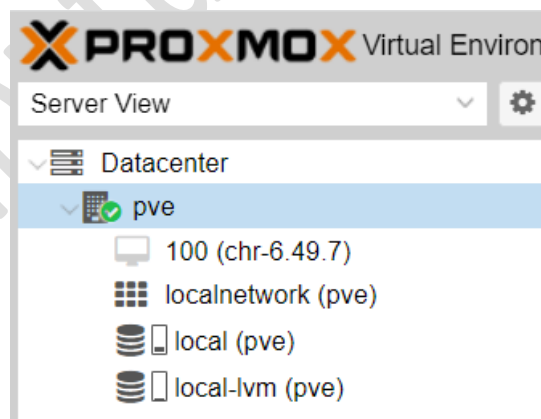
- Apabila sudah tidak diperlukan maka **VM CHR** dengan **ID 200** dapat dihapus dengan cara memilih “**200 (chr200.belajar.local)**” di bawah *node* “**pve**” dari menu **Datacenter**. Kemudian pada panel detail pilih *dropdown* **More** yang terdapat pada pojok kanan, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Confirm** yang meminta memasukkan **VM ID** yang akan dihapus. Masukkan **200** dan tekan tombol **Remove**, seperti terlihat pada gambar berikut:



Proses penghapusan VM CHR tersebut berhasil dilakukan dimana ditandai dengan pada panel sebelah kiri di bawah *node* “**pve**” dari menu **Datacenter** sudah tidak terlihat **VM ID 200**, seperti terlihat pada gambar berikut:



12. Untuk keluar dari *web interface* konfigurasi *Proxmox* maka klik pada *dropdown* menu **root@pam** di sebelah pojok kanan atas dan pilih **Logout**.

BAB VI

INSTALASI DAN KONFIGURASI LINUX CONTAINER (LXC)

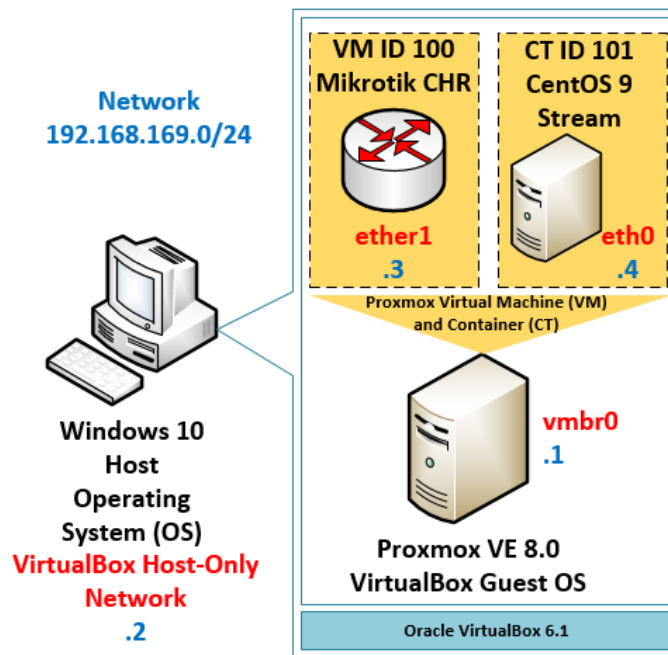
CENTOS 9 STREAM PADA PROXMOX VE 8.0

Pada bab ini akan dibahas penerapan teknologi virtualisasi yang didukung oleh *Proxmox VE* yaitu **Linux Container (LXC)** menggunakan **CentOS 9 Stream**, sebagai pelengkap dari contoh penerapan **Kernel-based Virtual Machine (KVM)** menggunakan **Mikrotik CHR** di bab sebelumnya. Menurut situs [Proxmox](#), **LXC** merupakan lingkungan virtualisasi level sistem operasi untuk menjalankan beberapa sistem Linux terisolasi pada sebuah kontrol host Linux. *LXC* menjadi alternatif dari *full machine virtualization* yang menawarkan *low overhead*. *Container* akan menggunakan sistem operasi dari *host* daripada mengemulasikan sistem operasi secara lengkap sehingga berdampak pada keseluruhan *container* menggunakan *kernel* yang sama dan dapat mengakses sumber daya secara langsung dari *host*. Pengguna Linux dapat membuat dan manajemen *container* sistem atau aplikasi menggunakan *Application Programming Interface (API)*.

Pembahasan pada bab ini terdiri dari 2 (dua) bagian yaitu (a) Rancangan Jaringan Ujicoba, (b) Instalasi dan Konfigurasi *LXC CentOS 9 Stream* pada *Proxmox VE*. **Sebelum mengikuti tutorial ini, pastikan Server Proxmox telah dapat terkoneksi ke Internet karena paket OpenSSH yang diperlukan untuk menyediakan layanan SSH Server pada container CentOS 9 Stream akan diambil langsung dari repository CentOS di Internet.**

A. RANCANGAN JARINGAN UJICOBA

Rancangan jaringan ujicoba yang digunakan, seperti terlihat pada gambar berikut:



Pada *Server Proxmox VE 8.0* akan dilakukan pembuatan *Container (CT)* dengan sistem operasi *CentOS 9 Stream* dan menggunakan ID **101** serta alamat IP **192.168.169.4/24**.

B. INSTALASI DAN KONFIGURASI LXC CENTOS 9 STREAM PADA PROXMOX VE

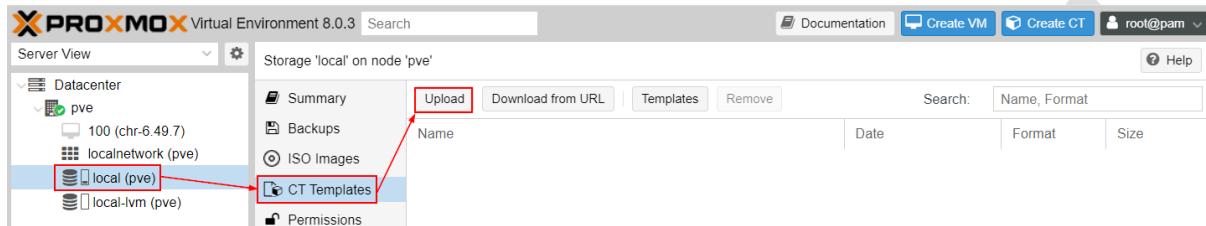
Adapun langkah-langkah instalasi dan konfigurasi *LXC CentOS 9 Stream* pada *Proxmox VE* adalah sebagai berikut:

1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**, seperti terlihat pada gambar berikut:

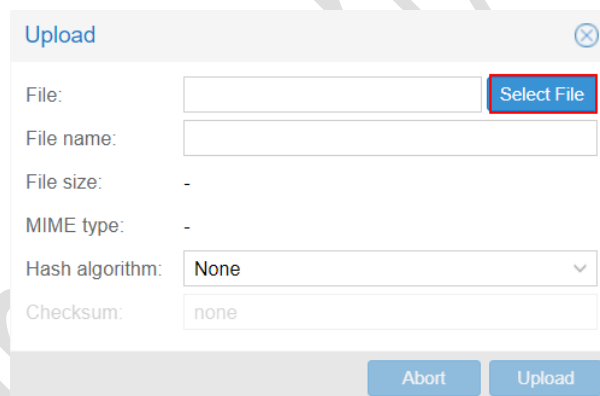
The screenshot shows the Proxmox VE Login dialog box. The User name field contains 'root', the Password field contains '.....', the Realm is set to 'Linux PAM standard authentication', and the Language is set to 'English - English'. There is a 'Login' button and a 'Save User name' checkbox.

Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

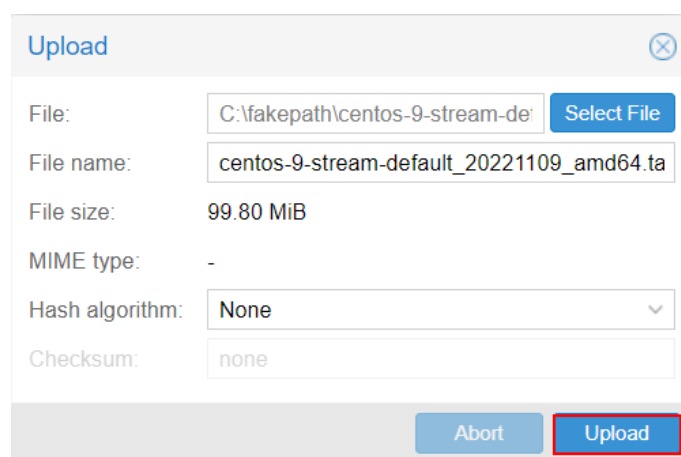
3. Mengunggah file **template container** ke *Server Proxmox* dengan mengakses **node "pve"** di bawah menu **Datacenter** pada panel sebelah kiri dan memilih **storage local (pve)**. Pilih menu **CT Templates** pada panel sebelah kanan dari **local (pve)** dan pilih **Upload** untuk mengunggah *file template container CentOS 8 Stream*, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Upload** dan tekan tombol **Select File...** untuk mengarahkan ke lokasi direktori penyimpanan file **template CentOS 9 Stream**, seperti terlihat pada gambar berikut:

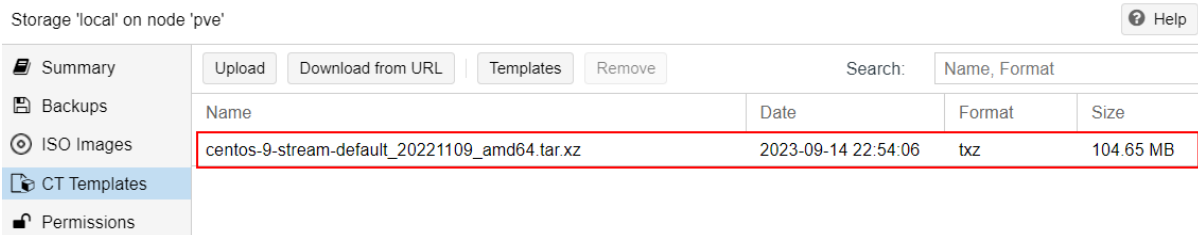


Sebagai contoh di **D:\ASJ\centos-9-stream-default_20221109_amd64.tar.xz**, seperti terlihat pada gambar berikut:

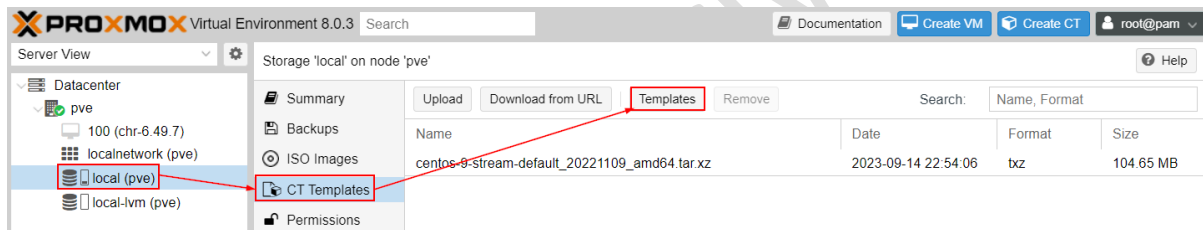


Tekan tombol **Upload** dan tunggu hingga proses pengunggahan file selesai dilakukan yang ditandai dengan pesan **TASK OK** pada kotak dialog **Task viewer: Copy data** yang tampil. Tutup kotak dialog tersebut.

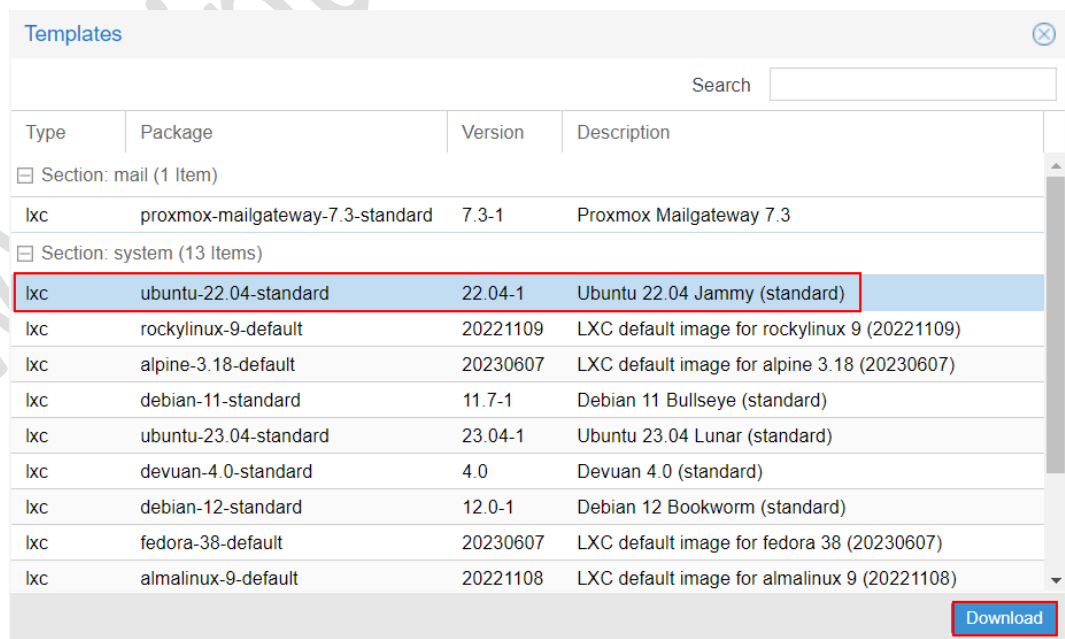
Apabila proses unggah berhasil dilakukan maka pada bagian **CT Templates** dari **storage local (pve)** akan menampilkan nama **file centos-9-stream-default_20221109_amd64.tar.xz**, seperti terlihat pada gambar berikut:



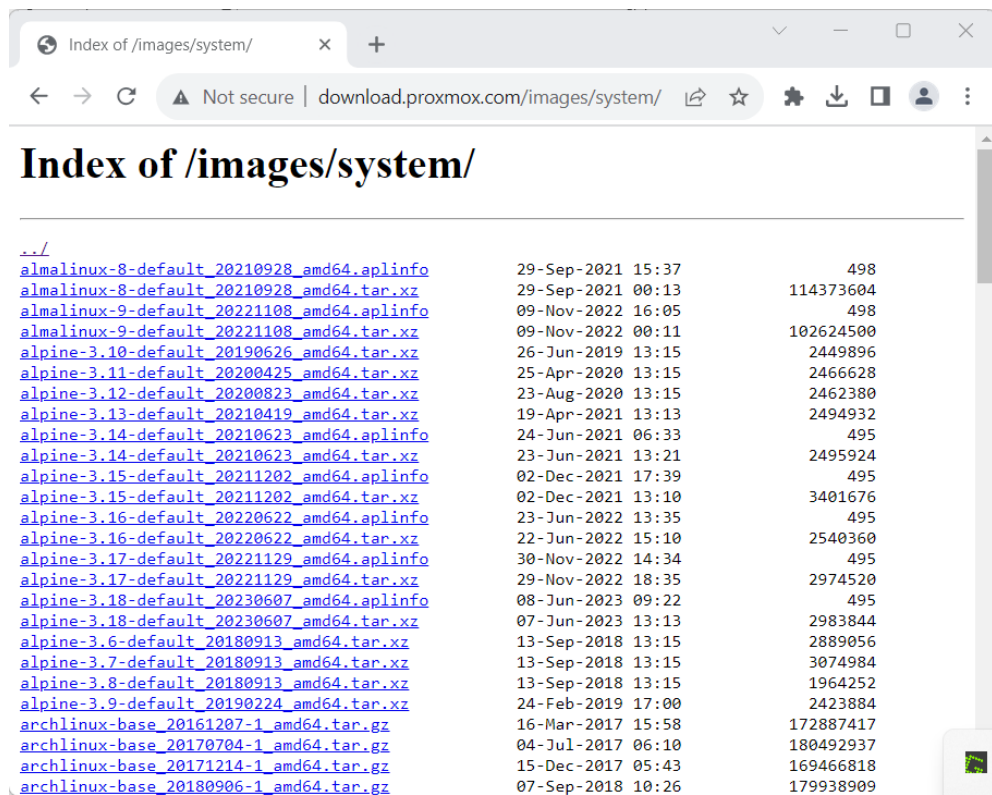
File *container template* juga dapat diunduh langsung dari *Internet* dengan menekan tombol **Templates** di bagian **CT Templates** dari **storage local (pve)**, seperti terlihat pada gambar berikut:



Pada kotak dialog **Templates** yang tampil, pilih **package** yang ingin diunduh dan tekan tombol **Download**, seperti terlihat pada gambar berikut:

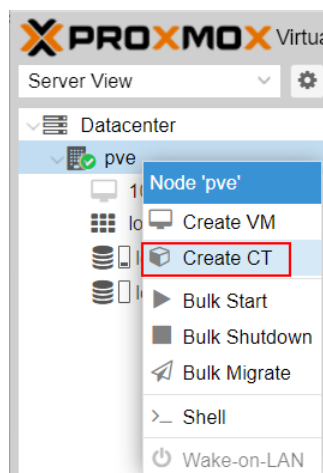


Tunggu hingga proses unduh selesai dilakukan. Atau file *template container* juga dapat diunduh secara manual melalui alamat <http://download.proxmox.com/images/system/>, seperti terlihat pada gambar berikut:



Selanjutnya file *template container* yang telah diunduh dapat diunggah ke *Server Proxmox* dengan mengikuti langkah-langkah proses unggah *template CentOS 9 Stream* yang telah dijelaskan sebelumnya.

4. Membuat **Container** dengan cara klik kanan pada *node "pve"* dibawah menu **Datacenter** di panel sebelah kiri dan memilih **Create CT**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Create: LXC Container**. Terdapat beberapa parameter yang diatur di bagian **General** dari **LXC Container**, seperti terlihat pada gambar berikut:

The screenshot shows the 'Create: LXC Container' dialog box with the 'General' tab selected. The fields are as follows:

- Node: pve
- CT ID: 101
- Hostname: server.belajar.local
- Unprivileged container:
- Nesting:
- Resource Pool: [empty]
- Password: [masked with dots]
- Confirm password: [masked with dots]
- SSH public key: [empty]

At the bottom right, the 'Next' button is highlighted with a red box.

Pada parameter **Hostname:**, masukkan nama komputer dan nama domain dari *Container CentOS 9 Stream*, sebagai contoh “**server.belajar.local**”. Sedangkan pada parameter **Password:** dan **Confirm password:**, masukkan sandi login dari user “**root**” untuk *container CentOS 9 Stream*, sebagai contoh “**12345678**”. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan bagian **Template** dari **LXC Container**. Pilih **centos-9-stream-default_20221109_amd64.tar.xz** pada parameter **Template:**, seperti terlihat pada gambar berikut:

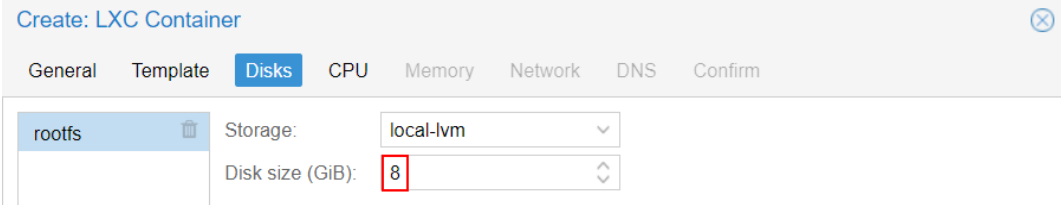
The screenshot shows the 'Create: LXC Container' dialog box with the 'Template' tab selected. The 'Storage' is set to 'local' and the 'Template' dropdown menu is open, showing the following options:

Name	For...	Size
centos-9-stream-default_20221109_amd64.tar.xz	txz	104.65 MB

The selected template is highlighted with a blue background and a red border.

Klik tombol **Next** untuk melanjutkan.

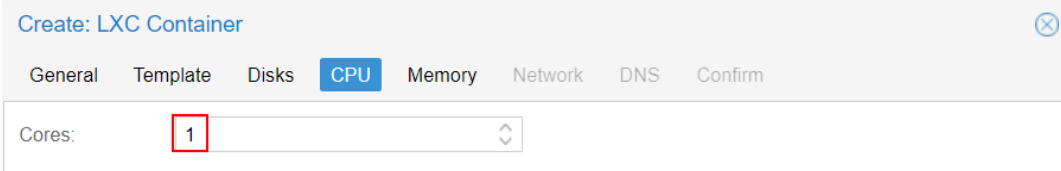
Tampil kotak dialog pengaturan bagian **Root Disk** dari **LXC Container**. Lakukan penyesuaian ukuran *hardisk* yang digunakan pada parameter **Disk size (GB)**: jika diperlukan, secara default menggunakan **8 GB**, seperti terlihat pada gambar berikut:



The screenshot shows the 'Create: LXC Container' dialog box with the 'Disks' tab selected. The 'Storage' dropdown menu is set to 'local-lvm'. The 'Disk size (GiB)' dropdown menu is set to '8'.

Klik tombol **Next** untuk melanjutkan.

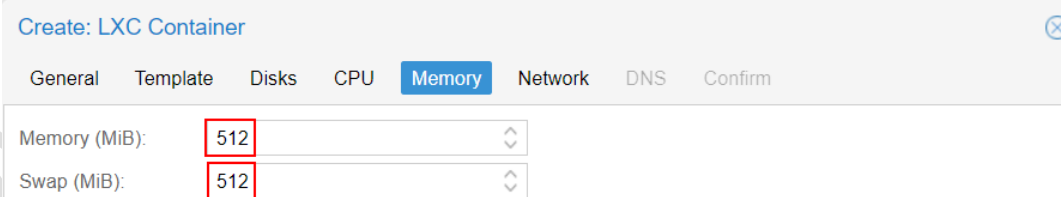
Tampil kotak dialog pengaturan **CPU** dari **LXC Container**. Pada parameter **Cores**:, lakukan penyesuaian jumlah *Core CPU* yang digunakan apabila diperlukan. Secara *default* bernilai 1 (satu), seperti terlihat pada gambar berikut:



The screenshot shows the 'Create: LXC Container' dialog box with the 'CPU' tab selected. The 'Cores' dropdown menu is set to '1'.

Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan **Memory** dari **LXC Container**. Terdapat 2 (dua) parameter yang dapat diatur yaitu **Memory (MiB)** dan **Swap (MiB)**. Secara *default* masing-masing parameter tersebut bernilai **512 MiB**, seperti terlihat pada gambar berikut:

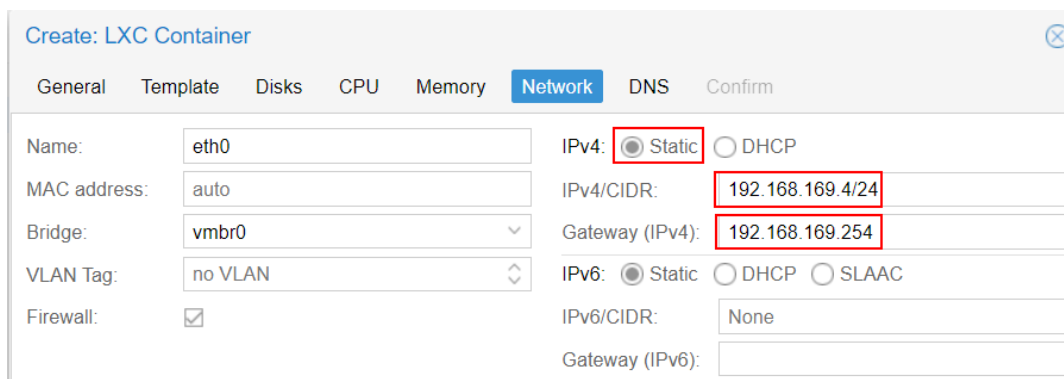


The screenshot shows the 'Create: LXC Container' dialog box with the 'Memory' tab selected. The 'Memory (MiB)' dropdown menu is set to '512' and the 'Swap (MiB)' dropdown menu is set to '512'.

Silakan menyesuaikan nilai dari parameter **Memory (MiB)** dan **Swap (MiB)**, jika diperlukan. Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan **Network** dari **LXC Container**. Secara *default* alokasi pengaturan pengalamatan **IPv4** pada **LXC Container** adalah secara **Static**. Pada parameter **IPv4/CIDR**: masukkan alamat IP dan *subnetmask* yang digunakan oleh *container CentOS 9 Stream* yaitu **192.168.169.4/24**. Sedangkan pada bagian

Gateway (IPv4):, masukkan alamat IP **192.168.169.254**, seperti terlihat pada gambar berikut:



Create: LXC Container

General Template Disks CPU Memory **Network** DNS Confirm

Name: eth0 IPv4: Static DHCP

MAC address: auto IPv4/CIDR: 192.168.169.4/24

Bridge: vubr0 Gateway (IPv4): 192.168.169.254

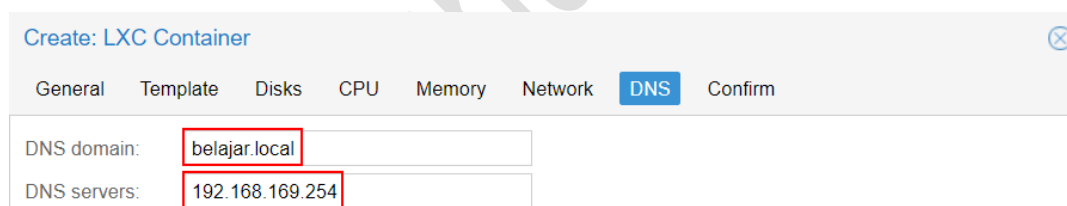
VLAN Tag: no VLAN IPv6: Static DHCP SLAAC

Firewall: IPv6/CIDR: None

Gateway (IPv6):

Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog pengaturan **DNS** dari **LXC Container**. Pada parameter **DNS domain:** masukkan nama domain yang digunakan oleh *container CentOS 7*, sebagai contoh menggunakan “**belajar.local**”. Sedangkan pada bagian **DNS server1:**, masukkan alamat IP dari **Primary Name Server**, sebagai contoh menggunakan alamat IP **192.168.169.254**, seperti terlihat pada gambar berikut:



Create: LXC Container

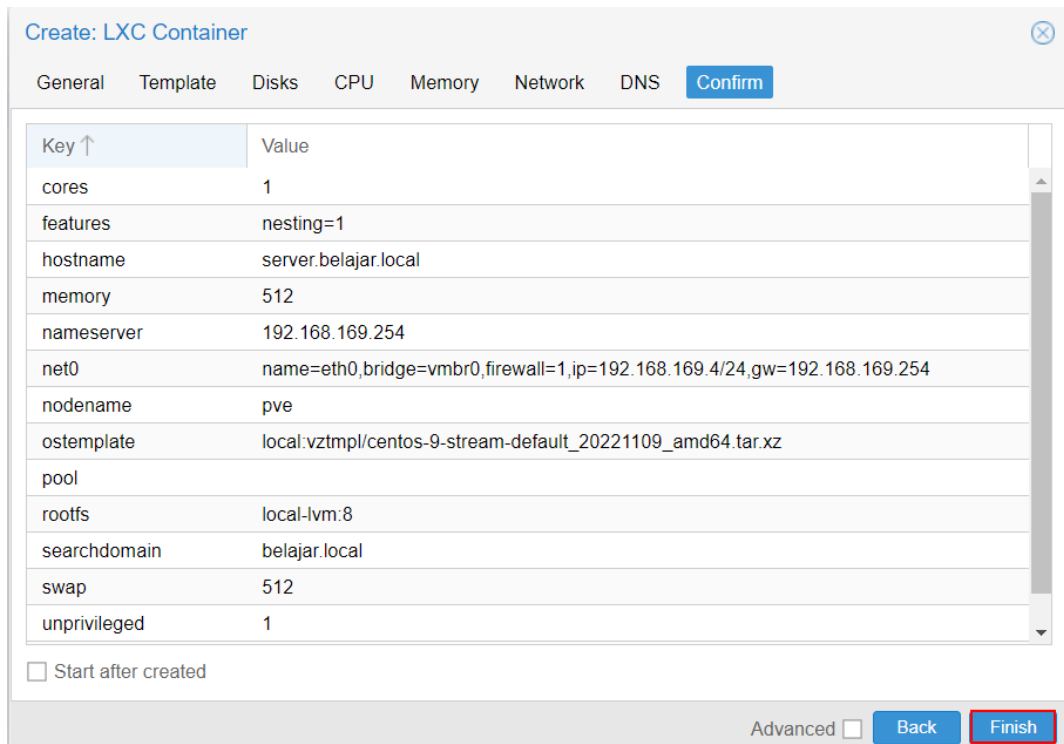
General Template Disks CPU Memory Network **DNS** Confirm

DNS domain: belajar.local

DNS servers: 192.168.169.254

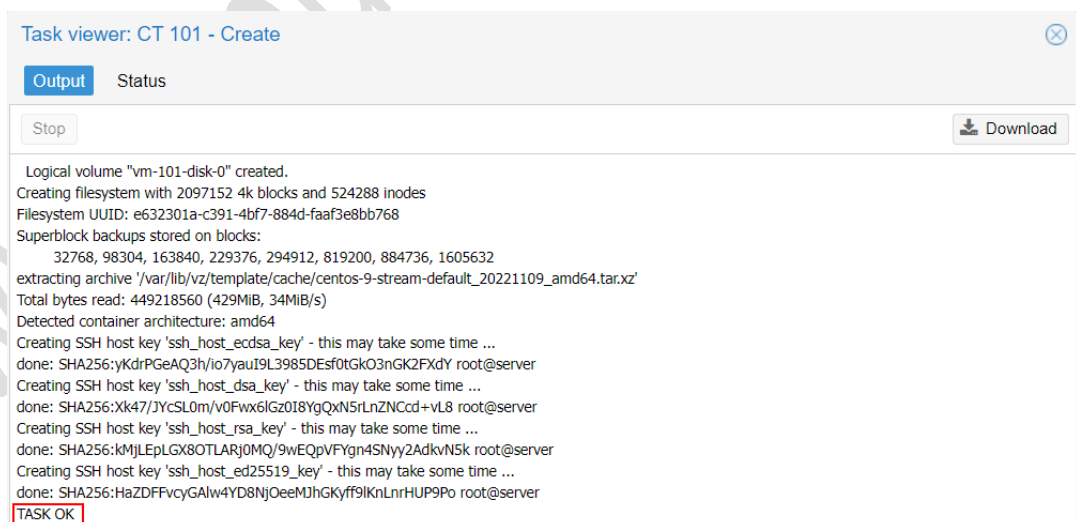
Klik tombol **Next** untuk melanjutkan.

Tampil kotak dialog **Confirm** dari **LXC Container** yang menampilkan ringkasan pengaturan yang telah dilakukan terkait pembuatan *container CentOS 9 Stream*, seperti terlihat pada gambar berikut:



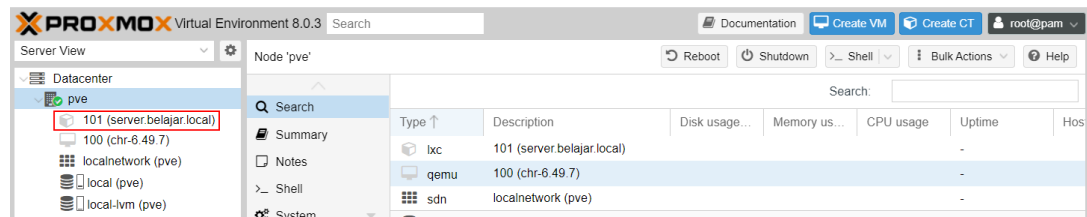
Klik tombol **Finish**.

Tampil kotak dialog **Task viewer: CT 101 – Create**. Tunggu hingga proses pembuatan *container CentOS 9 Stream* selesai dibuat dimana ditandai dengan pesan **“TASK OK”** pada bagian **Output** dari kotak dialog **Task viewer: CT 101 – Create**, seperti terlihat pada gambar berikut:

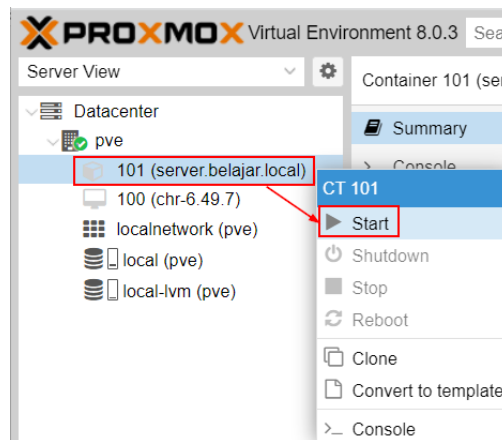


Tutup kotak dialog **Task viewer: CT 101 – Create**.

Hasil dari pembuatan *container CentOS 9 Stream* dengan ID 101, seperti terlihat pada gambar berikut:



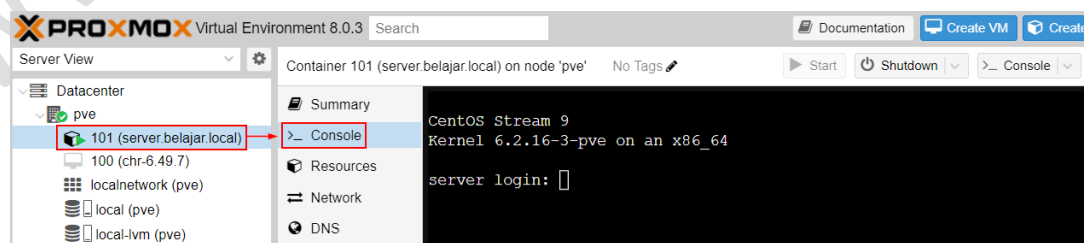
- Untuk menjalankan *Container CentOS 9 Stream*, klik kanan pada “101 (server.belajar.local)” di bawah node “pve” dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:



Container CentOS 9 Stream berhasil dijalankan dimana ditandai dengan pesan status **OK** untuk **CT 101 - Start** pada bagian **Tasks** dari **Log Panel**, seperti terlihat pada gambar berikut:

Start Time	End Time	Node	User name	Description	Status
Sep 15 21:26:42	Sep 15 21:26:42	pve	root@pam	Start all VMs and Containers	OK
Sep 15 13:58:27	Sep 15 13:58:30	pve	root@pam	CT 101 - Start	OK
Sep 15 13:46:36	Sep 15 13:46:52	pve	root@pam	CT 101 - Create	OK

- Untuk mengakses tampilan dari **CT 101**, pilih **Console** pada panel sebelah kanan dari **CT 101 (server.belajar.local)**, seperti terlihat pada gambar berikut:



Tampil inputan **Server Login** untuk proses otentikasi sebelum pengguna dapat mengakses **Command Line Interface (CLI)** dari *Container CentOS 9 Stream*. Masukkan nama login “**root**” pada inputan **Server Login** dan tekan tombol **Enter**.

Tampil inputan **Password:**, masukkan sandi *login* dari user “**root**” yaitu “**12345678**”, dan tekan tombol **Enter**. Apabila proses otentikasi login berhasil dilakukan maka akan tampil *prompt CLI* dari *container CentOS 9 Stream* yang ditandai dengan tanda #, seperti terlihat pada gambar berikut:

```
CentOS Stream 9
Kernel 6.2.16-3-pve on an x86_64

server login: root
Password:
[root@server ~]#
```

- Menginstalasi paket aplikasi **OpenSSH** agar *container CentOS 9 Stream* dapat di akses secara *remote* melalui **SSH Client** pada **Client Windows 10**.

```
[root@server ~]# yum -y install openssh openssh-server \
> openssh-clients openssl-libs
```

Tampil proses instalasi paket, seperti terlihat pada cuplikan gambar berikut:

```
Total download size: 5.0 M
Downloading Packages:
(1/5): openssh-8.7p1-34.el9.x86_64.rpm           39 kB/s | 461 kB      00:11
(2/5): openssh-clients-8.7p1-34.el9.x86_64.rpm  47 kB/s | 715 kB      00:15
(3/5): openssh-server-8.7p1-34.el9.x86_64.rpm  21 kB/s | 460 kB      00:21
[4-5/5]: openssl-libs- 76% [=====]          ] 117 kB/s | 3.8 MB     00:10 ETA
```

Tunggu hingga proses instalasi selesai dilakukan.

- Mengaktifkan *service sshd* agar layanan **SSH Server**.

```
[root@server ~]# systemctl start sshd
```

- Memverifikasi hasil pengaktifan *service sshd*.

```
[root@server ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset:
   enabled)
   Active: active (running) since Fri 2023-09-15 06:09:03 UTC; 3s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 230 (sshd)
     Tasks: 1 (limit: 18543)
    Memory: 1.4M
         CPU: 13ms
    CGroup: /system.slice/sshd.service
            └─230 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 15 06:09:03 server.belajar.local systemd[1]: Starting OpenSSH server daemon...
Sep 15 06:09:03 server.belajar.local sshd[230]: Server listening on 0.0.0.0 port 22
.
Sep 15 06:09:03 server.belajar.local sshd[230]: Server listening on :: port 22.
Sep 15 06:09:03 server.belajar.local systemd[1]: Started OpenSSH server daemon.
```

Terlihat *service sshd* telah aktif.

10. Mengatur agar *user* “**root**” dapat digunakan login ke **SSH Server** dari **LXC Container CentOS 9 Stream** dengan menambahkan *directive* `PermitRootLogin yes` pada *file* `/etc/ssh/sshd_config` menggunakan *editor* **nano**.

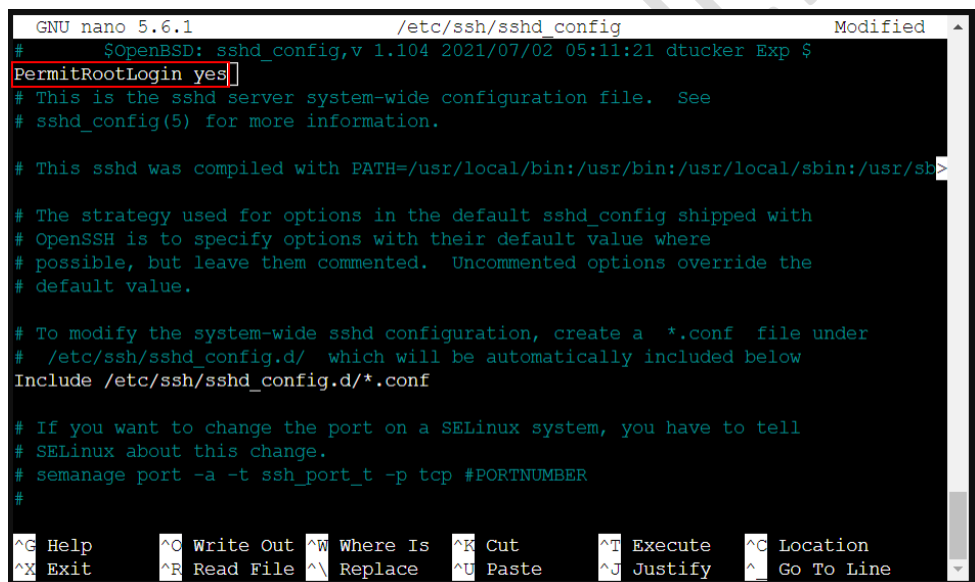
a) Menginstalasi paket aplikasi **nano**.

```
[root@server ~]# dnf -y install nano
```

b) Membuka *file* `/etc/ssh/sshd_config` menggunakan *editor* **nano**.

```
[root@server ~]# nano /etc/ssh/sshd_config
```

Menambahkan *directive* `PermitRootLogin yes` pada *file* `/etc/ssh/sshd_config`.



```
GNU nano 5.6.1 /etc/ssh/sshd_config Modified
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $
PermitRootLogin yes
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sb>

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#

^C Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^G Location
^X Exit      ^R Read File ^\ Replace   ^U Paste    ^J Justify  ^_ Go To Line
```

Menyimpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**.

Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

c) Melakukan **restart service sshd** agar perubahan konfigurasi berdampak.

```
[root@server ~]# systemctl restart sshd
```

d) Memverifikasi status dari *service sshd*.

```
[root@server ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset:
   enabled)
   Active: active (running) since Fri 2023-09-15 06:35:14 UTC; 3s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 252 (sshd)
      Tasks: 1 (limit: 18543)
     Memory: 1.3M
        CPU: 11ms
    CGroup: /system.slice/sshd.service
            └─252 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 15 06:35:14 server.belajar.local systemd[1]: Starting OpenSSH server daemon...
Sep 15 06:35:14 server.belajar.local sshd[252]: Server listening on 0.0.0.0 port 22
.
Sep 15 06:35:14 server.belajar.local sshd[252]: Server listening on :: port 22.
Sep 15 06:35:14 server.belajar.local systemd[1]: Started OpenSSH server daemon.
```

11. Menampilkan informasi pengalamatan IP pada **interface eth0** dari *container CentOS 9 Stream*.

```
[root@server ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
   link/ether 12:cf:9d:06:5e:9c brd ff:ff:ff:ff:ff:ff link-netnsid 0
   inet 192.168.169.4/24 brd 192.168.169.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::10cf:9dff:fe06:5e9c/64 scope link
       valid_lft forever preferred_lft forever
```

12. Memverifikasi koneksi dari **container CentOS 9 Stream** ke **Server Proxmox**.

```
[root@server ~]# ping 192.168.169.1 -c 4
PING 192.168.169.1 (192.168.169.1) 56(84) bytes of data.
64 bytes from 192.168.169.1: icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from 192.168.169.1: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 192.168.169.1: icmp_seq=3 ttl=64 time=0.202 ms
64 bytes from 192.168.169.1: icmp_seq=4 ttl=64 time=0.076 ms

--- 192.168.169.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.035/0.093/0.202/0.064 ms
```

Terlihat koneksi berhasil dilakukan.

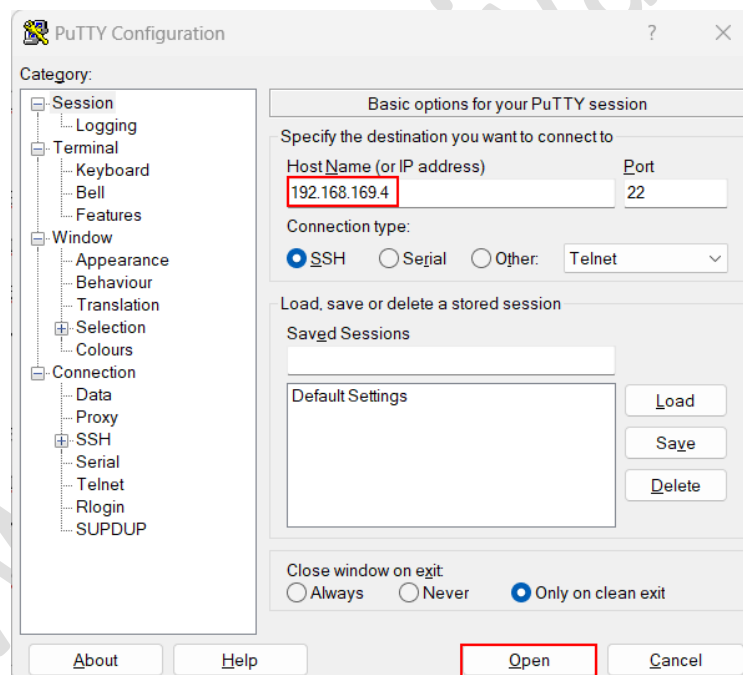
13. Memverifikasi koneksi dari **container CentOS 9 Stream** ke **Client Windows 10**.

```
[root@server ~]# ping 192.168.169.2 -c 4
PING 192.168.169.2 (192.168.169.2) 56(84) bytes of data.
64 bytes from 192.168.169.2: icmp_seq=1 ttl=128 time=0.794 ms
64 bytes from 192.168.169.2: icmp_seq=2 ttl=128 time=0.567 ms
64 bytes from 192.168.169.2: icmp_seq=3 ttl=128 time=0.420 ms
64 bytes from 192.168.169.2: icmp_seq=4 ttl=128 time=0.728 ms

--- 192.168.169.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3034ms
rtt min/avg/max/mdev = 0.420/0.627/0.794/0.145 ms
```

Terlihat koneksi berhasil dilakukan.

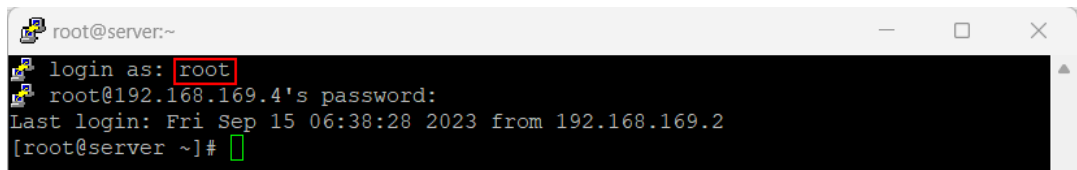
- Lakukan percobaan mengakses ke *container CentOS 9 Stream* melalui aplikasi **SSH Client Putty** yang terdapat pada **Client Windows 10**. Jalankan aplikasi *Putty* maka akan tampil kotak dialog *Putty Configuration*. Pada isian **Host Name (or IP Address)**, masukkan alamat IP dari *container CentOS 9 Stream* yaitu **192.168.169.4**, seperti terlihat pada gambar berikut:



Klik tombol **Open**.

Tampil kotak dialog **Putty Security Alert** yang menampilkan pesan peringatan terkait potensi pelanggaran keamanan, klik tombol **Accept** untuk melanjutkan.

Selanjutnya tampil kotak dialog *Putty* yang meminta pengguna untuk melakukan proses otentikasi login ke *container CentOS 9 Stream*, seperti terlihat pada gambar berikut:

A terminal window titled 'root@server:~' showing an SSH login session. The prompt 'login as:' is followed by 'root' (highlighted with a red box). The next prompt is 'root@192.168.169.4's password:'. Below that, it shows 'Last login: Fri Sep 15 06:38:28 2023 from 192.168.169.2' and the shell prompt '[root@server ~]#'.

```
root@server:~  
login as: root  
root@192.168.169.4's password:  
Last login: Fri Sep 15 06:38:28 2023 from 192.168.169.2  
[root@server ~]#
```

Pada inputan **login as:**, masukkan “**root**” dan tekan tombol **Enter**. Selanjutnya tampil inputan **password:**, masukkan “**12345678**” dan tekan tombol **Enter**. Apabila proses otentikasi berhasil dilakukan maka akan tampil *shell prompt* #.

Keluar dari *SSH* menggunakan perintah **exit**, seperti terlihat pada gambar berikut:

```
[root@server ~]# exit
```

15. Untuk mematikan **container CentOS 9 Stream**, pada **Console** dari *web interface* administrasi **Proxmox** eksekusi perintah “**poweroff**”, seperti terlihat pada gambar berikut:

```
[root@server ~]# poweroff
```

Tunggu hingga proses *shutdown* selesai dilakukan.

16. Untuk keluar dari *web interface* konfigurasi **Proxmox** maka klik pada *dropdown* menu **root@pam** di sebelah pojok kanan atas dan pilih **Logout**.

BAB VII

MANAJEMEN USER DAN PERMISSION PADA PROXMOX VE 8.0

Menurut wiki dari *Proxmox*, PVE mendukung berbagai sumber metode otentikasi pengguna meliputi *Linux PAM*, *Proxmox VE Authentication Server*, *LDAP* dan *Microsoft Active Directory*. Akses *granular* dapat didefinisikan dengan menggunakan manajemen *user* dan ijin akses (*permission*) berbasis *role* untuk keseluruhan objek seperti *Virtual Machine (VM)*, *storage*, *node* dan lain-lain.

User memerlukan ijin akses yang sesuai untuk dapat melakukan aktivitas seperti melihat, mengubah atau menghapus konfigurasi dari VM. PVE menggunakan sistem manajemen berbasis *role* dan *path*. *Role* merupakan daftar dari hak akses. Terdapat berbagai *role* yang telah didefinisikan oleh PVE, antara lain:

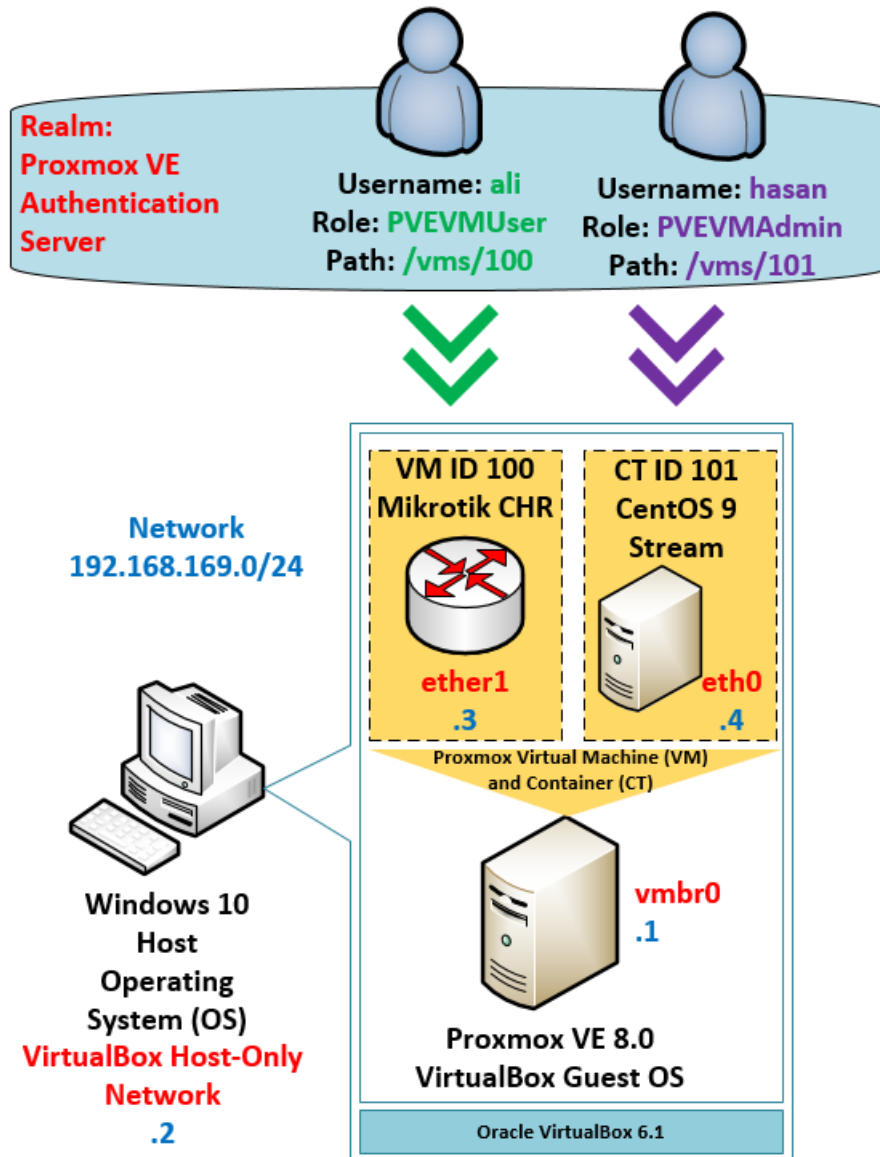
1. **Administrator**: memiliki keseluruhan hak akses.
2. **NoAccess**: tidak memiliki hak akses (digunakan untuk melarang akses)
3. **PVEAdmin**: dapat melakukan banyak hal, tetapi kehilangan hak untuk mengubah pengaturan sistem (*Sys.PowerMgmt*, *Sys.Modify*, *Realm.Allocate*).
4. **PVEAuditor**: hanya akses baca (*read only access*).
5. **PVEDatastoreAdmin**: membuat dan mengalokasikan ruang *backup* dan *templates*.
6. **PVEDatastoreUser**: mengalokasikan ruang backup dan melihat (*view*) media penyimpanan (*storage*).
7. **PVEPoolAdmin**: mengalokasikan *pools*.
8. **PVESysAdmin**: *User ACLs*, *audit*, *system console* dan *system logs*.
9. **PVETemplateUser**: melihat (*view*) dan melakukan *clone templates*.
10. **PVEUserAdmin**: administrasi pengguna (*user*).
11. **PVEVMAdmin**: sepenuhnya mengelola VM.
12. **PVEVMUser**: *view*, *backup*, *config CDRROM*, *VM console*, *VM power management*.

Ijin akses diterapkan terhadap objek meliputi *VM*, *storage* atau *pool* dari sumber daya. PVE menggunakan *path* untuk mengamati objek tersebut, sebagai contoh:

1. `/nodes/{node}`: akses ke mesin server *Proxmox VE*.
2. `/vms`: mencakup seluruh VM.
3. `/vms/{vmid}`: akses ke VM tertentu.

4. /storage/{storeid}: akses ke media penyimpanan (*storages*).
5. /pool/{poolname} : akses ke VM yang menjadi bagian dari *pool*.
6. /access/groups: administrasi grup.
7. /access/realms/{realmid}: akses administratif ke *realms*.

Rancangan *user* yang akan dibuat pada PVE, seperti terlihat pada gambar berikut:



Terdapat 2 (dua) *user* atau pengguna dengan metode otentikasi (**realm**) **Proxmox VE Authentication Server** yang akan dibuat yaitu **ali** dan **hasan**. *User ali* memiliki *role PVEVMUser* pada objek **VM ID 100 Mikrotik CHR**. Sedangkan *user hasan* memiliki *role PVEVMAdmin* pada objek **CT ID 101 CentOS 9 Stream**.

Adapun langkah-langkah pembuatan *user* dan pengaturan *permission* serta uji coba berdasarkan rancangan *user* tersebut adalah sebagai berikut:

1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**, seperti terlihat pada gambar berikut:

Proxmox VE Login

User name:

Password:

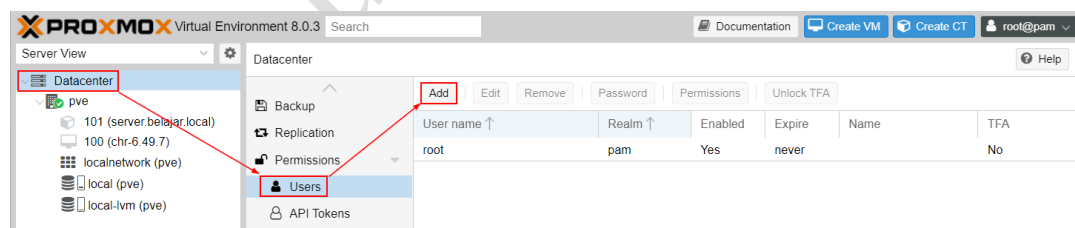
Realm: Linux PAM standard authentication

Language: English - English

Save User name:

Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

3. Membuat *user* baru yaitu **ali** dan **hasan** dengan mengakses menu **Data Center** pada panel sebelah kiri dan pada panel sebelah kanan memilih submenu **Users** dibawah menu **Permissions** serta memilih tombol **Add**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Add: User**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Penjelasan dari setiap parameter yang dikonfigurasi adalah sebagai berikut:

- User name:**, digunakan untuk mengatur nama login dari pengguna yaitu “ali”.
- Realm:**, digunakan untuk menentukan metode otentikasi yang digunakan yaitu **Proxmox VE authentication server**.
- Password:** dan **Confirm Password:** digunakan untuk mengatur sandi login dari user “ali” untuk *container* yaitu “12345678”.
- First Name:**, digunakan untuk mengatur nama depan dari akun pengguna yang dibuat yaitu “ali”.
- Comment:**, digunakan untuk mengatur deskripsi dari akun pengguna yang dibuat yaitu “ali”.

Klik tombol **Add** untuk memproses pembuatan *user* “ali” maka hasilnya akan terlihat seperti pada gambar berikut:

User name ↑	Realm ↑	Enabled	Expire	Name	TFA
ali	pve	Yes	never	ali	No
root	pam	Yes	never		No

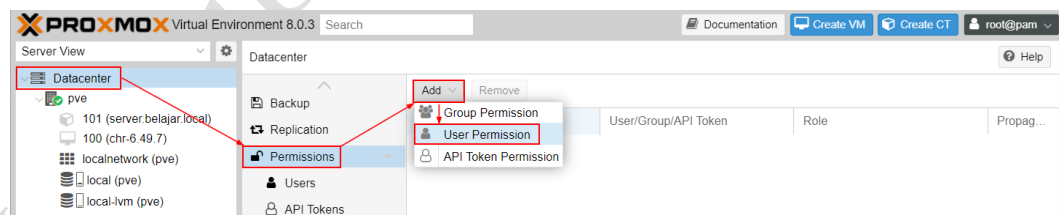
Selanjutnya dengan cara sama, lakukan pula pembuatan user “hasan”.

Klik tombol **Add** maka akan tampil kotak dialog **Add: User**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Klik tombol **Add** untuk memproses pembuatan *user* “**hasan**” maka hasilnya akan terlihat seperti pada gambar berikut:

User name ↑	Realm ↑	Enabled	Expire	Name	TFA
ali	pve	Yes	never	ali	No
hasan	pve	Yes	never	hasan	No
root	pam	Yes	never		No

- Menambahkan ijin akses agar *user* “**ali**” dapat mengakses objek **VM ID 100 Mikrotik CHR** dengan mengakses menu **Data Center** pada panel sebelah kiri dan pada panel sebelah kanan pilih **Permissions** serta klik tombol **Add > User Permission**, seperti terlihat pada gambar berikut:



Pada kotak dialog **Add: User Permission** yang tampil terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Add: User Permission

Path: /vms/100

User: ali@pve

Role: PVEVMUser

Propagate:

Help Add

Penjelasan dari setiap parameter yang dikonfigurasi adalah sebagai berikut:

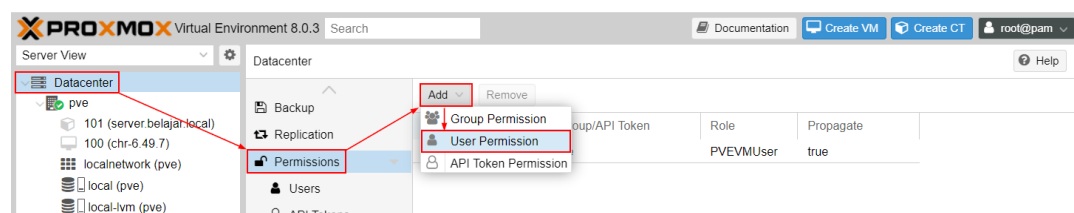
- Path:**, digunakan untuk mengatur ijin akses ke objek VM dengan ID tertentu yaitu “/vms/100”.
- User:**, digunakan untuk menentukan user yang diberikan akses terhadap *path* “/vms/100” yaitu “ali@pve”.
- Role:** digunakan untuk mengatur *role* yang dialokasikan untuk user “ali@pve” yaitu “PVEVMUser”. *Role* tersebut memiliki ijin akses untuk melakukan aktivitas *view*, *backup*, *config CDROM*, *VM console*, dan *VM power management*.

Setelah penekanan tombol **Add** maka akan terlihat hasil dari pembuatan ijin akses untuk user “ali@pve”, seperti terlihat pada gambar berikut:

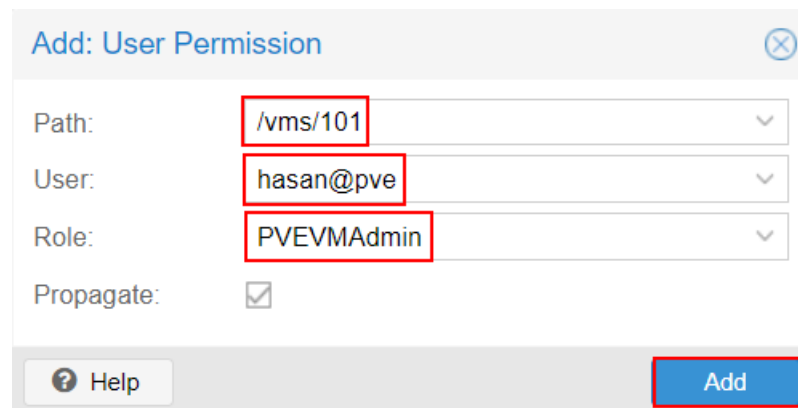
Datacenter

Path ↑	User/Group/API Token	Role	Propagate
/vms/100	ali@pve	PVEVMUser	true

- Menambahkan ijin akses agar user “hasan” dapat mengakses objek **CT ID 101 CentOS 9 Stream** dengan mengakses menu **Data Center** pada panel sebelah kiri dan pada panel sebelah kanan pilih **Permissions** serta klik tombol **Add > User Permission**, seperti terlihat pada gambar berikut:



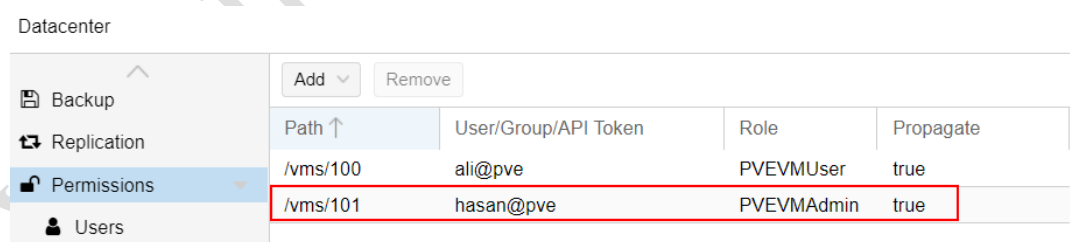
Pada kotak dialog **Add: User Permission** yang tampil terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:



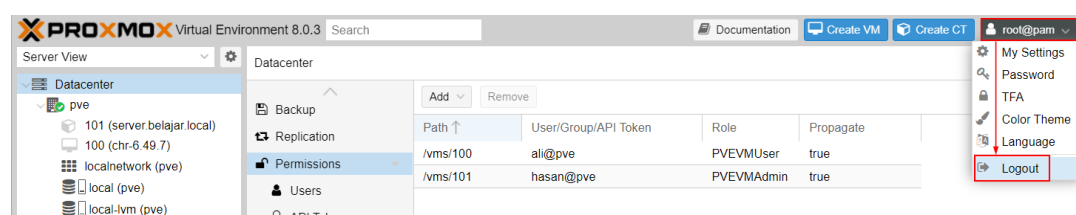
Penjelasan dari setiap parameter yang dikonfigurasi adalah sebagai berikut:

- a) **Path:**, digunakan untuk mengatur ijin akses ke objek LXC dengan ID tertentu yaitu “/vms/101”.
- b) **User:**, digunakan untuk menentukan user yang diberikan akses terhadap *path* “/vms/101” yaitu “hasan@pve”.
- c) **Role:** digunakan untuk mengatur *role* yang dialokasikan untuk user “hasan@pve” yaitu “PVEVMAdmin”. *Role* tersebut memiliki ijin akses untuk melakukan aktivitas manajemen pada *LXC ID 101* secara penuh.

Setelah penekanan tombol **Add** maka akan terlihat hasil dari pembuatan ijin akses untuk user “hasan@pve”, seperti terlihat pada gambar berikut:

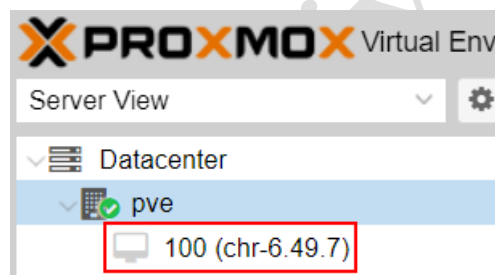


6. Keluar dari *Web GUI Proxmox* dengan memilih *dropdown* menu **root@pam** dan pilih **Logout**.



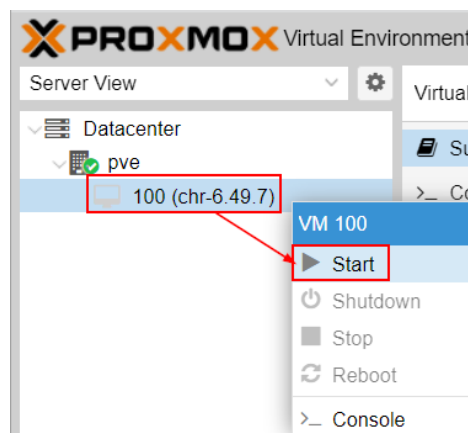
7. Lakukan login kembali ke *PVE WebGUI* menggunakan user “ali” dengan *password* “123456” dan *realm* “**Proxmox VE Authentication Server**”, seperti terlihat pada gambar berikut:

Klik tombol **Login**. Apabila login sukses maka akan tampil *Dashboard PVE*. Pada panel sebelah kiri pilih **Datacenter** > **PVE** maka akan terlihat **VM ID 100** seperti gambar berikut:



Hal ini sesuai dengan ijin akses yang diberikan pada user “ali” yaitu hanya dapat mengakses objek **VM ID 100 Mikrotik CHR**.

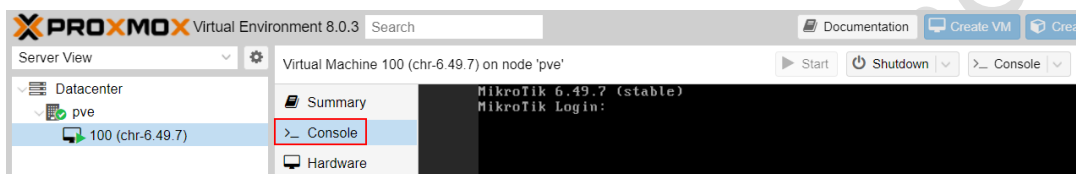
Selanjutnya jalankan *VM Mikrotik CHR* dengan cara klik kanan pada “**100 (chr-6.49.7)**” di bawah *node* “pve” dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:



Pada bagian **Tasks** dari **Log Panel** memperlihatkan pesan status **OK** untuk **VM 100** – **Start** yang menyatakan bahwa VM tersebut berhasil dijalankan, seperti terlihat pada gambar berikut:

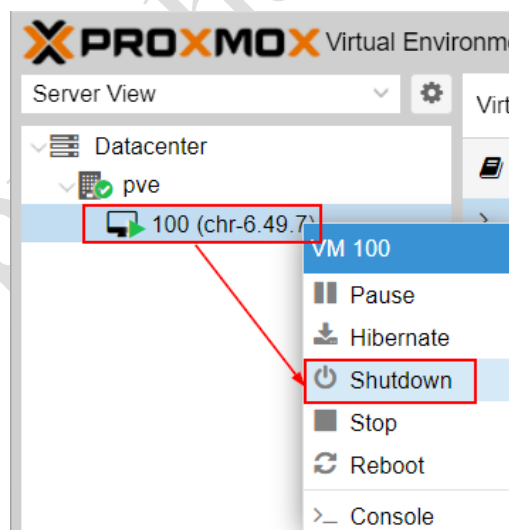
Start Time ↓	End Time	Node	User name	Description	Status
Sep 15 15:49:07	Sep 15 15:49:10	pve	ali@pve	VM 100 - Start	OK

Selanjutnya untuk mengakses tampilan dari **VM 100**, pilih **Console** pada panel sebelah kanan dari **VM 100 (chr-6.49.7)**, seperti terlihat pada gambar berikut:



Tampil inputan **Mikrotik Login** untuk proses otentikasi sebelum pengguna dapat mengakses **Command Line Interface (CLI)** dari *Mikrotik*.

Selanjutnya lakukan **shutdown VM 100** dengan cara klik kanan pada “**100 (chr-6.49.7)**” di bawah *node* “**pve**” dari menu **Datacenter** dan pilih **Shutdown**, seperti terlihat pada gambar berikut:



Tampil kotak dialog konfirmasi proses *shutdown*, tekan tombol **Yes**.

Tunggu hingga proses *shutdown* selesai dilakukan dan **Logout** sebagai user “**ali**” dari *PVE WebGUI*.

- Lakukan login kembali ke *PVE WebGUI* menggunakan *user* “**hasan**” dengan *password* “**123456**” dan *realm* “**Proxmox VE Authentication Server**”, seperti terlihat pada gambar berikut:

Proxmox VE Login

User name:

Password:

Realm:

Language:

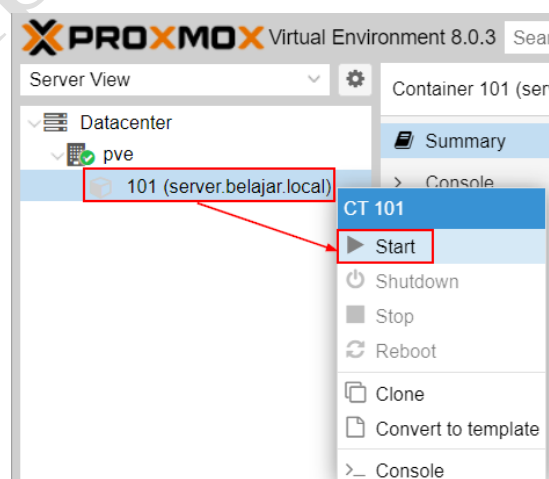
Save User name:

Klik tombol **Login**. Apabila login sukses maka akan tampil *Dashboard PVE*. Pada panel sebelah kiri pilih **Datacenter** > **PVE** maka akan terlihat **CT ID 101** seperti gambar berikut:



Hal ini sesuai dengan ijin akses yang diberikan pada user “**hasan**” yaitu hanya dapat mengakses objek **CT ID 101 CentOS 9 Stream**.

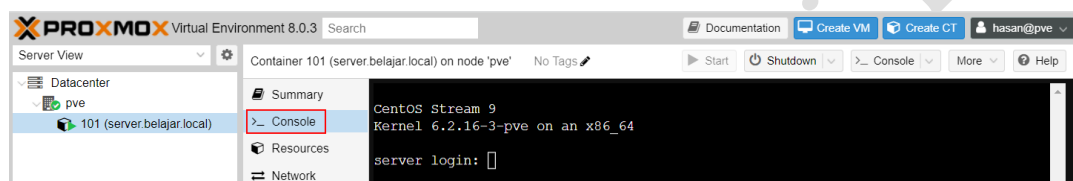
Selanjutnya jalankan *CT ID 101* dengan cara klik kanan pada “**101 (server.belajar.local)**” di bawah *node* “**pve**” dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:



Pada bagian **Tasks** dari **Log Panel** memperlihatkan pesan status **OK** untuk **CT 101** – **Start** yang menyatakan bahwa CT tersebut berhasil dijalankan, seperti terlihat pada gambar berikut:

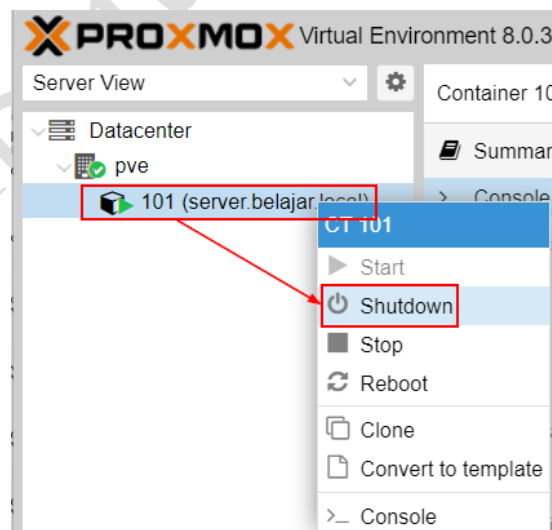
Start Time ↓	End Time	Node	User name	Description	Status
Sep 15 16:04:49	Sep 15 16:04:54	pve	hasan@pve	CT 101 - Start	OK

Selanjutnya untuk mengakses tampilan dari **CT 101**, pilih **Console** pada panel sebelah kanan dari **CT 101 (server.belajar.local)**, seperti terlihat pada gambar berikut:



Tampil inputan **server Login** untuk proses otentikasi sebelum pengguna dapat mengakses **Command Line Interface (CLI)** dari *CentOS 9 Stream*.

Selanjutnya lakukan **shutdown CT 101** dengan cara klik kanan pada “**101 (server.belajar.local)**” di bawah *node “pve”* dari menu **Datacenter** dan pilih **Shutdown**, seperti terlihat pada gambar berikut:



Tampil kotak dialog konfirmasi proses *shutdown*, tekan tombol **Yes**.

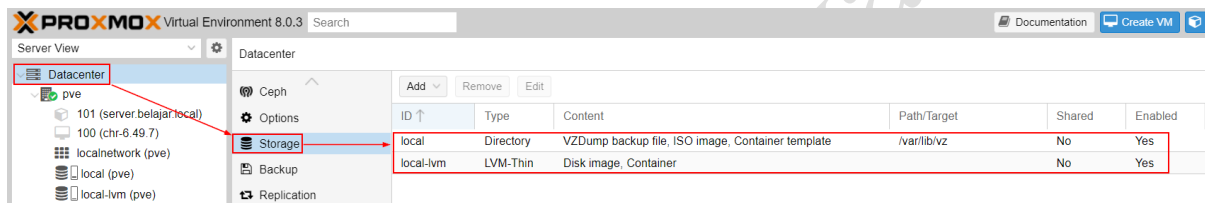
Tunggu hingga proses *shutdown* selesai dilakukan dan **Logout** sebagai user “**hasan**” dari *PVE WebGUI*.

BAB VIII

BACKUP DAN RESTORE PADA PROXMOX VE 8.0

A. BACKUP

Backup merupakan proses untuk membuat salinan dari data dan konfigurasi VM/CT untuk digunakan ketika data atau konfigurasi tersebut hilang atau rusak. *PVE backup* bertipe **full backup** yang didalamnya memuat konfigurasi VM/CT dan data. *Backup storage* perlu didefinisikan terlebih dahulu sebelum *backup* dapat dijalankan. Hal ini dapat diketahui dengan mengakses *PVE WebGUI* dan memilih **Datacenter** pada panel sebelah kiri dari halaman *Server View* serta memilih **Storage** pada panel sebelah kanan, seperti terlihat pada gambar berikut:



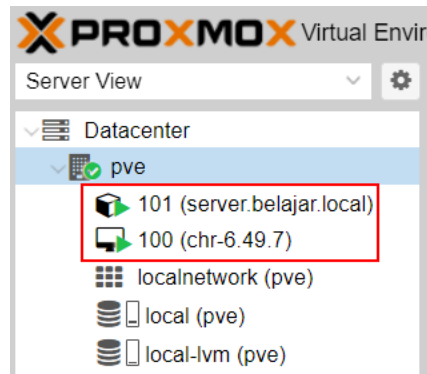
Terlihat secara *default*, storage “**local**” dapat digunakan untuk menyimpan *file backup*.

Adapun langkah-langkah untuk melakukan *backup VM* dan **LXC** pada PVE adalah sebagai berikut:

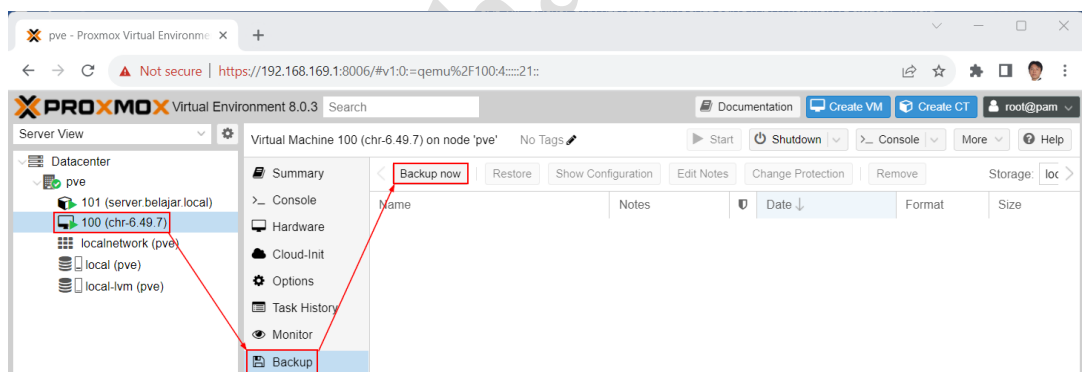
1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**. Selain itu pastikan pilihan “**Realm**” adalah **Linux PAM standard authentication**, seperti terlihat pada gambar berikut:

Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

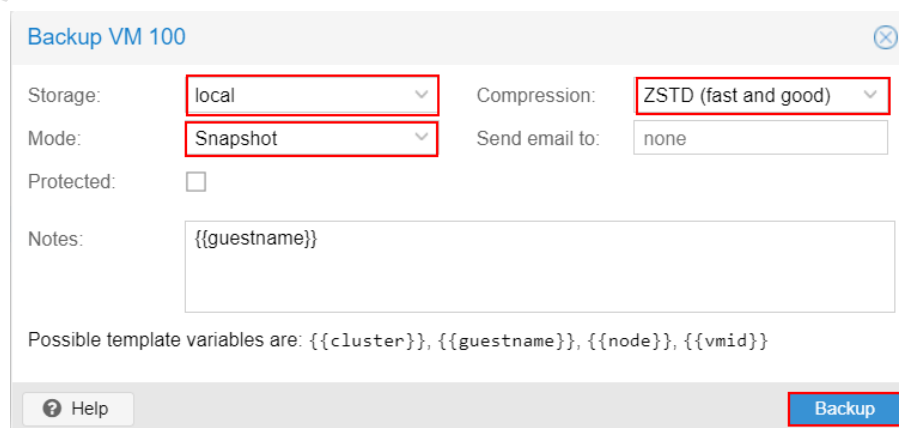
3. Pastikan **VM ID 100 (chr-6.49.7)** dan **CT ID 101 (server.belajar.local)** dalam keadaan aktif atau *running*. Apabila belum maka lakukan pengaktifan terlebih dahulu sehingga hasilnya akhirnya terlihat seperti gambar berikut:



4. Proses *backup* VM diawali dengan melakukan navigasi ke menu **Datacenter > PVE** pada panel sebelah kiri dari halaman *Server view* dan memilih **VM ID 100 (chr-6.49.7)**. Selanjutnya pilih **Backup** → **Backup Now** pada panel sebelah kanan, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Backup VM 100**. Terdapat beberapa parameter yang harus dikonfigurasi, seperti terlihat pada gambar berikut:



Penjelasan parameter:

- a) *Storage*: digunakan untuk menentukan lokasi penyimpanan file *backup* yaitu **local**.
- b) *Mode*:, untuk menentukan *mode backup* yang akan digunakan.

Menurut *wiki* dari *Proxmox* terdapat 3 (tiga) pilihan *mode backup* untuk VM yaitu **stop**, **suspend** dan **snapshot**.

- **Stop mode**

Mode ini memberikan konsistensi tertinggi dari *backup* namun memberikan *downtime* singkat pada operasi VM. Hal ini bekerja dengan mengeksekusi *shutdown* pada VM, dan kemudian menjalankan proses **Qemu** secara *background* untuk membackup data VM. Setelah backup dimulai, VM beralih ke mode operasi penuh jika sebelumnya telah berjalan. Konsistensi dijamin dengan menggunakan fitur *live backup*.

- **Suspend mode**

Mode ini disediakan untuk kompatibilitas dan menanggihkan VM sebelum memanggil *snapshot mode*. Disarankan untuk menggunakan mode *snapshot* karena ketika VM ditanggihkan maka akan mengakibatkan *downtime* yang lama dan tidak selalu meningkatkan konsistensi data.

- **Snapshot mode**

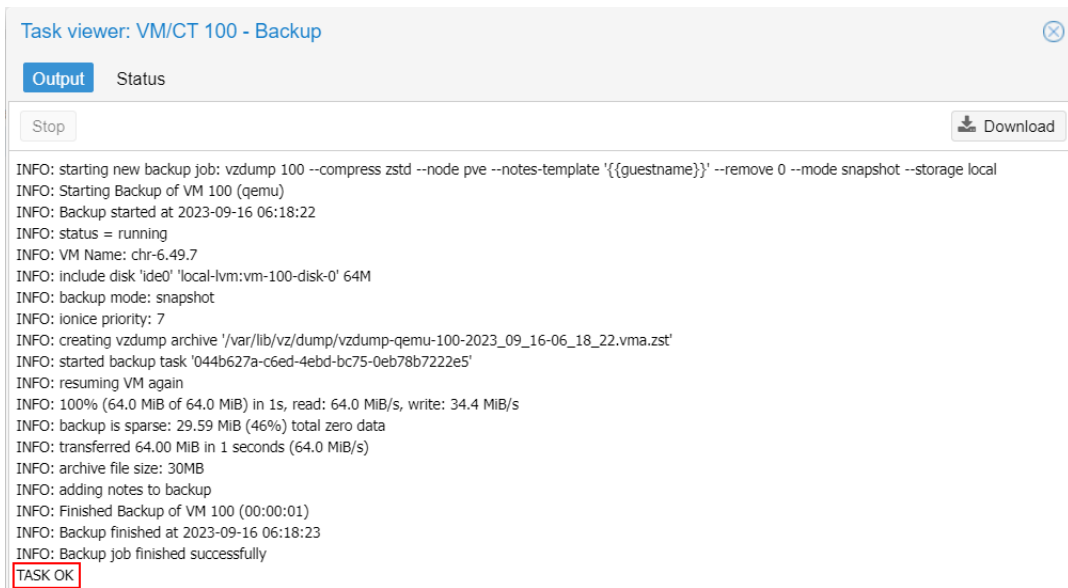
Mode ini menyediakan operasi *downtime* **terendah** dan bekerja dengan melakukan *PVE live backup* dimana data block disalin ketika VM sedang berjalan.

Secara *default* telah terpilih yaitu **snapshot**.

- c) *Compression*:, digunakan untuk menentukan jenis kompresi dari *file backup*. Terdapat 4 (empat) pilihan yaitu **none** (tanpa kompresi), **LZO (fast)** dan **GZIP (good)** serta **ZSTD (fast and good)**. Secara *default* telah terpilih **ZSTD (fast and good)**.

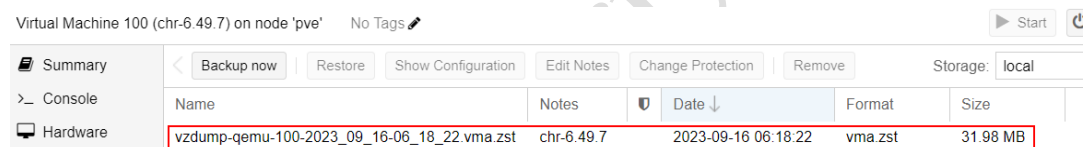
Klik tombol **Backup** untuk memulai *backup*.

Tampil kotak dialog **Task viewer: Backup** yang menampilkan proses backup, seperti terlihat pada gambar berikut:

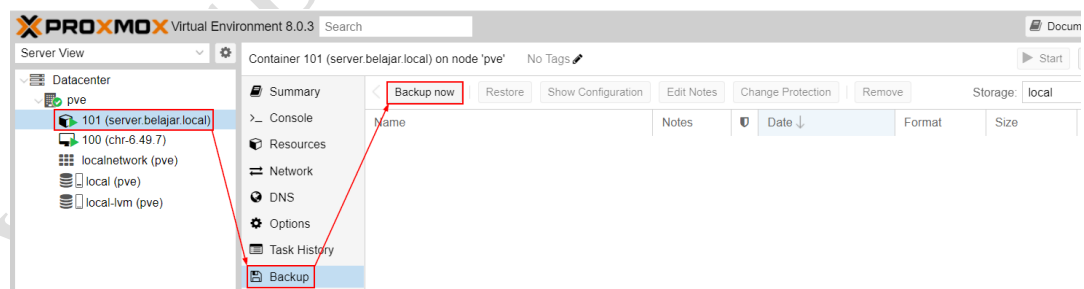


Tunggu hingga proses *backup* selesai dilakukan yang ditandai dengan pesan **TASK OK**. Tutup kotak dialog **Task viewer: Backup**.

Hasil dari *backup*, seperti terlihat pada gambar berikut:



- Proses *backup* CT diawali dengan melakukan navigasi ke menu **Datacenter > PVE** pada panel sebelah kiri dari halaman *Server view* dan memilih **CT ID 101 (server.belajar.local)**. Selanjutnya pilih **Backup → Backup Now** pada panel sebelah kanan, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Backup CT 101**. Terdapat beberapa parameter yang harus dikonfigurasi, seperti terlihat pada gambar berikut:

Backup CT 101

Storage: local Compression: ZSTD (fast and good)

Mode: Snapshot Send email to: none

Protected:

Notes: {{guestname}}

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

Help Backup

Penjelasan parameter:

- Storage*: digunakan untuk menentukan lokasi penyimpanan file *backup* yaitu **local**.
- Mode*:, untuk menentukan *mode backup* yang akan digunakan.

Menurut *wiki* dari *Proxmox* terdapat 3 (tiga) pilihan *mode backup* untuk CT yaitu **stop**, **suspend** dan **snapshot**.

- **Stop mode**

Container akan dihentikan (*stop*) selama proses *backup* sehingga memiliki *downtime* yang sangat lama.

- **Suspend mode**

Menggunakan *rsync* untuk menyalinkan data dari *container* ke lokasi sementara. Selanjutnya *container* akan ditangguhkan (*suspended*) dan salinan *rsync* kedua mengubah file. Setelah itu *container* akan dijalankan kembali sehingga memiliki *downtime* yang minimal tetapi membutuhkan tambahan kapasitas penyimpanan untuk menampung salinan dari *container*.

- **Snapshot mode**

Mode ini menggunakan fasilitas *snapshotting* dari penyimpanan yang mendasarinya. Pertama, *container* akan ditangguhkan untuk memastikan konsistensi pada data. *Snapshot* sementara dari *volume container* akan dibuat dan konten *snapshot* akan diarsipkan dalam file **tar**. Terakhir, *snapshot* sementara akan dihapus lagi.

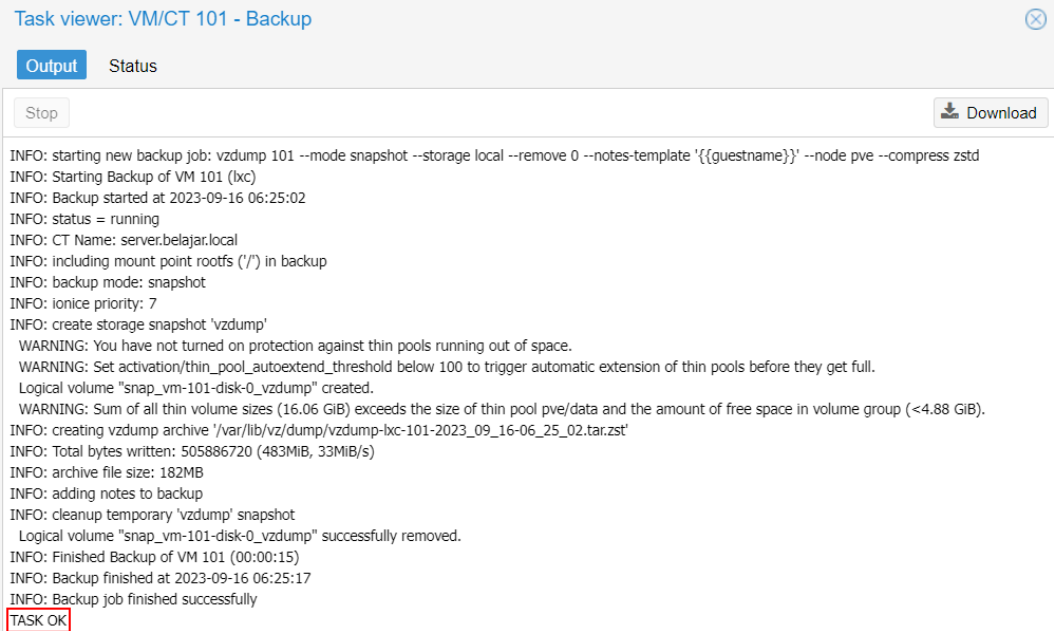
Secara *default* telah terpilih yaitu **snapshot**.

- Compression*:, digunakan untuk menentukan jenis kompresi dari *file backup*. Terdapat 4 (empat) pilihan yaitu **none** (tanpa kompresi), **LZO (fast)** dan

GZIP (good) serta **ZSTD (fast and good)**. Secara *default* telah terpilih **ZSTD (fast and good)**.

Klik tombol **Backup** untuk memulai *backup*.

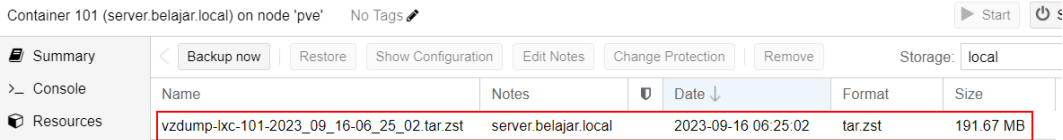
Tampil kotak dialog **Task viewer: Backup** yang menampilkan proses backup, seperti terlihat pada gambar berikut:



```
Task viewer: VM/CT 101 - Backup
Output Status
Stop Download
INFO: starting new backup job: vzdump 101 --mode snapshot --storage local --remove 0 --notes-template '{{(guestname)}}' --node pve --compress zstd
INFO: Starting Backup of VM 101 (lxc)
INFO: Backup started at 2023-09-16 06:25:02
INFO: status = running
INFO: CT Name: server.belajar.local
INFO: including mount point rootfs (/) in backup
INFO: backup mode: snapshot
INFO: ionice priority: 7
INFO: create storage snapshot 'vzdump'
WARNING: You have not turned on protection against thin pools running out of space.
WARNING: Set activation/thin_pool_autoextend_threshold below 100 to trigger automatic extension of thin pools before they get full.
Logical volume "snap_vm-101-disk-0_vzdump" created.
WARNING: Sum of all thin volume sizes (16.06 GiB) exceeds the size of thin pool pve/data and the amount of free space in volume group (<4.88 GiB).
INFO: creating vzdump archive '/var/lib/vz/dump/vzdump-lxc-101-2023_09_16-06_25_02.tar.zst'
INFO: Total bytes written: 505886720 (483MiB, 33MiB/s)
INFO: archive file size: 182MB
INFO: adding notes to backup
INFO: cleanup temporary 'vzdump' snapshot
Logical volume "snap_vm-101-disk-0_vzdump" successfully removed.
INFO: Finished Backup of VM 101 (00:00:15)
INFO: Backup finished at 2023-09-16 06:25:17
INFO: Backup job finished successfully
TASK OK
```

Tunggu hingga proses *backup* selesai dilakukan yang ditandai dengan pesan **TASK OK**. Tutup kotak dialog **Task viewer: Backup**.

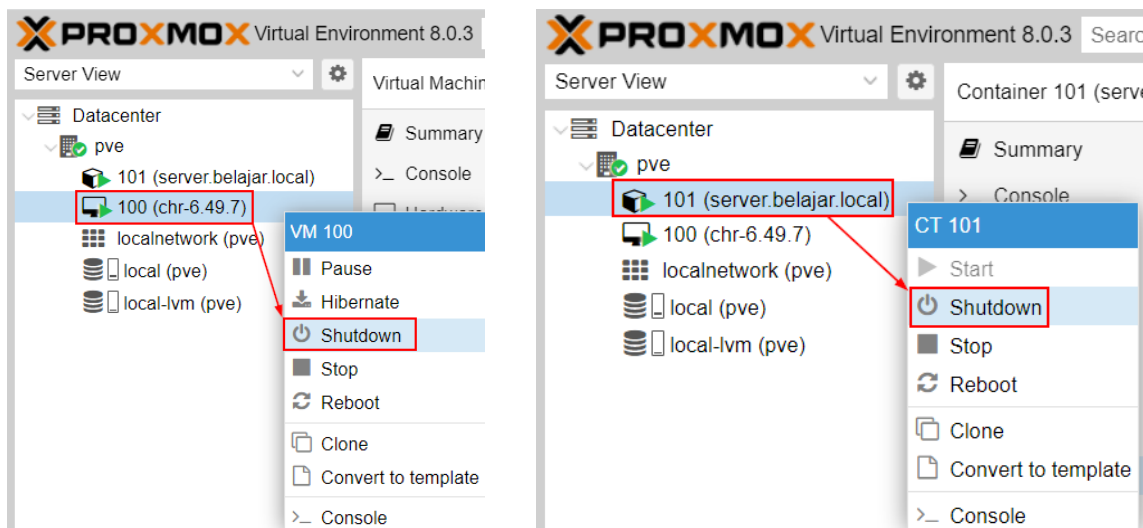
Hasil dari *backup*, seperti terlihat pada gambar berikut:



Name	Notes	Date	Format	Size
vzdump-lxc-101-2023_09_16-06_25_02.tar.zst	server.belajar.local	2023-09-16 06:25:02	tar.zst	191.67 MB

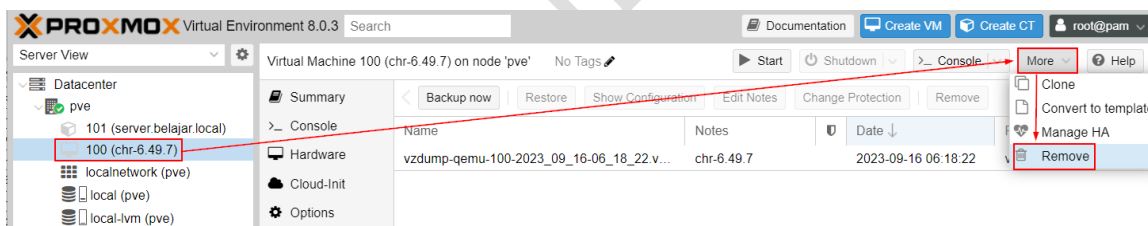
B. RESTORE

Sebelum mencontohkan operasi *restore* dari *file backup* maka terlebih dahulu akan dilakukan *shutdown* pada **VM ID 100 (chr-6.49.7)** dan **CT ID 101 (server.belajar.local)**. Proses *shutdown* dilakukan dengan cara klik kanan pada **VM ID 100** dan **CT ID 101** dan memilih **Shutdown** pada panel sebelah kiri dari *Server View PVE*, seperti terlihat pada gambar berikut:

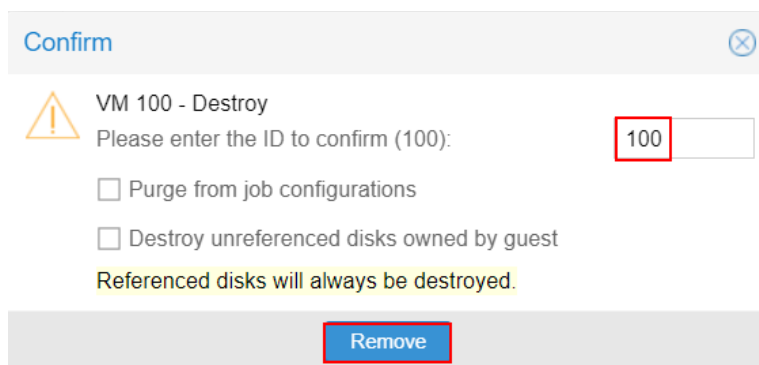


Tampil kotak dialog **Confirm** dari VM/CT yang di *shutdown* dan tekan tombol **Yes**. Tunggu hingga proses *shutdown* selesai dilakukan.

Selanjutnya akan dilakukan penghapusan VM 100 (chr-6.49.7) dan CT ID 101 (server.belajar.local). Proses penghapusan dilakukan dengan cara memilih VM 100 (chr-6.49.7) pada panel sebelah kiri dari *Server View PVE* dan pada panel sebelah kanan memilih tombol **More > Remove**, seperti terlihat pada gambar berikut:

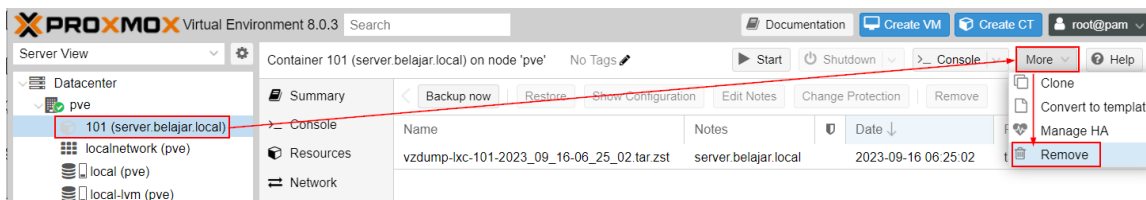


Tampil kotak dialog konfirmasi VM 100 –**Destroy**. Pada inputan parameter “*Please enter the ID to confirm (100):*”, masukkan **100** dan tekan tombol **Remove**, seperti terlihat pada gambar berikut:

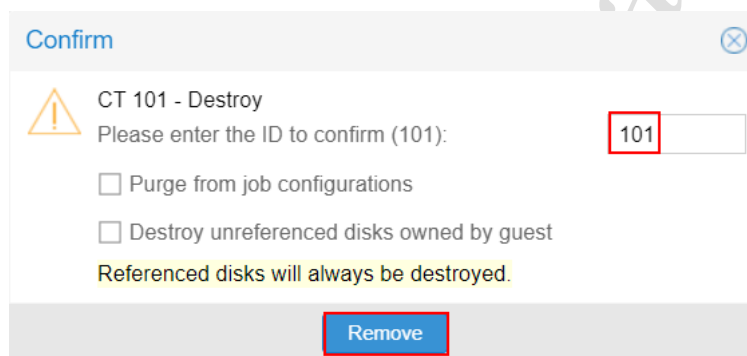


Tunggu hingga proses penghapusan VM selesai dilakukan.

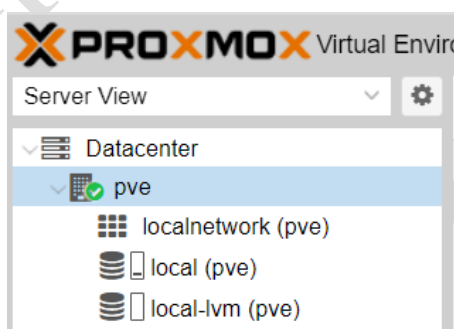
Dengan cara yang sama maka lakukan penghapusan **CT ID 101 (server.belajar.local)**. Proses penghapusan dilakukan dengan cara memilih **CT ID 101 (server.belajar.local)** pada panel sebelah kiri dari *Server View PVE* dan pada panel sebelah kanan memilih tombol **More > Remove**, seperti terlihat pada gambar berikut:



Tampil kotak dialog konfirmasi **CT 101 –Destroy**. Pada inputan parameter “*Please enter the ID to confirm (101):*”, masukkan **101** dan tekan tombol **Remove**, seperti terlihat pada gambar berikut:

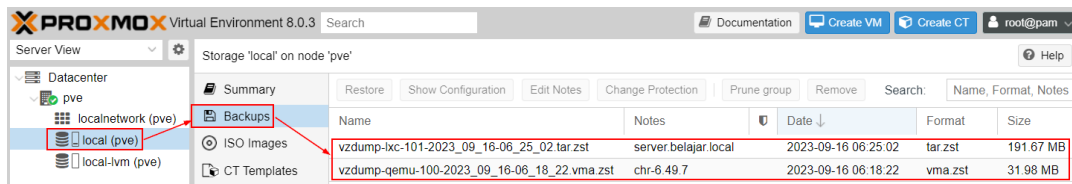


Tunggu hingga proses penghapusan CT selesai dilakukan. Hasil akhir ketika seluruh VM dan CT telah dihapus, seperti terlihat pada gambar berikut:



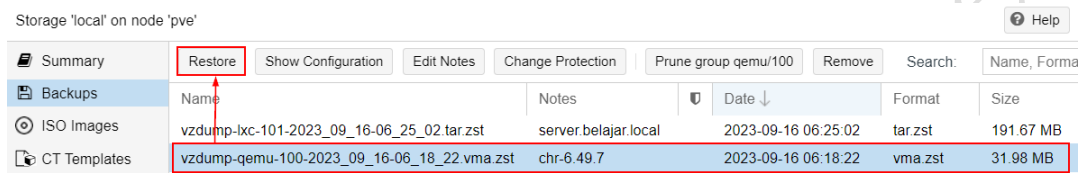
Adapun langkah-langkah untuk melakukan *restore* VM dan CT adalah sebagai berikut:

1. Mengakses konten dari *storage local* yang menampung *file backup* dengan cara memilih **Datacenter > PVE > local (pve)** pada panel sebelah kiri dari *Server View PVE*, seperti terlihat pada gambar berikut:

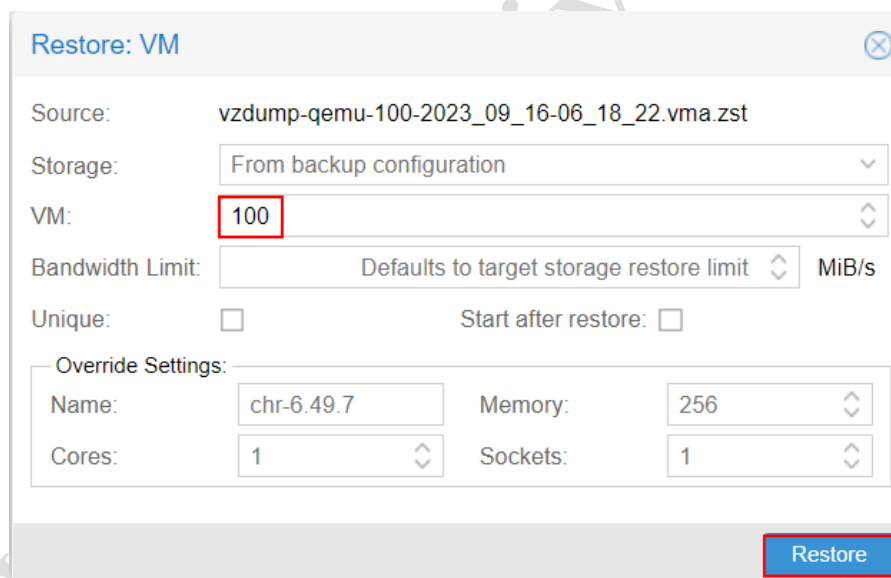


Terlihat 2 (dua) file backup dari **VM ID 100** dan **CT ID 101**.

- Pilih file “**vzdump-qemu-100-2023_09_16-06_18_22.vma.zst**” dan klik tombol **Restore** untuk melakukan pemulihan atau pengembalian **VM ID 100**, seperti terlihat pada gambar berikut:

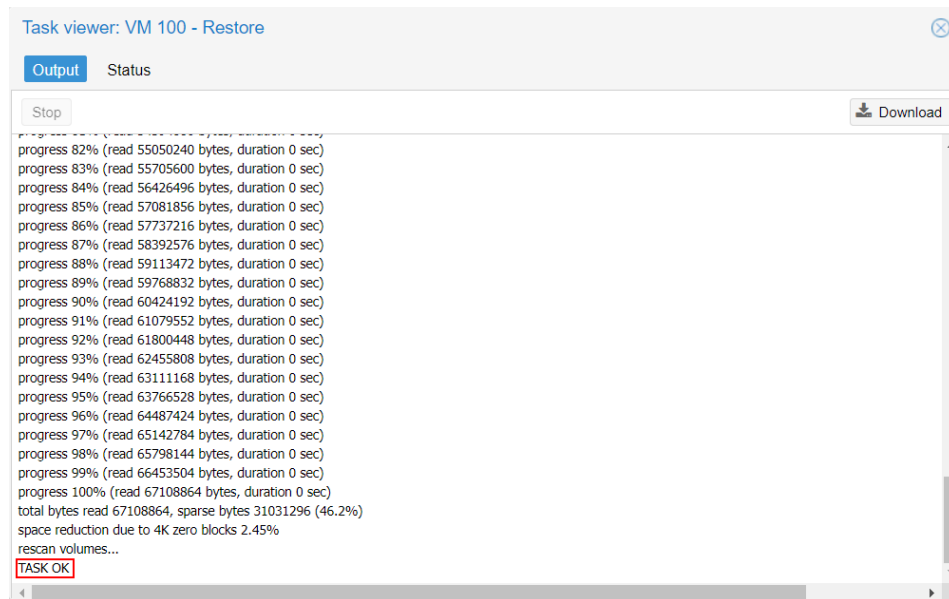


Tampil kotak dialog **Restore: VM**. Terdapat beberapa parameter yang dapat disesuaikan, seperti terlihat pada gambar berikut:



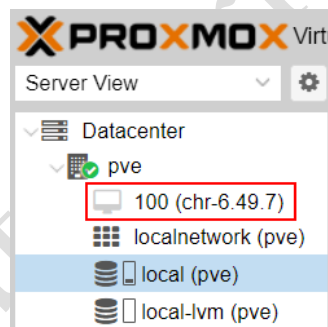
Sebagai contoh parameter **VM ID**: untuk menentukan *Virtual Machine Identifier (ID)* yang akan digunakan oleh VM yang dipulihkan yaitu **100**.

Klik tombol **Restore** maka akan tampil kotak dialog **Task viewer: VM 100 – Restore** yang memperlihatkan proses pemulihan VM, seperti terlihat pada gambar berikut:



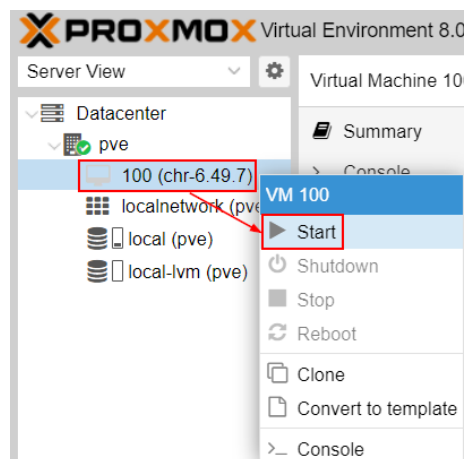
Tunggu hingga proses pemulihan VM selesai dilakukan yang ditandai dengan pesan **TASK OK**. Tutup kotak dialog **Task viewer: VM 100 – Restore**.

Hasil akhir dari proses *restore* VM ID 100, seperti terlihat pada gambar berikut:

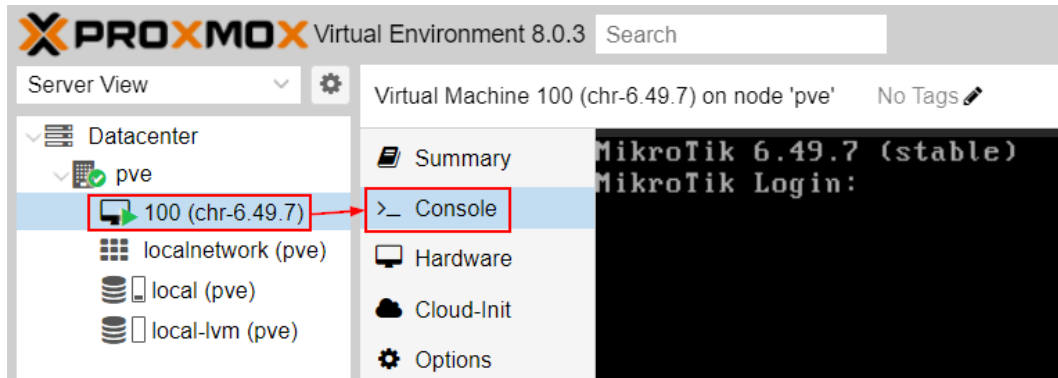


Terlihat VM ID 100 telah berhasil dipulihkan.

Selanjutnya VM tersebut dapat diujicoba untuk dijalankan dengan melakukan klik kanan pada **“100 (chr-6.49.7)”** dibawah *node* **“pve”** dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:

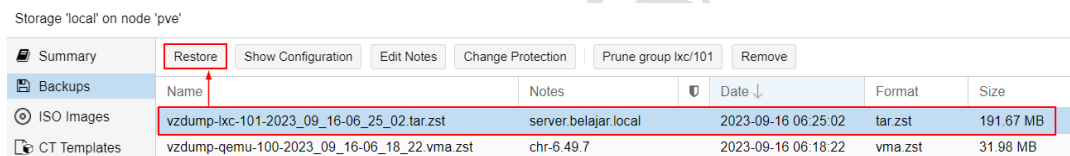


Lakukan pengaksesan *Console* dari VM tersebut, seperti terlihat pada gambar berikut:

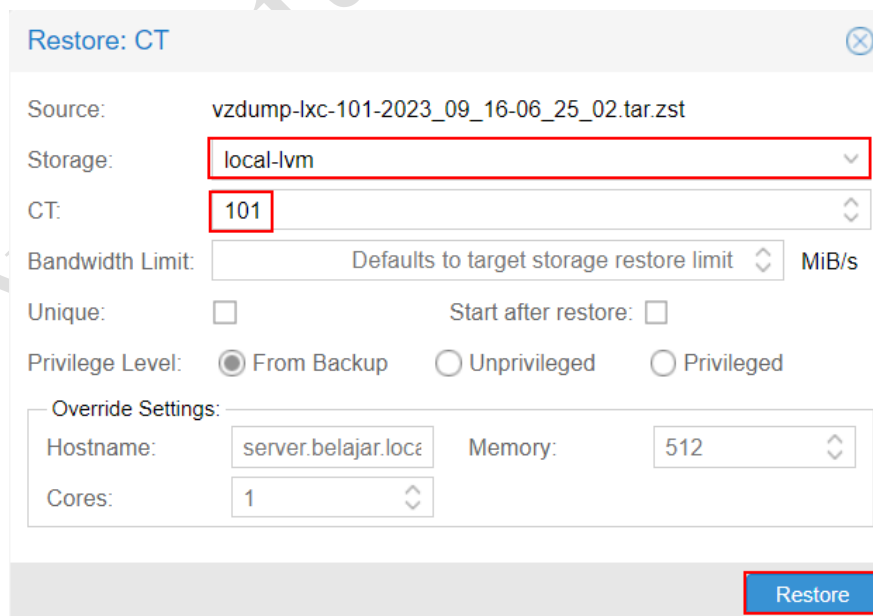


Terlihat *Console* dari VM ID 100 telah berhasil diakses.

3. Dengan cara yang sama, lakukan proses *restore* untuk CT. Pilih file “**vzdump-lxc-101-2023_09_16-06_25_02.tar.zst**” dan klik tombol **Restore** untuk melakukan pemulihan atau pengembalian CT ID 101, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Restore: CT**. Terdapat beberapa parameter yang memerlukan pengaturan, seperti terlihat pada gambar berikut:

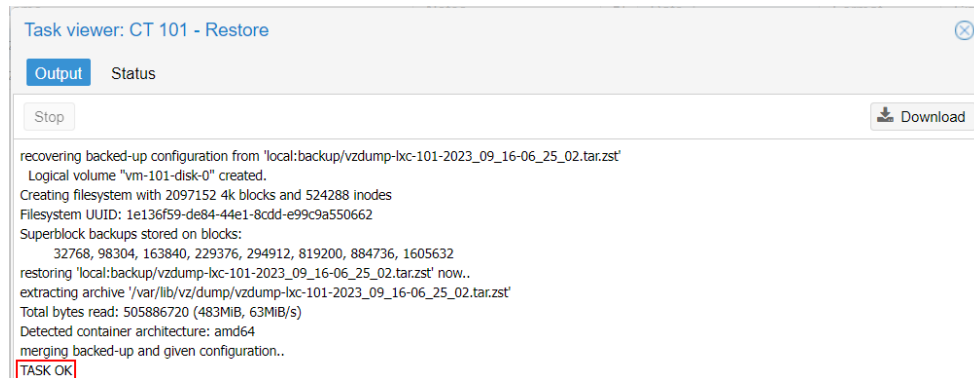


Penjelasan parameter:

- a) *Storage*:, menentukan media penyimpanan yang akan digunakan sebagai tujuan pemulihan CT yaitu **local-lvm**.

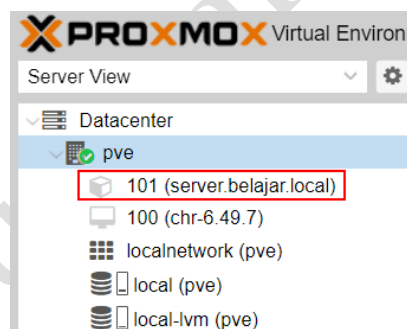
- b) *CT ID*:, menentukan *Container Identifier (ID)* yang akan digunakan oleh CT yang dipulihkan yaitu **101**.

Klik tombol **Restore** maka akan tampil kotak dialog **Task viewer: CT 101 – Restore** yang memperlihatkan proses pemulihan CT, seperti terlihat pada gambar berikut:

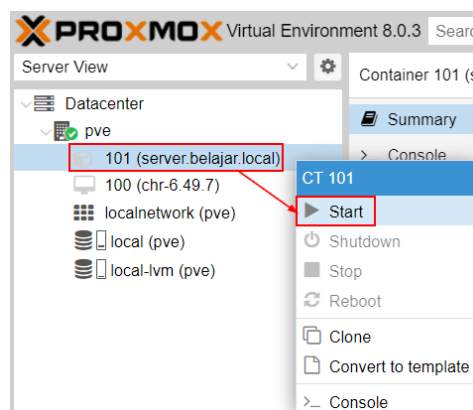


Tunggu hingga proses pemulihan CT selesai dilakukan yang ditandai dengan pesan **TASK OK**. Tutup kotak dialog **Task viewer: CT 101 – Restore**.

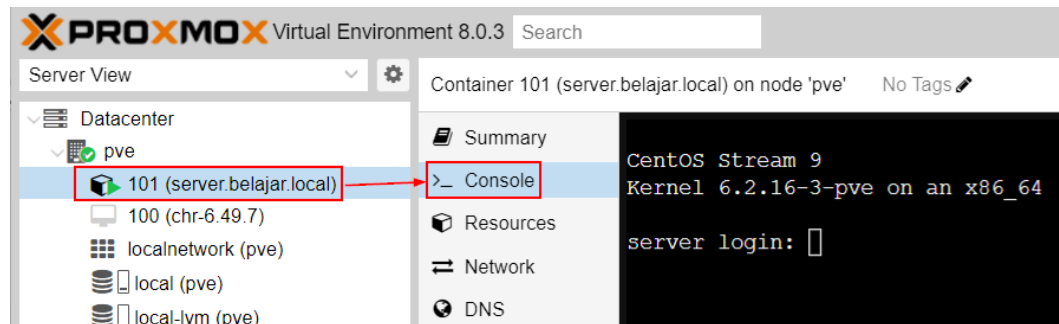
Hasil akhir dari proses *restore* **CT ID 101**, seperti terlihat pada gambar berikut:



Terlihat **CT ID 101** telah berhasil dipulihkan. Selanjutnya CT tersebut dapat diujicoba untuk dijalankan dengan melakukan klik kanan pada “**101 (server.belajar.local)**” dibawah *node* “**pve**” dari menu **Datacenter** dan pilih **Start** seperti terlihat pada gambar berikut:



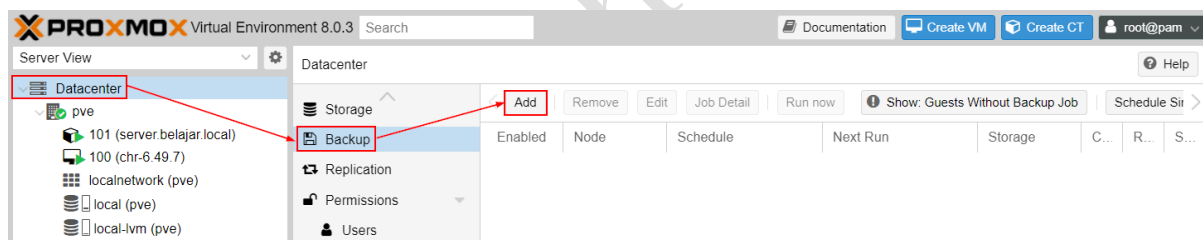
Lakukan pengaksesan *Console* dari CT tersebut, seperti terlihat pada gambar berikut:



Terlihat *Console* dari CT ID 101 telah berhasil diakses.

C. SCHEDULED BACKUP

Aktivitas backup dapat dieksekusi secara terjadwal sehingga eksekusi dilakukan berdasarkan waktu yang ditentukan dan untuk *node* atau sistem *guest* (VM/CT) terpilih. Backup terjadwal dapat dilakukan dengan memilih menu **Datacenter** pada panel sebelah kiri dari *Server View PVE* dan pada panel sebelah kanan memilih menu **Backup** serta klik tombol **Add**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Create: Backup Job**, seperti terlihat pada gambar berikut:

Create: Backup Job

General Retention Note Template

Node: -- All -- Send email to:

Storage: local Email: Notify always

Schedule: */30 Compression: ZSTD (fast and good)

Selection mode: Include selected VMs Mode: Snapshot

Enable:

Job Comment:

<input checked="" type="checkbox"/>	ID ↑	Node	Status	Name	Type
<input checked="" type="checkbox"/>	100	pve	running	chr-6.49.7	Virtual Machine
<input checked="" type="checkbox"/>	101	pve	running	server.belajar.local	LXC Container

Help Advanced Create

Terdapat beberapa parameter yang memerlukan pengaturan pada kotak dialog tersebut, antara lain:

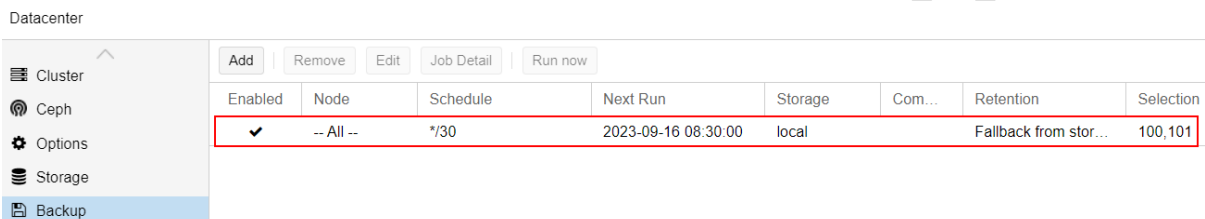
- Storage*, digunakan untuk menentukan lokasi penyimpanan file *backup* yaitu **local**.
- Schedule*, digunakan untuk menentukan setiap kapan *backup* tersebut akan dieksekusi. Terdapat 11 (sebelas) pilihan jadwal meliputi *Every 30 minutes*, *Every two hours*, *Every day 21.00*, *Every daya 02:30, 22:30*, *Monday to Friday 00:00*, *Monday to Friday: hourly*, *Monday to Friday, 07:00 to 18:45: Every 15 minutes*, *Sunday 01:00*, *Every first day of the Month 00:00*, *First Saturday each month 15:00*, *First day of the year 00:00*. Sebagai contoh dipilih **Every 30 minutes** agar *backup* dieksekusi setiap 30 menit sehingga isian pada parameter ini bernilai ***/30**.
- Selection mode*, digunakan untuk menentukan mode seleksi dari VM/CT yang akan dibackup yaitu **Include selected VMs** (memasukkan VM terpilih untuk dibackup). Terdapat pilihan lainnya yaitu *All* dan *Exclude selected VMs*.
- Compression*, digunakan untuk menentukan jenis kompresi dari *file backup*. Terdapat 4 (empat) pilihan yaitu **none** (tanpa kompresi), **LZO (fast)** dan **GZIP**

- (good) sert **ZSTD (fast and good)**. Secara *default* telah terpilih **ZSTD (fast and good)**.
- e) *Mode*, untuk menentukan *mode backup* yang akan digunakan. Terdapat 3 (tiga) pilihan yaitu **stop**, **suspend** dan **snapshot**. Secara *default* telah terpilih yaitu **snapshot**.
- f) Seleksi atau tandai VM atau CT yang akan dibackup yaitu **VM ID 100** dan **CT ID 101**.

Klik tombol **Create** untuk membuat backup terjadwal.

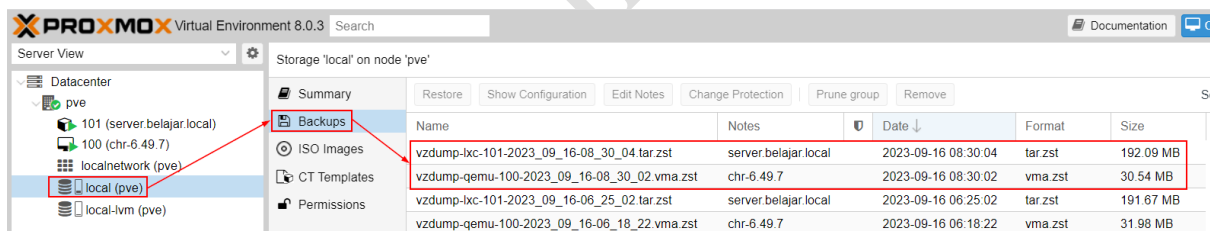
Hasil dari pembuatan backup terjadwal, terlihat seperti pada gambar berikut:

Datacenter



Enabled	Node	Schedule	Next Run	Storage	Com...	Retention	Selection
✓	-- All --	* /30	2023-09-16 08:30:00	local		Fallback from stor...	100,101

Sedangkan hasil dari backup terjadwal yang telah tereksekusi pada jadwal yang telah ditentukan untuk **VM ID 100** dan **CT ID 101**, seperti terlihat pada gambar berikut:



Name	Notes	Date ↓	Format	Size
vzdump-lxc-101-2023_09_16-08_30_04.tar.zst	server.belajar.local	2023-09-16 08:30:04	tar.zst	192.09 MB
vzdump-qemu-100-2023_09_16-08_30_02.vma.zst	chr-6.49.7	2023-09-16 08:30:02	vma.zst	30.54 MB
vzdump-lxc-101-2023_09_16-06_25_02.tar.zst	server.belajar.local	2023-09-16 06:25:02	tar.zst	191.67 MB
vzdump-qemu-100-2023_09_16-06_18_22.vma.zst	chr-6.49.7	2023-09-16 06:18:22	vma.zst	31.98 MB

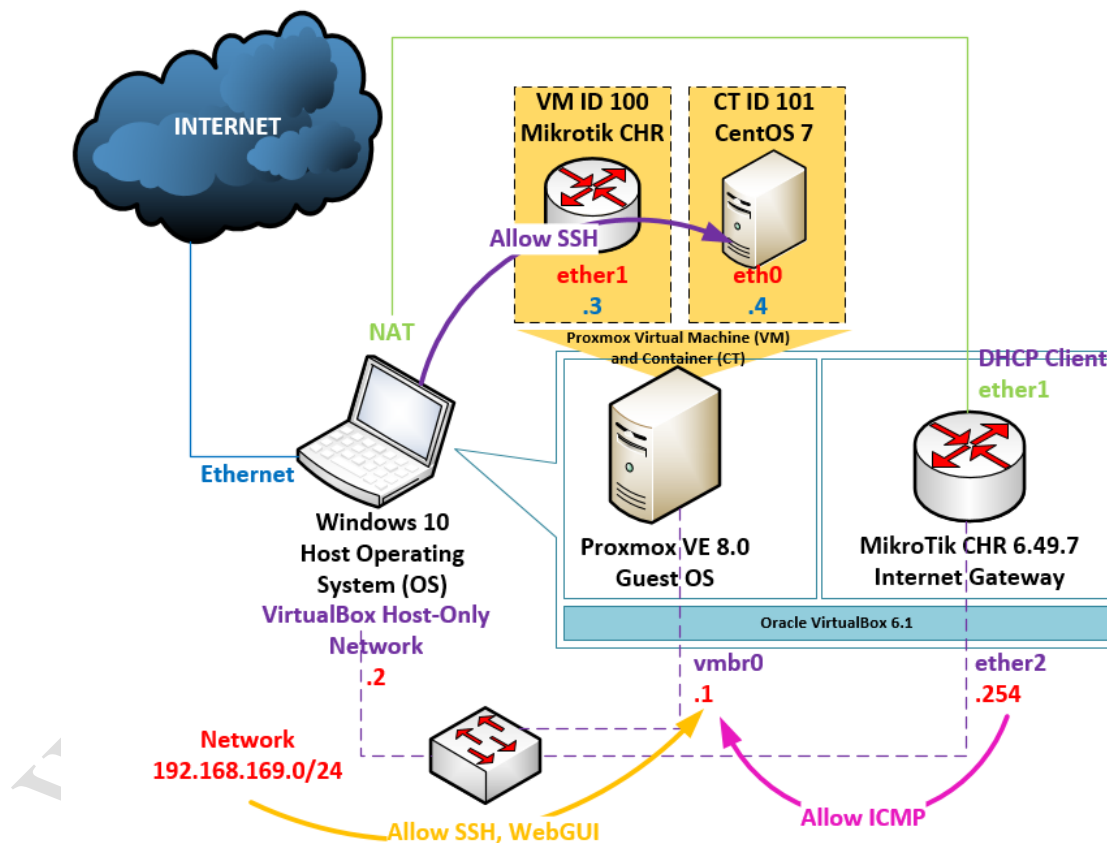
Terlihat *file backup* berhasil terbuat.

BAB IX

MANAJEMEN FIREWALL PADA PROXMOX VE 8.0

Menurut *wiki* dari *Proxmox*, PVE menyediakan fitur *firewall* yang mendukung IPv4 dan IPv6 dan dapat digunakan untuk membuat aturan (*rule*) sehingga melindungi semua host di dalam *cluster* atau *virtual machine* dan *container*. *Firewall* pada PVE mengelompokkan jaringan ke dalam *zone* logikal yaitu **host** (memfilter trafik dari atau ke *node cluster*) dan **VM** (memfilter trafik dari atau ke VM tertentu).

Rancangan jaringan yang digunakan untuk mengujicoba penerapan *firewall* pada PVE, seperti terlihat pada gambar berikut:



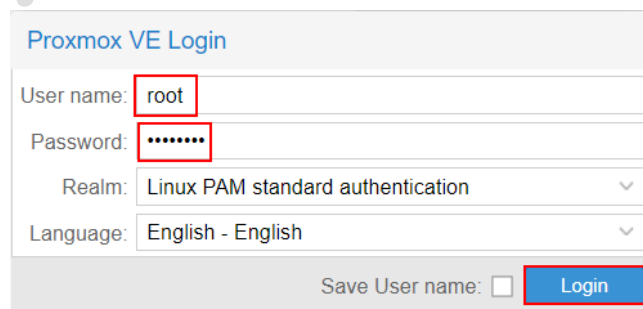
Secara default fitur *firewall* dari PVE pada lingkup *cluster* masih tidak aktif sehingga memerlukan pengaktifan agar aturan (*rule*) yang dibuat dapat berfungsi. **Apabila fitur firewall ini diaktifkan maka trafik dari seluruh host akan ditolak secara default dengan pengecualian pada WebGUI (8006) dan SSH (22) yang diakses dari jaringan lokal.**

Namun berdasarkan pengalaman penulis terkadang koneksi ke *WebGUI* dan *SSH* dari host-host pada jaringan lokal tidak dapat dilakukan. Untuk itu akan dibuat aturan (*rule*) yang akan diterapkan pada *PVE firewall* dengan lingkup *cluster* secara eksplisit yaitu hanya mengizinkan akses **SSH (tcp/22)** dan **WebGUI (tcp/8006)** dari alamat *network* **192.168.169.0/24** ke PVE. Sedangkan aturan (*rule*) yang akan diterapkan pada *PVE firewall* dengan lingkup *node* yaitu hanya mengizinkan akses **ICMP** dari *Mikrotik CHR Internet Gateway* dengan alamat IP **192.168.169.254** ke PVE. Terakhir aturan (*rule*) yang akan diterapkan pada *PVE firewall* dengan lingkup *container* yaitu hanya mengizinkan akses **SSH** dari **Windows 10** ke **Container CT ID 101**.

A. PENGAKTIFAN DAN KONFIGURASI FIREWALL RULE PADA LINGKUP CLUSTER

Adapun langkah-langkah pengaktifan *firewall* dan konfigurasi aturan (*rule*) *firewall* pada lingkup cluster adalah sebagai berikut:

1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**. Selain itu pastikan pilihan “**Realm**” adalah **Linux PAM standard authentication**, seperti terlihat pada gambar berikut:

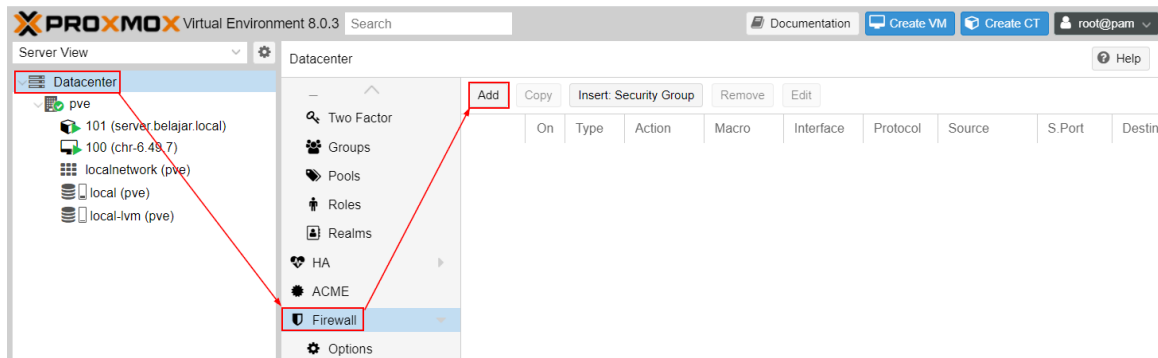


The image shows a 'Proxmox VE Login' dialog box. It has four input fields: 'User name' with 'root', 'Password' with masked characters, 'Realm' with 'Linux PAM standard authentication', and 'Language' with 'English - English'. There is a 'Save User name' checkbox and a 'Login' button at the bottom right.

Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

3. Membuat *firewall rule* untuk **mengizinkan akses SSH** dari **host-host pada jaringan lokal dengan alamat network 192.168.169.0/24** ke PVE pada lingkup

cluster dapat dilakukan dengan mengakses menu **Datacenter** pada panel sebelah kiri dari *Server View PVE* dan memilih menu **Firewall** pada panel sebelah kanan serta memilih tombol **Add**, seperti terlihat pada gambar berikut:



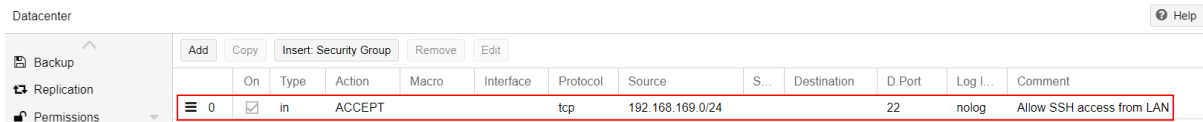
Tampil kotak dialog **Add: Rule**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Penjelasan parameter:

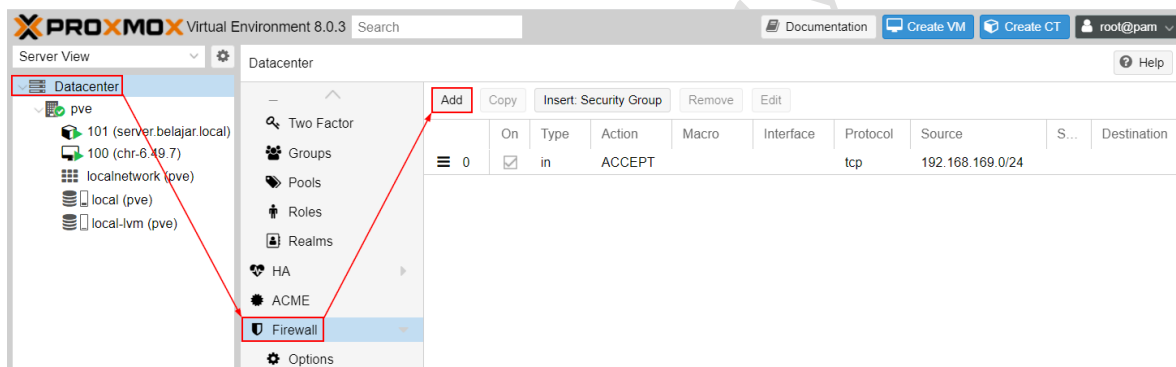
- Direction*., digunakan untuk menentukan arah pemfilteran trafik yaitu **IN** (paket yang masuk).
- Action*., digunakan untuk menentukan aksi atau tindakan yang diambil ketika terdapat trafik dengan nilai parameter yang sesuai dengan *rule* yaitu **ACCEPT** (diterima).
- Source*., digunakan untuk menentukan alamat IP atau *network* sumber yang diijinkan untuk mengakses layanan SSH yaitu **192.168.169.0/24**.
- Enable*., digunakan untuk mengaktifkan rule firewall. Pastikan tercentang (√).
- Protocol*., digunakan untuk menentukan metode transport yang digunakan oleh SSH yaitu **tcp**.

- f) *Dest. Port.*:, digunakan untuk menentukan nomor port tujuan yaitu **22** untuk layanan SSH.
- g) *Comment.*:, digunakan untuk menentukan deskripsi singkat terkait *rule firewall* yang dibuat yaitu **Allow SSH access from LAN**.

Klik tombol **Add** untuk memproses pembuatan *rule firewall*. Hasil dari penambahan *rule* tersebut, seperti terlihat pada gambar berikut:



4. Dengan cara yang sama lakukan pembuatan *firewall rule* untuk **mengijinkan akses WebGUI dari host-host pada jaringan lokal dengan alamat network 192.168.169.0/24 ke PVE pada lingkup cluster**. Pada panel sebelah kiri dari *Server View PVE* pilih menu **Datacenter** dan pada panel sebelah kanan pilih menu **Firewall** serta klik tombol **Add**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Add: Rule**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Add: Rule ✕

Direction:	<input type="text" value="in"/>	Enable:	<input checked="" type="checkbox"/>		
Action:	<input type="text" value="ACCEPT"/>	Macro:	<input type="text" value=""/>		
Interface:	<input type="text" value=""/>	Protocol:	<input type="text" value="tcp"/>		
Source:	<input type="text" value="192.168.169.0/24"/>	Source port:	<input type="text" value=""/>		
Destination:	<input type="text" value=""/>	Dest. port:	<input type="text" value="8006"/>		
Comment:	<input type="text" value="Allow WEBGUI access from LAN"/>				

Advanced Add

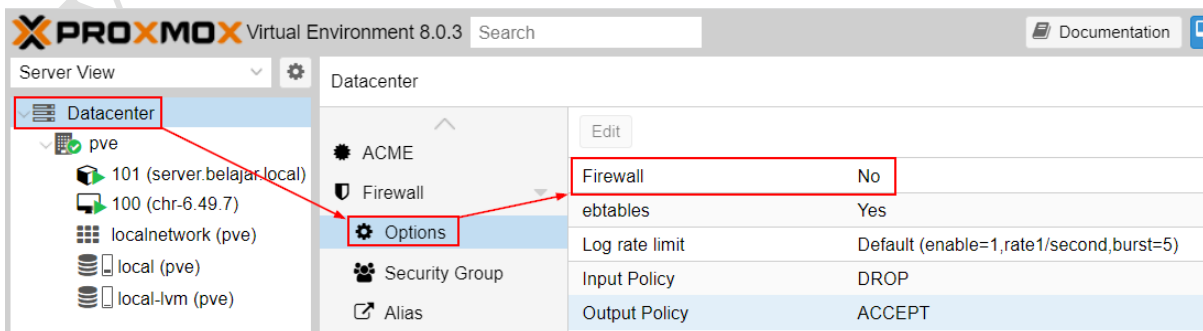
Penjelasan parameter:

- a) *Direction*., digunakan untuk menentukan arah pemfilteran trafik yaitu **IN** (paket yang masuk).
- b) *Action*., digunakan untuk menentukan aksi atau tindakan yang diambil ketika terdapat trafik dengan nilai parameter yang sesuai dengan *rule* yaitu **ACCEPT** (diterima).
- c) *Source*., digunakan untuk menentukan alamat IP atau network sumber yang diijinkan untuk mengakses layanan *WebGUI* yaitu **192.168.169.0/24**.
- d) *Enable*., digunakan untuk mengaktifkan rule firewall. Pastikan tercentang (✓).
- e) *Protocol*., digunakan untuk menentukan metode transport yang digunakan oleh *WebGUI* yaitu **tcp**.
- f) *Dest. Port*., digunakan untuk menentukan nomor port tujuan yaitu **8006** untuk layanan *WebGUI*.
- g) *Comment*., digunakan untuk menentukan deskripsi singkat terkait *rule firewall* yang dibuat yaitu **Allow WebGUI access from LAN**.

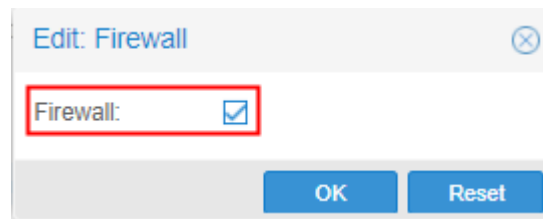
Klik tombol **Add** untuk memproses pembuatan *rule firewall*. Hasil dari penambahan *rule* tersebut, seperti terlihat pada gambar berikut:

	Add	Copy	Insert Security Group	Remove	Edit											
	On	Type	Action	Macro	Interface	Protocol	Source	S...	Destination	D.Port	Log I...	Comment				
0	<input checked="" type="checkbox"/>	in	ACCEPT			tcp	192.168.169.0/24			8006	nolog	Allow WEBGUI access from LAN				
1	<input checked="" type="checkbox"/>	in	ACCEPT			tcp	192.168.169.0/24			22	nolog	Allow SSH access from LAN				

5. Mengaktifkan fitur **PVE Firewall lingkup cluster** dengan mengakses menu **Datacenter** pada panel sebelah kiri dari *Server View PVE* dan memilih menu **Firewall > Options** pada panel sebelah kanan. Pada panel detail dari submenu **Options** terdapat parameter **Firewall** dengan nilai default **No** yang bermakna bahwa fitur firewall PVE saat ini dalam keadaan tidak aktif, seperti terlihat pada gambar berikut:



Klik dua kali pada parameter **Firewall** tersebut maka akan tampil kotak dialog **Edit: Firewall**. Tandai atau centang (✓) pada parameter *Firewall*, seperti terlihat pada gambar berikut:



Klik tombol **OK** untuk menyimpan perubahan.

Hasil dari pengaktifan fitur *PVE firewall* lingkup *cluster* terlihat seperti pada gambar berikut:

Datacenter

	Value
Firewall	Yes
eatables	Yes
Log rate limit	Default (enable=1,rate1/second,burst=5)
Input Policy	DROP
Output Policy	ACCEPT

Terlihat nilai parameter **Firewall** telah berubah dari **No** menjadi **Yes** yang bermakna bahwa *firewall* lingkup *cluster* telah aktif. Selain itu terdapat pula informasi terkait nilai parameter **Input Policy** bernilai **DROP** (semua trafik yang menuju ke PVE secara default akan **ditolak sehingga diperlukan penambahan rule untuk mengijinkan**) dan **Output Policy** bernilai **ACCEPT** (semua trafik yang keluar dari PVE akan **diijinkan**).

- Memverifikasi hasil penambahan *rule firewall* pada lingkup *cluster* melalui *host Windows 10* dengan melakukan *remote access SSH* menggunakan *Putty* ke **PVE** dengan alamat IP **192.168.169.1**. Pastikan koneksi SSH berhasil dilakukan, seperti terlihat pada gambar berikut:

```

192.168.169.1 - PuTTY
login as: root
root@192.168.169.1's password:
Linux pve 6.2.16-3-pve #1 SMP PREEMPT_DYNAMIC PVE 6.2.16-3 (2023-06-17T05:58Z) x86_64

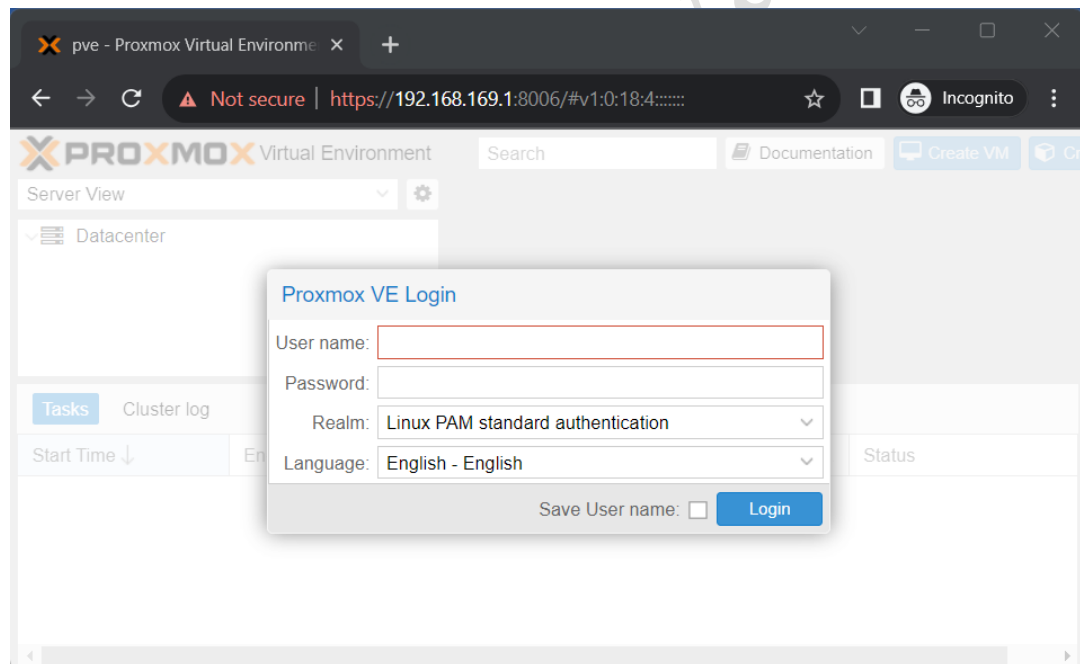
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 15 13:35:35 2023 from 192.168.169.2
root@pve:~#

```

Selain itu lakukan percobaan pengaksesan kembali **WebGUI** dari **PVE** melalui *browser Chrome* dari *host Windows 10* pada alamat <https://192.168.169.1:8006> menggunakan **Incognito Window**. Pastikan juga akses berhasil dilakukan, seperti terlihat pada gambar berikut:

c



Terlihat halaman *login* otentikasi dari PVE.

- Mengujicoba pengaksesan layanan selain **SSH** dan **WebGUI** yang diijinkan pada **PVE** dari *host Windows 10* sehingga aksesnya akan ditolak. Sebagai contoh, dilakukan verifikasi koneksi menggunakan perintah **ping 192.168.169.1** dari *command prompt*, seperti terlihat pada gambar berikut:

```

C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PUTU>ping 192.168.169.1

Pinging 192.168.169.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.169.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\PUTU>

```

Terlihat *output* **Request timed out** yang menyatakan bahwa verifikasi koneksi gagal dilakukan karena *firewall PVE* menolak permintaan *echo request* yang dikirim oleh *host Windows 10*.

- Mengujicoba akses SSH dari *CLI MikroTik CHR Internet Gateway* ke PVE menggunakan perintah “`system ssh 192.168.169.1 user=root`”, seperti terlihat pada gambar berikut:

```

[admin@MikroTik] > system ssh 192.168.169.1 user=root
password:
Linux pve 6.2.16-3-pve #1 SMP PREEMPT_DYNAMIC PVE 6.2.16-3 (2023-06-17T05:58Z) x
86_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: Sat Sep 16 09:04:48 2023 from 192.168.169.2
root@pve:~#

```

Pada inputan **password:** yang tampil masukkan “**12345678**”. Terlihat koneksi SSH berhasil dilakukan.

Eksekusi perintah “**exit**” untuk keluar dari PVE, seperti terlihat pada gambar berikut:

```

root@pve:~# exit
logout

Welcome back!
[admin@MikroTik] >

```

- Mengujicoba verifikasi koneksi dari *CLI MikroTik CHR Internet Gateway* ke PVE menggunakan perintah **ping 192.168.169.1**, seperti terlihat pada gambar berikut:


```

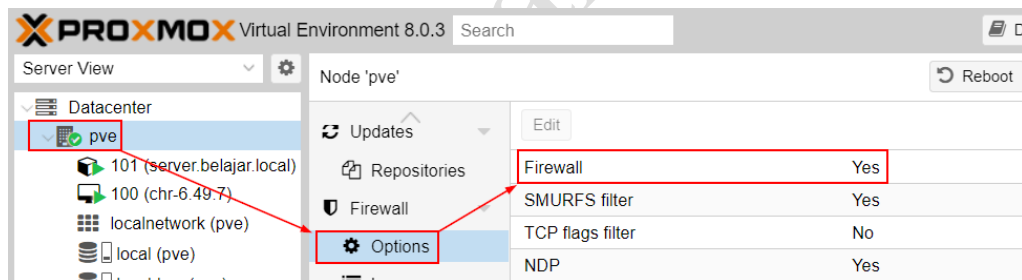
[admin@MikroTik] > ping 192.168.169.1
  SEQ HOST                               SIZE TTL TIME   STATUS
  0  192.168.169.1                         64  64  0.000  timeout
  1  192.168.169.1                         64  64  0.000  timeout
  2  192.168.169.1                         64  64  0.000  timeout
  3  192.168.169.1                         64  64  0.000  timeout
sent=4 received=0 packet-loss=100%
[admin@MikroTik] >
    
```

Tekan **CTRL+C** untuk menghentikan *ping*. Terlihat *output timeout* yang menyatakan bahwa verifikasi koneksi gagal dilakukan karena *firewall PVE* menolak permintaan *echo request* yang dikirim oleh *MikroTik CHR Internet Gateway*.

B. KONFIGURASI FIREWALL RULE PADA LINGKUP NODE

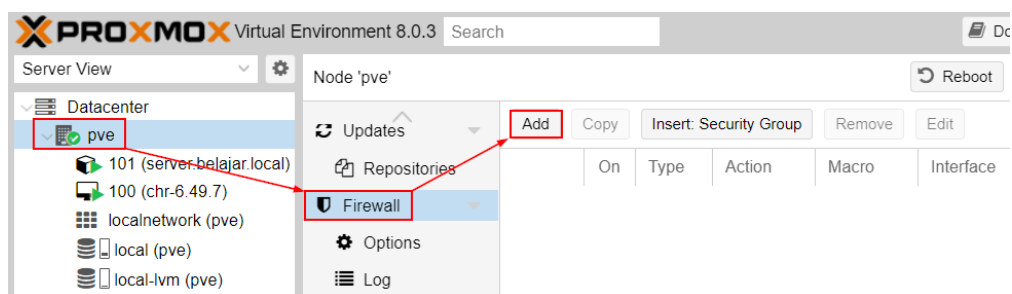
Adapun langkah-langkah konfigurasi aturan (*rule*) *firewall* pada lingkup *node PVE* adalah sebagai berikut:

1. Memverifikasi fitur *firewall* telah aktif di lingkup *node* dengan mengakses menu **Datacenter > PVE** pada panel sebelah kiri dari *Server View PVE* dan memilih menu **Firewall > Options** pada panel sebelah kanan, seperti terlihat pada gambar berikut:



Terlihat secara default *Firewall* telah aktif yang ditandai dengan nilai dari parameter **Firewall** adalah **Yes**.

2. Membuat aturan (*rule*) *firewall* untuk **mengijinkan akses ICMP** dari **MikroTik CHR Internet Gateway** dengan alamat IP **192.168.169.254** ke *node PVE*. Dapat dibuat dengan mengakses menu **Datacenter > PVE** pada panel sebelah kiri dari *Server View PVE* dan memilih menu **Firewall** pada panel sebelah kanan serta memilih tombol **Add**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Add: Rule**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Penjelasan parameter:

- Direction*., digunakan untuk menentukan arah pemfilteran trafik yaitu **IN** (paket yang masuk).
- Action*., digunakan untuk menentukan aksi atau tindakan yang diambil ketika terdapat trafik dengan nilai parameter yang sesuai dengan *rule* yaitu **ACCEPT** (diterima).
- Source*., digunakan untuk menentukan alamat IP sumber yang diijinkan untuk mengakses layanan SSH yaitu **192.168.169.254**.
- Enable*., digunakan untuk mengaktifkan rule firewall. Pastikan tercentang (✓).
- Protocol*., digunakan untuk menentukan protokol yang difilter yaitu **icmp**.
- Comment*., digunakan untuk menentukan deskripsi singkat terkait *rule firewall* yang dibuat yaitu **Allow ICMP access from Mikrotik CHR Internet Gateway**.

Klik tombol **Add** untuk memproses pembuatan *rule firewall*. Hasil dari penambahan *rule* tersebut, seperti terlihat pada gambar berikut:

On	Type	Action	Macro	Interface	Protocol	Source	S...	Destination	D Port	Lo...	Comment
<input checked="" type="checkbox"/>	in	ACCEPT			icmp	192.168.169.254					Allow ICMP access from Mikrotik CHR Internet Gateway

- Mengujicoba verifikasi koneksi dari *CLI MikroTik CHR Internet Gateway* ke PVE menggunakan perintah **ping 192.168.169.1**, seperti terlihat pada gambar berikut:

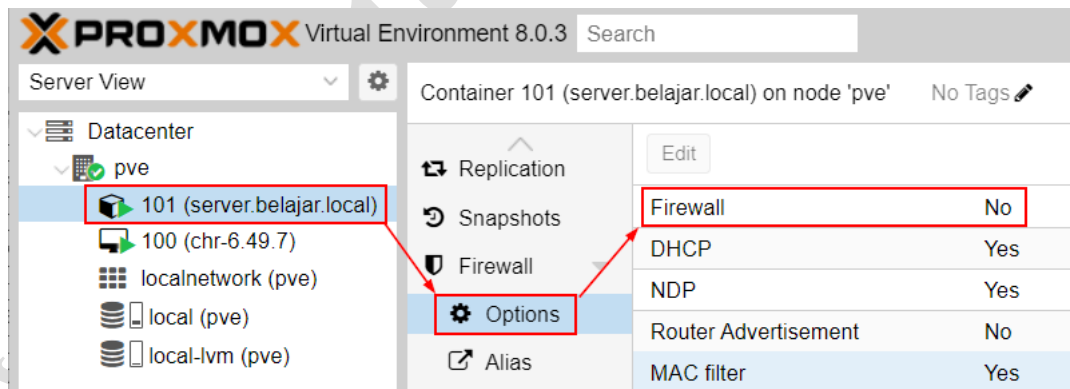
```
[admin@MikroTik] > ping 192.168.169.1
SEQ HOST                               SIZE TTL TIME STATUS
0 192.168.169.1                       56 64 0ms
1 192.168.169.1                       56 64 1ms
2 192.168.169.1                       56 64 1ms
sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
[admin@MikroTik] > _
```

Tekan **CTRL+C** untuk menghentikan *ping*. Terlihat *output* yang menyatakan bahwa verifikasi koneksi sukses dilakukan karena *firewall PVE* di lingkup node memungkinkan permintaan *echo request* yang dikirim oleh *MikroTik CHR Internet Gateway*.

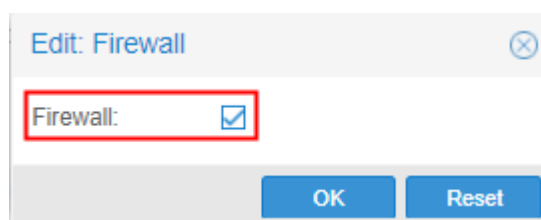
C. KONFIGURASI FIREWALL RULE PADA LINGKUP CONTAINER

Adapun langkah-langkah konfigurasi aturan (*rule*) *firewall* pada lingkup *container PVE* adalah sebagai berikut:

1. Mengaktifkan fitur **PVE Firewall lingkup container** dengan cara memilih *container* “**101 (server.belajar.local)**” di bawah *node pve* dari menu **Datacenter**. Pada panel detail sebelah kanan dari *container* tersebut dan pilih menu **Firewall > Options**. Pada panel detail dari submenu **Options** terdapat parameter **Firewall** dengan nilai default **No** yang bermakna bahwa fitur *firewall PVE* saat ini dalam keadaan tidak aktif, seperti terlihat pada gambar berikut:

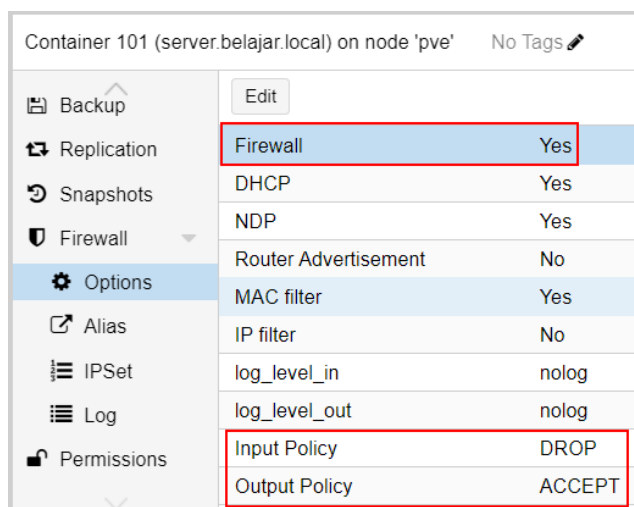


Klik dua kali pada parameter **Firewall** tersebut maka akan tampil kotak dialog **Edit: Firewall**. Tandai atau centang (✓) pada parameter *Firewall*, seperti terlihat pada gambar berikut:



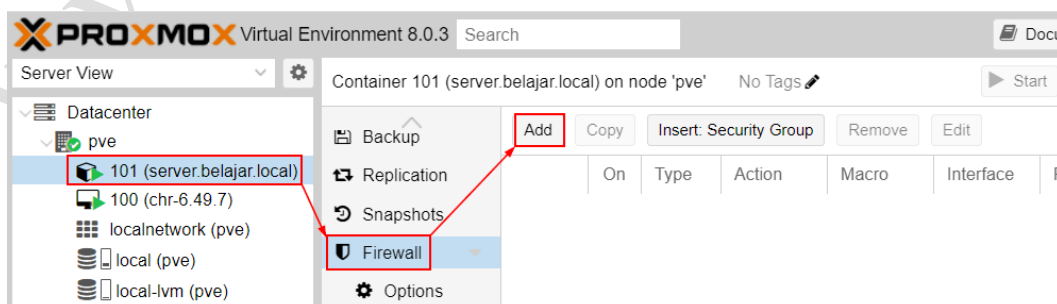
Klik tombol **OK** untuk menyimpan perubahan.

Hasil dari pengaktifan fitur *PVE firewall* lingkup *container* terlihat seperti pada gambar berikut:



Terlihat nilai parameter **Firewall** telah berubah dari **No** menjadi **Yes** yang bermakna bahwa *firewall* lingkup *container* telah aktif. Selain itu terdapat pula informasi terkait nilai parameter **Input Policy** bernilai **DROP** (semua trafik yang menuju ke *container* tersebut secara default akan **ditolak sehingga diperlukan penambahan rule untuk mengizinkan**) dan **Output Policy** bernilai **ACCEPT** (semua trafik yang keluar dari *container* tersebut akan **dijinkan**).

2. Membuat aturan (*rule*) *firewall* untuk **mengizinkan akses SSH dari Windows dengan alamat IP 192.168.169.2 ke CT ID 101**. Dapat dibuat dengan mengakses menu **Datacenter > PVE** pada panel sebelah kiri dari *Server View PVE* dan di bawah *node pve*, pilih **container “101 (server.belajar.local)”** menu **Firewall** pada panel sebelah kanan serta memilih tombol **Add**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Add: Rule**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Penjelasan parameter:

- a) *Direction*., digunakan untuk menentukan arah pemfilteran trafik yaitu **IN** (paket yang masuk).
- b) *Action*., digunakan untuk menentukan aksi atau tindakan yang diambil ketika terdapat trafik dengan nilai parameter yang sesuai dengan *rule* yaitu **ACCEPT** (diterima).
- c) *Source*., digunakan untuk menentukan alamat IP sumber yang diijinkan untuk mengakses layanan SSH yaitu **192.168.169.2**.
- d) *Enable*., digunakan untuk mengaktifkan rule firewall. Pastikan tercentang (√).
- e) *Protocol*., digunakan untuk menentukan protokol yang difilter yaitu **tcp**.
- f) *Dest. Port*., digunakan untuk menentukan nomor port tujuan yaitu **22**.
- g) *Comment*., digunakan untuk menentukan deskripsi singkat terkait *rule firewall* yang dibuat yaitu **Allow SSH From Windows**.

Klik tombol **Add** untuk memproses pembuatan *rule firewall*. Hasil dari penambahan *rule* tersebut, seperti terlihat pada gambar berikut:

On	Type	Action	Macro	Interface	Protocol	Source	S...	Destination	D.Port	Lo...	Comment
<input checked="" type="checkbox"/>	in	ACCEPT			tcp	192.168.169.2			22	no...	Allow SSH From Windows

3. Memverifikasi hasil penambahan *rule firewall* pada lingkup *container* melalui *host Windows 10* dengan melakukan *remote access SSH* menggunakan *Putty* ke **CT ID 101** dengan alamat IP **192.168.169.4**. Pastikan koneksi SSH berhasil dilakukan, seperti terlihat pada gambar berikut:

```

root@server:~
login as: root
root@192.168.169.4's password:
Last login: Fri Sep 15 06:38:44 2023 from 192.168.169.2
[root@server ~]#

```

4. Memverifikasi hasil penambahan *rule firewall* pada lingkup *container* dengan melakukan koneksi menggunakan utilitas **ping** dari *host Windows 10* ke alamat IP **Container (CT) ID 101** dengan mengeksekusi perintah `ping 192.168.169.4`. Pastikan koneksi gagal dilakukan, seperti terlihat pada gambar berikut:

```

C:\WINDOWS\system32\cmd. x + v
C:\Users\PUTU>ping 192.168.169.4

Pinging 192.168.169.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.169.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\PUTU>

```

5. Menguji coba akses SSH dari **CLI MikroTik CHR Internet Gateway** ke **CT ID 101** menggunakan perintah `system ssh 192.168.169.4 user=root`, seperti terlihat pada gambar berikut:

```

[admin@MikroTik] > system ssh 192.168.169.4 user=root
connectHandler: Connection timed out

Welcome back!
[admin@MikroTik] >

```

Tunggu hingga muncul pesan **connectHandler: Connection timed out. Welcome back!** yang menginformasikan bahwa akses SSH ke **CT ID 101** gagal dilakukan.

6. Menguji coba verifikasi koneksi dari **CLI MikroTik CHR Internet Gateway** ke **CT ID 101** menggunakan perintah `ping 192.168.169.4`, seperti terlihat pada gambar berikut:

```

[admin@MikroTik] > ping 192.168.169.4
SEQ HOST                SIZE TTL TIME  STATUS
0 192.168.169.4          32  64  0ms  timeout
1 192.168.169.4          32  64  0ms  timeout
2 192.168.169.4          32  64  0ms  timeout
3 192.168.169.4          32  64  0ms  timeout
sent=4 received=0 packet-loss=100%

[admin@MikroTik] >

```

Tekan **CTRL+C** untuk menghentikan *ping*. Terlihat *output timeout* yang menyatakan bahwa verifikasi koneksi gagal dilakukan karena *firewall container* menolak permintaan *echo request* yang dikirim oleh *MikroTik CHR Internet Gateway*.

www.iputuhariyadi.net

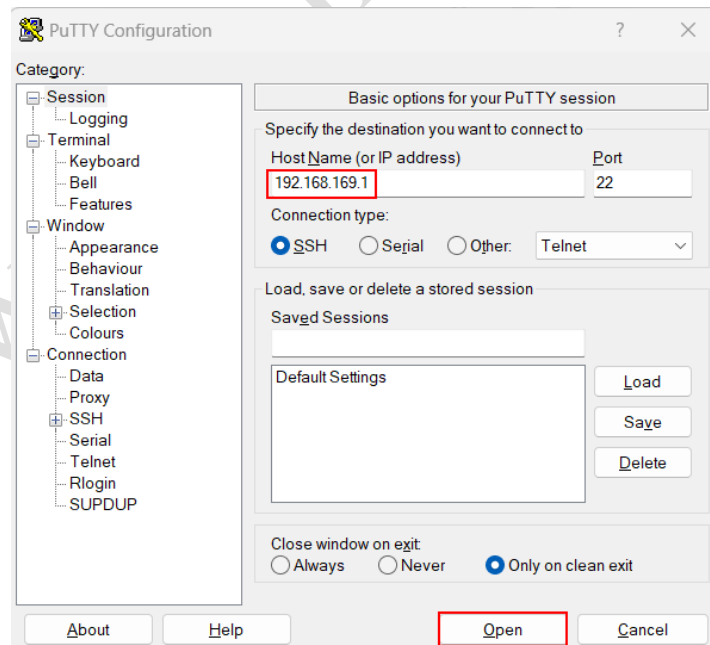
BAB X

PROTEKSI BRUTE FORCE PADA PROXMOX VE 8.0
MENGUNAKAN FAIL2BAN

[Fail2ban](#) merupakan aplikasi yang dapat melakukan pemindaian (**scan**) *file log* dan melarang atau memblokir (**ban**) alamat **Internet Protocol (IP)** yang menunjukkan tanda-tanda berbahaya berdasarkan pada seperangkat aturan (**rules**) dan pemfilteran (**filter**) yang dapat dikelola. *Fail2ban* dapat diterapkan pada **server Proxmox** untuk memproteksi terhadap serangan *brute force* pada layanan seperti *Secure Shell (SSH)*, *HyperText Transfer Protocol (HTTP)* dan *HyperText Transfer Protocol Secure (HTTPS)*.

Adapun langkah-langkah dalam menginstalasi dan mengkonfigurasi *fail2ban* untuk memproteksi brute force pada *Proxmox VE 8.0* melalui SSH adalah sebagai berikut:

1. Jalankan aplikasi *SSH Client*, sebagai contoh menggunakan *Putty*. Tampil kotak dialog *Putty Configuration*. Pada isian **Host Name (or IP Address)**, masukkan alamat IP dari *Server Proxmox* yaitu **192.168.169.1**, seperti terlihat pada gambar berikut:



Klik tombol **Open**.

2. Tampil kotak dialog *Putty* yang meminta pengguna untuk melakukan proses otentikasi login ke *Server Proxmox*, seperti terlihat pada gambar berikut:


```

192.168.169.1 - PuTTY
login as: root
root@192.168.169.1's password:
Linux pve 6.2.16-3-pve #1 SMP PREEMPT_DYNAMIC PVE 6.2.16-3 (2023-06-17T05:58Z) 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: Sat Sep 16 09:09:20 2023 from 192.168.169.254
root@pve:~#

```

Pada inputan **login as:**, masukkan “**root**” dan tekan tombol **Enter**. Selanjutnya tampil inputan **password:**, masukkan “**12345678**” dan tekan tombol **Enter**. Apabila proses otentikasi berhasil dilakukan maka akan tampil *shell prompt #*.

- Memperbaharui *server Proxmox* dengan mengeksekusi perintah “`apt update`”.

```

192.168.169.1 - PuTTY
root@pve:~# apt update
Get:1 http://security.debian.org bookworm-security InRelease [48.0 kB]
Hit:2 http://ftp.debian.org/debian bookworm InRelease
Hit:3 http://ftp.debian.org/debian bookworm-updates InRelease
Hit:4 http://download.proxmox.com/debian/pve bookworm InRelease
Hit:5 http://download.proxmox.com/debian/ceph-quincy bookworm InRelease
Fetched 48.0 kB in 4s (12.6 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
66 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@pve:~#

```

Tunggu hingga proses pembaharuan selesai dilakukan.

- Menginstalasi paket aplikasi **fail2ban** dengan mengeksekusi perintah “`apt -y install fail2ban`”, seperti terlihat pada cuplikan gambar berikut:

```

192.168.169.1 - PuTTY
root@pve:~# apt -y install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  system-log-daemon monit python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 66 not upgraded.
Need to get 549 kB of archives.
After this operation, 2,684 kB of additional disk space will be used.
Get:1 http://ftp.debian.org/debian bookworm/main amd64 fail2ban all 1.0.2-2 [451
kB]

```

5. Membuat *file* `jail.local` yang menampung konfigurasi dari **fail2ban server** terkait pemblokiran serangan **brute force** pada **port** dari layanan **SSH, HTTPS** dan **HTTP** serta **WEBGUI Proxmox** dan disimpan di direktori “`/etc/fail2ban`” dengan mengeksekusi perintah:

```
# nano -l /etc/fail2ban/jail.local
```

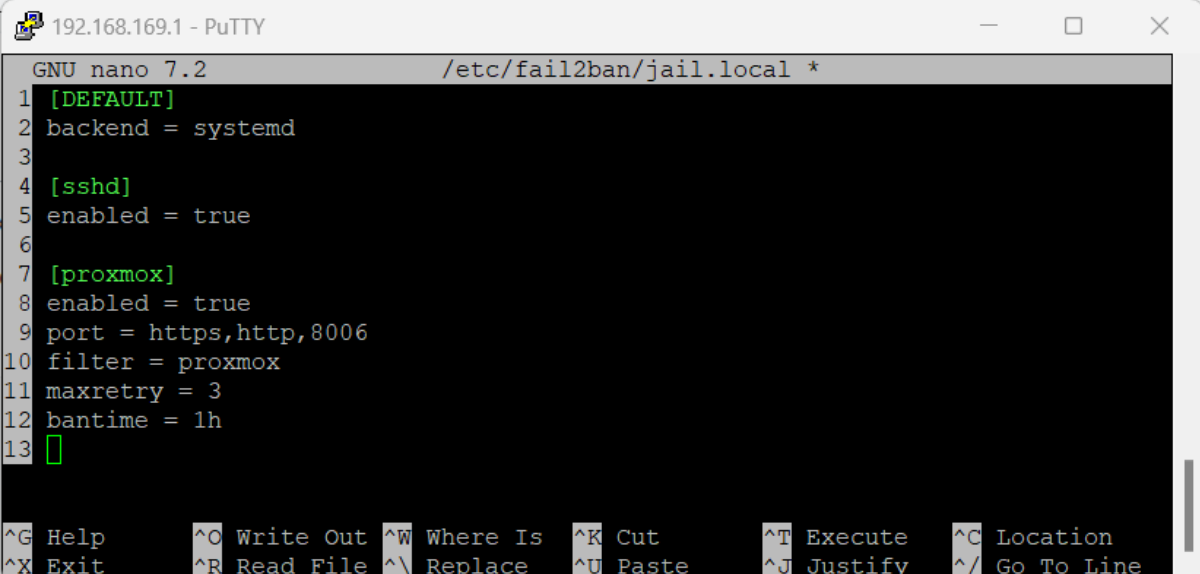
Konten pada *file* tersebut adalah sebagai berikut:

```
[DEFAULT]
backend = systemd

[sshd]
enabled = true

[proxmox]
enabled = true
port = https,http,8006
filter = proxmox
maxretry = 3
bantime = 1h
```

Sehingga hasilnya seperti terlihat pada gambar berikut:



```
192.168.169.1 - PuTTY
GNU nano 7.2 /etc/fail2ban/jail.local *
1 [DEFAULT]
2 backend = systemd
3
4 [sshd]
5 enabled = true
6
7 [proxmox]
8 enabled = true
9 port = https,http,8006
10 filter = proxmox
11 maxretry = 3
12 bantime = 1h
13 [
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Baris ke satu sampai dengan ke dua merupakan *section* (bagian) dengan nama “**DEFAULT**” yang merupakan konfigurasi global dari *jail*. Baris ke dua yaitu `backend = systemd`

menentukan **backend** untuk memperoleh *file-file* yang dimodifikasi yaitu **systemd** yang menggunakan *systemd python library* untuk mengakses *systemd journal*.

Baris ke empat sampai dengan ke lima merupakan *section* (bagian) dengan nama “**sshd**” yang merupakan konfigurasi *jail* terkait layanan **sshd**. Baris ke lima yaitu `enabled = true` digunakan untuk mengaktifkan *jail*.

Baris ke tujuh hingga ke duabelas merupakan konfigurasi *jail* terkait layanan **proxmox**. Diawali dengan nama *section* yaitu **proxmox** di baris ke tujuh. Baris ke delapan `enabled = true` digunakan untuk mengaktifkan *jail*. Baris ke sembilan `port = https, http, 8006` digunakan untuk merujuk ke layanan **HTTPS, HTTP** menggunakan nama *service*-nya dan **WEBGUI Proxmox** yang menggunakan nomor **port 8006**. Baris ke sepuluh `filter=proxmox` menentukan nama dari *file* yang ditemukan di direktori `/etc/fail2ban/filter.d` yang memuat informasi terkait *fail regex* untuk melakukan *parsing log* dengan tepat. Sedangkan baris ke sebelas `maxretry=3` digunakan untuk menentukan jumlah kecocokan atau nilai penghitung yang memicu tindakan pelarangan pada IP yaitu 3 (tiga). Terakhir baris ke duabelas yaitu `bantime=1h` digunakan untuk menentukan durasi waktu untuk alamat IP tersebut diblokir (*banned*) yaitu **1 jam (h=hour)**.

Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

6. Membuat *file proxmox.conf* yang memuat pola (**pattern**) atau **regular expression** terkait bagaimana menemukan *event* atau peristiwa pada *file log* yaitu terkait usaha kegagalan login dan disimpan di direktori “`/etc/fail2ban/filter.d`” dengan mengeksekusi perintah:

```
# nano -l /etc/fail2ban/filter.d/proxmox.conf
```

Konten pada *file* tersebut adalah sebagai berikut:

```
[Definition]
```

```
failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
ignoreregex =
```

Sehingga hasilnya seperti terlihat pada gambar berikut:

```

192.168.169.1 - PuTTY
GNU nano 7.2 /etc/fail2ban/filter.d/proxmox.conf *
1 [Definition]
2 failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
3 ignoreregex =
4
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line

```

Baris pertama merupakan **section Definition**. Sedangkan baris kedua, **failregex** digunakan untuk mencocokkan dengan teks yang ditulis oleh **Proxmox** ke *file log* dengan nama “**daemon.log**” ketika terdeteksi kegagalan *login*. Nilai dari **rhost** yaitu **<HOST>** menampung alamat IP dari *remote host* yang gagal melakukan *login* sehingga nilai tersebut dijadikan acuan oleh *fail2ban* untuk melakukan pemblokiran. Terakhir baris ketiga, **ignoreregex** digunakan mengidentifikasi entri log yang harus diabaikan oleh *Fail2Ban*, meskipun cocok dengan *failregex*.

Simpan perubahan dengan menekan tombol **CTRL+O** dan tekan **Enter**. Tekan tombol **CTRL+X** untuk keluar dari editor *nano*.

7. Merestart *service fail2ban* agar perubahan konfigurasi yang telah dilakukan berdampak dengan mengeksekusi perintah “`systemctl restart fail2ban`”.

```
root@pve:~# systemctl restart fail2ban
```

8. Memverifikasi status *service fail2ban* dengan mengeksekusi perintah “`systemctl status fail2ban`”.

```

root@pve:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: ena
   Active: active (running) since Sat 2023-09-16 10:22:12 WITA; 13s ago
     Docs: man:fail2ban(1)
    Main PID: 38472 (fail2ban-server)
      Tasks: 7 (limit: 3476)
     Memory: 41.7M
           CPU: 435ms
    CGroup: /system.slice/fail2ban.service
            └─38472 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Sep 16 10:22:12 pve systemd[1]: Started fail2ban.service - Fail2Ban Service.
Sep 16 10:22:12 pve fail2ban-server[38472]: 2023-09-16 10:22:12,886 fail2ban.co
Sep 16 10:22:13 pve fail2ban-server[38472]: Server ready

```

Tekan tombol **q** untuk keluar dari *output* perintah `systemctl status fail2ban` tersebut.

9. Memverifikasi *service fail2ban* aktif ketika *booting server Proxmox* dengan mengeksekusi perintah “`systemctl is-enabled fail2ban`”.

```
root@pve:~# systemctl is-enabled fail2ban
enabled
```

10. Memverifikasi apakah **ban** terkait **sshd** telah berfungsi dengan mengeksekusi perintah “fail2ban-client status sshd”.

```
root@pve:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
   |- Currently banned: 0
   |- Total banned: 0
   \- Banned IP list:
```

11. Memverifikasi apakah **ban** terkait **proxmox** telah berfungsi dengan mengeksekusi perintah “fail2ban-client status proxmox”.

```
root@pve:~# fail2ban-client status proxmox
Status for the jail: proxmox
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| \- Journal matches:
\-- Actions
   |- Currently banned: 0
   |- Total banned: 0
   \- Banned IP list:
```

12. Menampilkan informasi terkait **log** dari **fail2ban** yang tersimpan di file **/var/log/fail2ban.log** dengan mengeksekusi perintah “tail /var/log/fail2ban.log”.
13. Memverifikasi hasil konfigurasi **fail2ban** dengan melakukan uji coba **brute force attack** terkait layanan **SSH** di server **Proxmox** melalui **VM Mikrotik CHR Internet Gateway** dengan mengeksekusi perintah “system ssh 192.168.169.1 user=root”. Pada inputan **password:**, dengan sengaja masukkan sandi yang salah. Ulangi sampai 6 (enam) kali percobaan dan memunculkan pesan **Welcome back!** serta menunjukkan *prompt Mikrotik* kembali, seperti terlihat pada gambar berikut:

```
[admin@MikroTik] > system ssh user=root 192.168.169.1
password:
password:
password:
password:
password:
password:
Welcome back!
[admin@MikroTik] >
```

Sedangkan ketika dilakukan percobaan akses SSH kembali maka akan memunculkan pesan **connectHandler: Connection refused**, seperti terlihat pada gambar berikut:

```
[admin@MikroTik] > system ssh user=root 192.168.169.1
connectHandler: Connection refused

Welcome back!
[admin@MikroTik] >
```

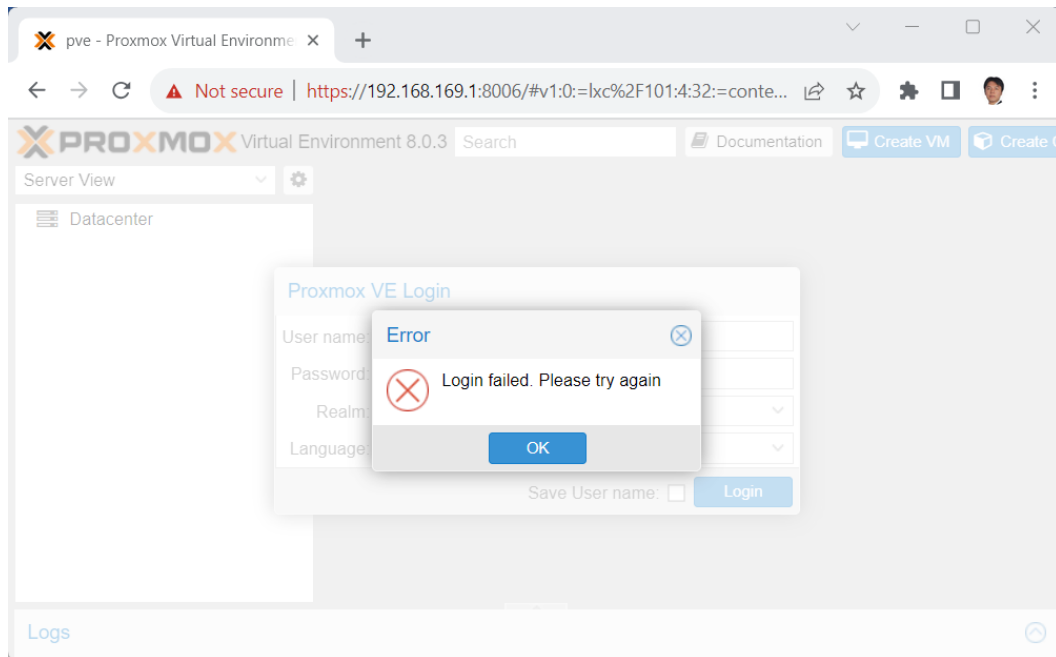
Ini menandakan bahwa koneksi SSH telah ditolak oleh **server Proxmox** karena secara *default* pada *file* konfigurasi `/etc/fail2ban/jail.conf` memuat maksimal percobaan yang diijinkan adalah 5 (**maxretry**) dan jika gagal akan melarang usaha SSH selama **600 detik** atau **10 menit (bantime)**.

14. Memverifikasi dampak dari **brute force attack** yang telah dilakukan ke layanan SSH sebelumnya melalui terminal (**Putty**) dari **server Proxmox** dengan mengeksekusi perintah “`fail2ban-client status sshd`”.

```
root@pve:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 192.168.169.254
```

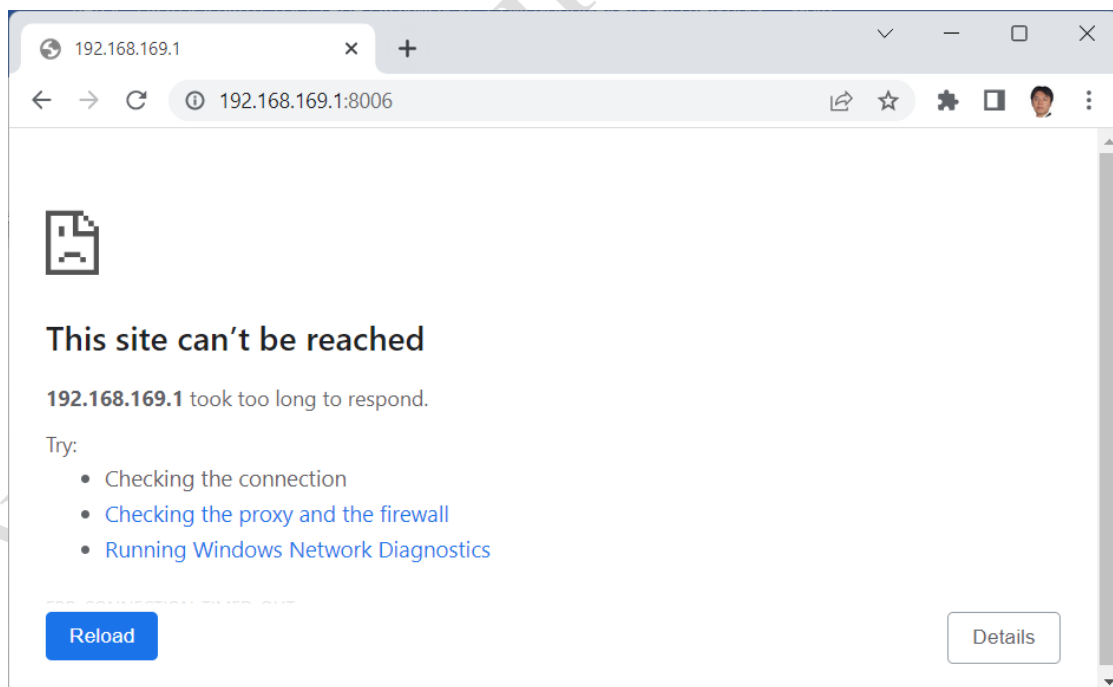
Terlihat nilai dari parameter **Total failed** pada bagian **Filter** adalah **5** sesuai dengan jumlah usaha **brute force attack** dari **VM Mikrotik CHR Internet Gateway**. Sedangkan pada parameter **Currently banned** dan **Total banned** di bagian **Actions** memperlihatkan jumlah yang di *banned* yaitu 1 (satu). Terakhir pada parameter **Banned_IP list** dari bagian **Actions**, terlihat nilai dari alamat IP yang di **banned** yaitu **192.168.169.254** yang merupakan alamat IP dari **VM Mikrotik CHR Internet Gateway**.

15. Memverifikasi hasil konfigurasi **fail2ban** dengan melakukan ujicoba **brute force attack** terkait layanan **WEBGUI** dari **server Proxmox** menggunakan *browser* pada **Windows** yaitu dengan mengakses alamat <https://192.168.169.1:8006> sehingga memunculkan halaman **login** dari **Proxmox**. Lakukan usaha *login* menggunakan **user name “root”** dengan **password** yang sengaja disalahkan sehingga memunculkan pesan **Login failed. Please try again**, seperti terlihat pada gambar berikut:



Ulangi usaha *login* dengan *password* yang sengaja disalahkan tersebut sebanyak 3 (tiga) kali.

16. Melakukan percobaan akses kembali ke **WEBGUI Proxmox** melalui *browser* menggunakan alamat <https://192.168.169.1:8006> maka akan memunculkan pesan **This site can't be reached**, seperti terlihat pada gambar berikut:



Ini menandakan bahwa koneksi ke **WEBGUI** telah ditolak oleh **server Proxmox** karena secara *default* pada *file* konfigurasi **/etc/fail2ban/jail.local** memuat maksimal percobaan yang diijinkan adalah 3 (**maxretry**) dan jika gagal akan melarang usaha akses melalui

HTTP, HTTPS dan 8006 (WEBGUI) selama 1 (satu) jam sesuai dengan nilai dari *directive bantime* yaitu **1h (h=hour)**.

- Memverifikasi dampak dari **brute force attack** yang telah dilakukan ke layanan **WEBGUI** sebelumnya melalui terminal (**Putty**) dari **server Proxmox** dengan mengeksekusi perintah “fail2ban-client status proxmox”.

```
root@pve:~# fail2ban-client status proxmox
Status for the jail: proxmox
|- Filter
| |- Currently failed: 0
| |- Total failed: 3
| `-- Journal matches:
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 192.168.169.2
```

Terlihat nilai dari parameter **Total failed** pada bagian **Filter** adalah **4** sesuai dengan jumlah usaha **brute force attack** dari *browser* pada **system Windows**. Sedangkan pada parameter **Currently banned** dan **Total banned** di bagian **Actions** memperlihatkan jumlah yang di *banned* yaitu 1 (satu). Terakhir pada parameter **Banned_IP list** dari bagian **Actions**, terlihat nilai dari alamat IP yang di **banned** yaitu **192.168.169.2** yang merupakan alamat IP dari **system Windows**.

- Membatalkan larangan (**unban**) untuk alamat IP **192.168.169.2** secara manual sebelum masa berakhir larangan sehingga **WEBGUI Proxmox** dapat diakses melalui **system Windows** dengan mengeksekusi perintah “fail2ban-client set proxmox unbanip 192.168.169.2”, seperti terlihat pada gambar berikut:

```
root@pve:~# fail2ban-client set proxmox unbanip 192.168.169.2
1
```

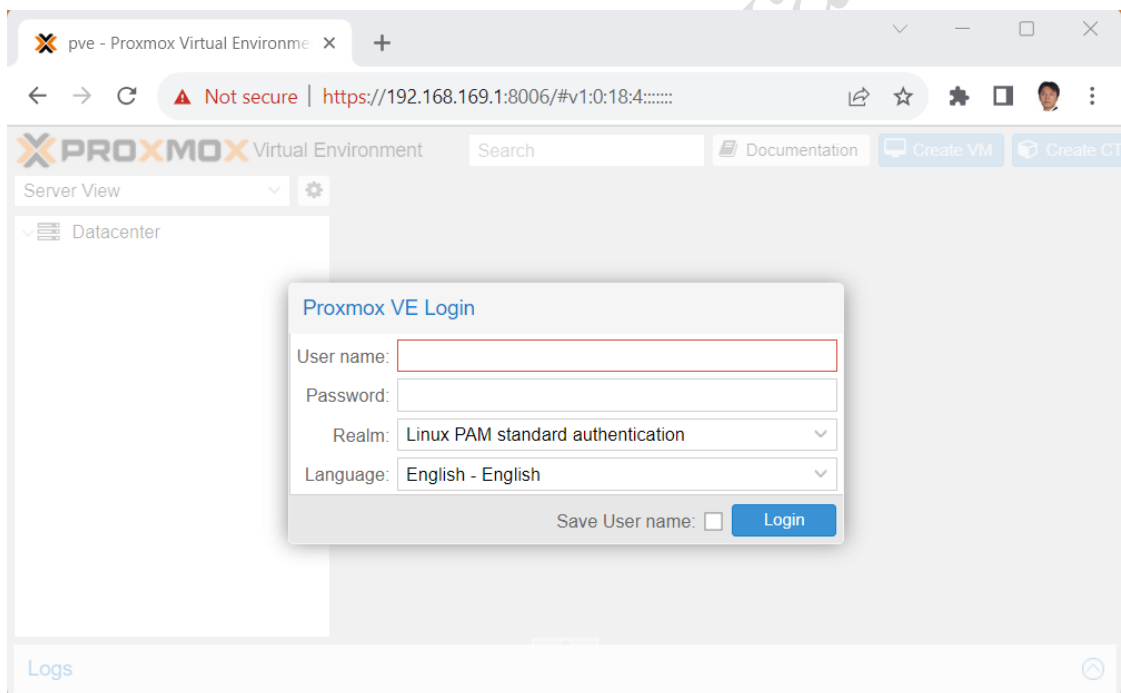
Parameter **proxmox** pada perintah tersebut merupakan nama dari **jail** yang terdapat pada *file jail.local*.

- Memverifikasi konfigurasi **unban** yang telah dilakukan sebelumnya melalui *terminal* (**Putty**) dari **server Proxmox** dengan mengeksekusi perintah “fail2ban-client status proxmox”.


```
root@pve:~# fail2ban-client status proxmox
Status for the jail: proxmox
|- Filter
| |- Currently failed: 0
| |- Total failed:    3
| `-- Journal matches:
`-- Actions
   |- Currently banned: 0
   |- Total banned:    1
   `-- Banned IP list:
```

Terlihat pada parameter **Currently banned** dari bagian **Actions**, bernilai **0** (nol) dan pada parameter **Banned_IP list** sudah tidak terlihat alamat IP dari **system Windows** yang di **banned** sebelumnya yaitu **192.168.169.2**.

20. Memverifikasi hasil **unban** dengan mengakses kembali **WEBGUI Proxmox** melalui **browser system Windows** pada alamat <https://192.168.169.1:8006>, seperti terlihat pada gambar berikut:



Terlihat halaman login dari **Proxmox** sehingga membuktikan proses *unban* berhasil dilakukan.

BAB XI

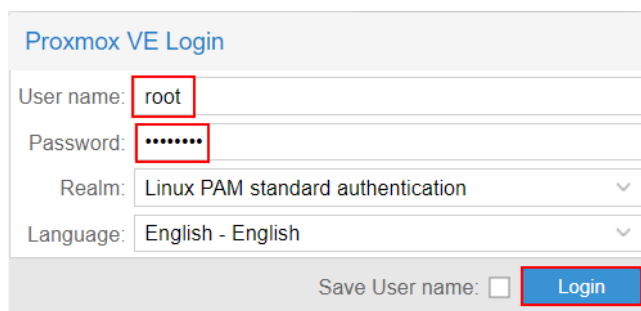
KONFIGURASI LINUX CONTAINER (LXC) CENTOS 9 STREAM
SEBAGAI SERVER INTERNET PADA PROXMOX VE 8.0

Layanan Internet yang akan dikonfigurasi pada **Linux Container (LXC) CentOS 9 Stream** dengan **ID 101** pada *Proxmox* VE 8.0 adalah **HyperText Transfer Protocol (HTTP)** menggunakan **Apache** dan **File Transfer Protocol (FTP)** menggunakan **very secure File Transfer Daemon (vsFTPd)**. Terdapat 3 (tiga) skenario pada bab ini yaitu manajemen *user*, instalasi dan konfigurasi serta ujicoba *server* FTP dan HTTP.

A. Manajemen User

Aktivitas manajemen *user* pada **LXC CentOS 9 Stream** dengan **ID 101** adalah pembuatan user baru dan pengaturan sandi *login* atau *password user*. Pastikan login ke *container* menggunakan “**root**” sebelum dapat melakukan aktivitas tersebut. Sebagai contoh akan dilakukan pembuatan 2 (dua) *user* dengan nama login “**badu**” dan “**wati**”. Sandi login untuk kedua *user* diatur sama yaitu menggunakan “**12345678**”. Adapun langkah-langkah untuk memajemen user pada LXC *CentOS 9 Stream* dengan ID 101 pada *Proxmox* VE 8.0 adalah sebagai berikut:

1. Buka *browser*, sebagai contoh menggunakan **Chrome**. Pada *address bar* dari browser, masukkan URL <https://192.168.169.1:8006>.
2. Tampil kotak dialog otentikasi *Proxmox VE Login*, lengkapi isian “**User name**” dan “**Password**”. Pada isian “*User name*”, masukkan “**root**”. Sedangkan pada isian “*Password*”, masukkan sandi login dari user “*root*” yaitu **12345678**, seperti terlihat pada gambar berikut:



Proxmox VE Login

User name: root

Password: 12345678

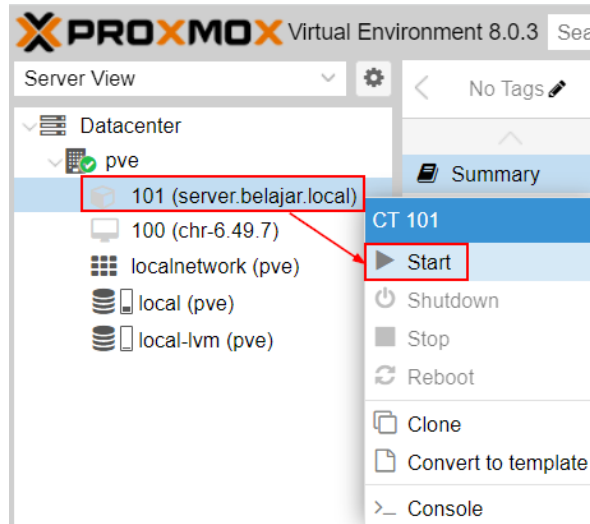
Realm: Linux PAM standard authentication

Language: English - English

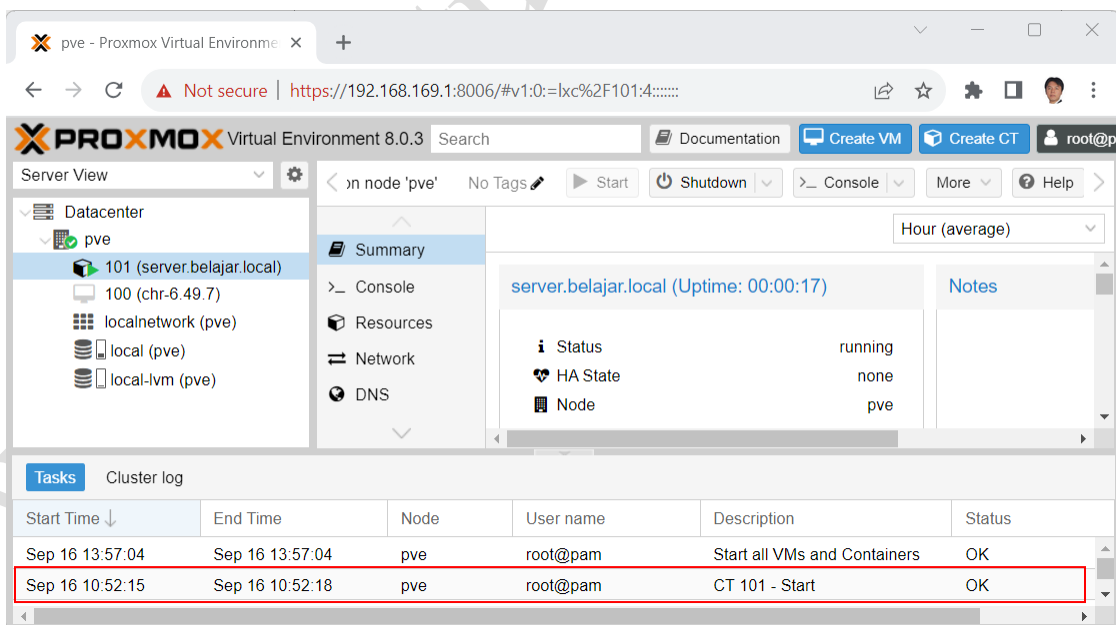
Save User name: Login

Klik tombol **Login**. Pengguna langsung diarahkan ke tampilan halaman *Server View* dari *Proxmox*.

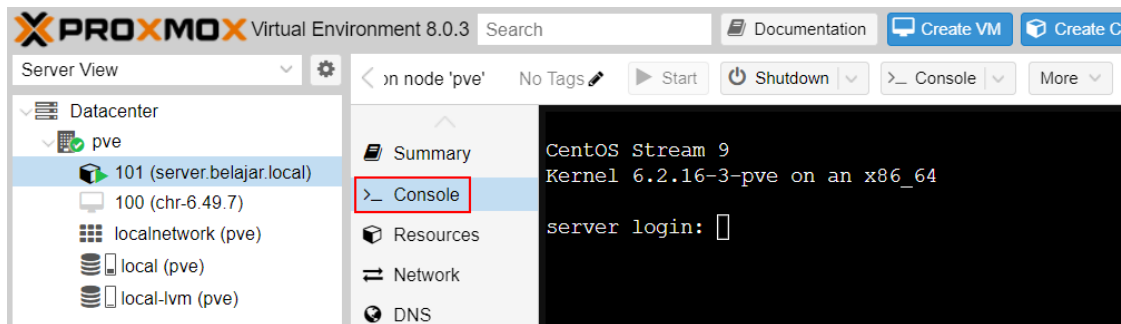
- Menjalankan *Container CentOS 9 Stream* dengan cara klik kanan pada “**101 (server.belajar.local)**” di bawah *node “pve”* dari menu **Datacenter** dan pilih **Start**, seperti terlihat pada gambar berikut:



Container CentOS 9 Stream berhasil dijalankan dimana ditandai dengan pesan status **OK** untuk **CT 101 - Start** pada bagian **Tasks** dari **Log Panel**, seperti terlihat pada gambar berikut:



Untuk mengakses tampilan dari **CT 101**, pilih **Console** pada panel sebelah kanan dari **CT 101 (server.belajar.local)**, seperti terlihat pada gambar berikut:



Tampil inputan **Server Login** untuk proses otentikasi sebelum pengguna dapat mengakses **Command Line Interface (CLI)** dari *Container CentOS 9 Stream* Masukkan nama login “**root**” pada inputan **Server Login** dan tekan tombol **Enter**.

Tampil inputan **Password:**, masukkan sandi *login* dari user “**root**” yaitu “**12345678**”, dan tekan tombol **Enter**. Apabila proses otentikasi login berhasil dilakukan maka akan tampil *prompt CLI* dari *container CentOS 9 Stream* yang ditandai dengan tanda #, seperti terlihat pada gambar berikut:

```
CentOS Stream 9
Kernel 6.2.16-3-pve on an x86_64

server login: root
Password:
Last login: Sat Sep 16 01:35:52 from 192.168.169.2
[root@server ~]# [ ]
```

4. Membuat *user* baru masing-masing dengan nama login “**badu**” dan “**wati**” menggunakan perintah “**useradd**”.

```
# useradd badu
```

```
# useradd wati
```

Hasil eksekusi perintah tersebut seperti terlihat pada gambar berikut:

```
[root@server ~]# useradd badu
[root@server ~]# useradd wati
```

5. Memverifikasi hasil pembuatan user yang telah dibuat dengan menampilkan isi dari *file* `/etc/passwd` dengan mengeksekusi perintah:

```
# tail /etc/passwd
```

```
[root@server ~]# tail /etc/passwd
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
systemd-oom:x:994:994:systemd Userspace OOM Killer:/:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
badu:x:1000:1000:/:home/badu:/bin/bash
wati:x:1001:1001:/:home/wati:/bin/bash
```

6. Setiap *user* yang dibuat pada sistem operasi linux secara otomatis akan dibuatkan group atas nama dirinya sendiri atau *primary group*. Informasi dari *group user* tersimpan pada file */etc/group*. Isi dari file tersebut dapat ditampilkan dengan mengeksekusi perintah:

```
# tail /etc/group
```

Hasil eksekusi dari perintah tersebut, seperti terlihat pada gambar berikut:

```
[root@server ~]# tail /etc/group
systemd-journal:x:190:
systemd-coredump:x:997:
dbus:x:81:
tss:x:59:
ssh_keys:x:996:
sgx:x:995:
systemd-oom:x:994:
sshd:x:74:
badu:x:1000:
wati:x:1001:
```

7. Mengatur sandi *login* dari setiap *user* menggunakan perintah “`passwd namaloginuser`”.

```
[root@server ~]# passwd badu
Changing password for user badu.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]# passwd wati
Changing password for user wati.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
```

Masukkan sandi login dari setiap user dengan nilai “12345678” pada inputan “**New password:**”. Selanjutnya tampil pesan *BAD PASSWORD* yang menginformasikan bahwa sandi login yang dimasukkan terlalu sederhana. Abaikan pesan tersebut dan masukkan

kembali sandi login dengan nilai “12345678” pada inputan “**Retype new password:**”. Apabila inputan “**New password:**” dan “**Retype new password:**” telah sama dan berhasil disimpan ke sistem linux maka akan terlihat pesan “**passwd: all authentication tokens updated successfully.**”.

8. Informasi terkait sandi *login* dari setiap pengguna di *Linux* akan disimpan pada file */etc/shadow*. Isi dari file tersebut dapat ditampilkan dengan mengeksekusi perintah:

```
# tail /etc/shadow
```

Hasil eksekusi dari perintah tersebut, seperti terlihat pada gambar berikut:

```
[root@server ~]# tail /etc/shadow
games:*:19121:0:99999:7:::
ftp:*:19121:0:99999:7:::
nobody:*:19121:0:99999:7:::
systemd-coredump:!!:19305:::::::
dbus:!!:19305:::::::
tss:!!:19305:::::::
systemd-oom:*:19615:::::::
sshd:!!:19615:::::::
badu:$6$P1lRc1nbYVez35Sd$EiWRw/MbwPvMOJSA8/QKmmH.kdh/cpgTwrAVdDtZW
s0wB8poZezBtNspcAMYyFwj7RUqfn23AZ.nw0Bn0rJw9.:19616:0:99999:7:::
wati:$6$u5DAKA3tsMcJSah0$yb1W/N4vdfNG/R4HptI6MTrBWQQxpkRbi1NWBdtW0
xRAFD8VgA0Ayqz4wY5p.XEZRUO3mXLF5kYvfOKtKhK1L/:19616:0:99999:7:::
```

9. Setiap *user* yang dibuat akan memiliki *home* direktori sebagai lokasi penyimpanan data dari masing-masing pengguna di direktori */home*. Isi dari direktori */home* dapat ditampilkan dengan mengeksekusi perintah:

```
# ls -l /home
```

Hasilnya akan terlihat seperti terlihat pada gambar berikut:

```
[root@server ~]# ls -l /home
total 8
drwx----- 2 badu badu 4096 Sep 16 02:55 badu
drwx----- 2 wati wati 4096 Sep 16 02:55 wati
```

Terlihat terdapat 2 (dua) direktori masing-masing dengan nama “*badu*” dan “*wati*” sesuai dengan nama *login* dari pengguna yang telah dibuat pada langkah sebelumnya

B. Instalasi dan Konfigurasi serta Ujicoba Server FTP

File Transfer Protocol (FTP) merupakan salah satu protokol yang digunakan untuk melakukan transfer *file* dari *client* ke *server* dan sebaliknya. FTP menggunakan mode *client/server*. *Container CentOS 7* dapat difungsikan sebagai server FTP dengan menginstalasi paket aplikasi *very secure File Transfer Protocol daemon (vsftpd)*.

Adapun langkah-langkah menginstalasi dan mengkonfigurasi serta mengujicoba *server* FTP pada **CT ID 100** adalah sebagai berikut:

1. Memverifikasi apakah paket aplikasi *vsftpd* telah terinstalasi pada sistem *Linux* menggunakan perintah:

```
# dnf list installed | grep vsftpd
```

Terlihat paket aplikasi *vsftpd* belum terinstal.

2. Menginstalasi paket aplikasi *vsftpd* sebagai FTP Server menggunakan perintah:

```
# dnf -y install vsftpd
```

```
[root@server ~]# dnf -y install vsftpd
Last metadata expiration check: 0:40:41 ago on Sat 16 Sep 2023 02:22:06 AM UTC.
Dependencies resolved.
=====
Package      Arch          Version      Repository    Size
=====
Installing:
vsftpd       x86_64        3.0.5-5.e19  appstream    168 k
Transaction Summary
=====
Install 1 Package

Total download size: 168 k
Installed size: 347 k
Downloading Packages:
vsftpd-3.0.5-5.e19.x86_64.rpm      80 kB/s | 168 kB    00:02
-----
Total                               45 kB/s | 168 kB    00:03
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : vsftpd-3.0.5-5.e19.x86_64    1/1
  Running scriptlet: vsftpd-3.0.5-5.e19.x86_64    1/1
  Verifying      : vsftpd-3.0.5-5.e19.x86_64    1/1
```

```
Installed:
vsftpd-3.0.5-5.e19.x86_64

Complete!
```

Terlihat paket aplikasi *vsftpd* telah berhasil diinstalasi.

3. Mengaktifkan *service vsftpd* secara permanen menggunakan perintah “`systemctl enable vsftpd`” agar diaktifkan secara langsung ketika *booting Linux*.

```
[root@server ~]# systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
```

4. Menjalankan *service vsftpd* dengan mengeksekusi perintah “`systemctl start vsftpd`”.

```
[root@server ~]# systemctl start vsftpd
```

5. Memverifikasi status *service vsftpd* menggunakan perintah “`systemctl status vsftpd`”.

```
[root@server ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2023-09-16 03:06:42 UTC; 4s ago
     Process: 269 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
    Main PID: 270 (vsftpd)
       Tasks: 1 (limit: 18543)
      Memory: 708.0K
         CPU: 2ms
       CGroup: /system.slice/vsftpd.service
              └─270 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Sep 16 03:06:42 server.belajar.local systemd[1]: Starting Vsftpd ftp daemon...
Sep 16 03:06:42 server.belajar.local systemd[1]: Started Vsftpd ftp daemon.
```

Terlihat *service vsftpd* telah aktif atau berjalan.

6. Menginstalasi paket aplikasi FTP *client* dengan nama “*ftp*” menggunakan perintah “`dnf -y install ftp`” agar dapat mengujicoba layanan server FTP yang telah dibangun secara lokal.

```
[root@server ~]# dnf -y install ftp
Last metadata expiration check: 0:46:50 ago on Sat 16 Sep 2023 02:22:06 AM UTC.
Dependencies resolved.
=====
Package           Architecture  Version      Repository    Size
=====
Installing:
ftp                x86_64        0.17-89.e19  appstream    62 k
Transaction Summary
-----
Install 1 Package
```



```

Total download size: 62 k
Installed size: 112 k
Downloading Packages:
ftp-0.17-89.el9.x86_64.rpm                13 kB/s | 62 kB    00:04
-----
Total                                    10 kB/s | 62 kB    00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : ftp-0.17-89.el9.x86_64        1/1
  Running scriptlet: ftp-0.17-89.el9.x86_64      1/1
  Verifying      : ftp-0.17-89.el9.x86_64        1/1

Installed:
  ftp-0.17-89.el9.x86_64

Complete!

```

Terlihat paket aplikasi *ftp* telah berhasil diinstalasi.

7. Menguji coba akses ke *server FTP* menggunakan *regular user*.

- a. Membuka koneksi ke server FTP *localhost*.

```

[root@server ~]# ftp localhost
Trying ::1...
Connected to localhost (::1).
220 (vsFTPd 3.0.5)

```

- b. Login menggunakan user “*badu*” dengan sandi “*12345678*”.

```

Name (localhost:root): badu
331 Please specify the password.
Password: 12345678
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

```

- c. Menampilkan informasi di direktori mana saat ini berada menggunakan perintah “*pwd*”.

```

ftp> pwd
257 "/home/badu" is the current directory

```

- d. Menampilkan isi direktori saat ini berada menggunakan perintah “*dir*”.

Terlihat tidak terdapat *file* atau direktori di dalam home direktori dari *user* “*badu*”.

```

ftp> dir
229 Entering Extended Passive Mode (|||61957|)
150 Here comes the directory listing.
226 Directory send OK.

```

- e. Keluar dari FTP menggunakan perintah “*quit*”.

```
ftp> quit
221 Goodbye.
[root@server ~]#
```

Dengan cara yang sama lakukan ujicoba akses FTP menggunakan user “wati”.

C. Instalasi dan Konfigurasi serta Ujicoba Server HTTP

HyperText Transfer Protocol (HTTP) merupakan protokol yang digunakan untuk menyediakan layanan web. HTTP menggunakan model *client/server*. *Server HTTP* dapat dibangun menggunakan aplikasi *Apache* dengan nama paket **httpd** pada *CentOS 9 Stream*.

Adapun langkah-langkah menginstalasi dan mengkonfigurasi serta mengujicoba server HTTP pada **CT ID 101** adalah sebagai berikut:

1. Memverifikasi apakah paket aplikasi *httpd* telah terinstalasi pada sistem *Linux* menggunakan perintah “`dnf list installed | grep httpd`”.

```
[root@server ~]# dnf list installed | grep httpd
```

Terlihat paket aplikasi *httpd* belum terinstal.

2. Menginstalasi paket aplikasi *httpd* sebagai *Server HTTP* menggunakan perintah:

```
# dnf -y install httpd
```

Seperti terlihat pada cuplikan gambar berikut:

```
[root@server ~]# dnf -y install httpd
Last metadata expiration check: 1:05:02 ago on Sat 16 Sep 2023 02:22:06 AM UTC.
Dependencies resolved.
=====
Package                Arch      Version      Repository    Size
=====
Installing:
httpd                  x86_64    2.4.57-5.el9  appstream    47 k
Installing dependencies:
apr                    x86_64    1.7.0-11.el9  appstream    123 k
apr-util               x86_64    1.6.1-23.el9  appstream    95 k
apr-util-bdb           x86_64    1.6.1-23.el9  appstream    13 k
centos-logos-httpd    noarch    90.4-1.el9    appstream    252 k
httpd-core             x86_64    2.4.57-5.el9  appstream    1.4 M
httpd-filesystem      noarch    2.4.57-5.el9  appstream    14 k
httpd-tools            x86_64    2.4.57-5.el9  appstream    81 k
mailcap                noarch    2.1.49-5.el9  baseos       33 k
Installing weak dependencies:
apr-util-openssl      x86_64    1.6.1-23.el9  appstream    15 k
mod_http2              x86_64    1.15.19-5.el9 appstream    149 k
mod_lua                x86_64    2.4.57-5.el9  appstream    61 k
Transaction Summary
=====
Install 12 Packages
```

Tunggu hingga proses instalasi paket aplikasi *httpd* selesai dilakukan.

3. Mengaktifkan *service httpd* secara permanen menggunakan perintah “systemctl enable httpd” agar diaktifkan secara langsung ketika *booting Linux*.

```
[root@server ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
```

4. Menjalankan *service httpd* dengan mengeksekusi perintah `systemctl start httpd`.

```
[root@server ~]# systemctl start httpd
```

5. Memverifikasi status *service httpd* menggunakan perintah “systemctl status httpd”.

```
[root@server ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2023-09-16 03:29:06 UTC; 3s ago
     Docs: man:httpd.service(8)
  Main PID: 401 (httpd)
   Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 18543)
  Memory: 14.7M
     CPU: 73ms
   CGroup: /system.slice/httpd.service
           └─401 /usr/sbin/httpd -DFOREGROUND
             └─402 /usr/sbin/httpd -DFOREGROUND
               └─403 /usr/sbin/httpd -DFOREGROUND
                 └─404 /usr/sbin/httpd -DFOREGROUND
                   └─405 /usr/sbin/httpd -DFOREGROUND

Sep 16 03:29:06 server.belajar.local systemd[1]: Starting The Apache HTTP Server
...
Sep 16 03:29:06 server.belajar.local systemd[1]: Started The Apache HTTP Server.
Sep 16 03:29:07 server.belajar.local httpd[401]: Server configured, listening on
: port 80
```

Terlihat *service httpd* telah aktif atau berjalan.

6. Menginstalasi *browser* berbasis teks dengan nama “lynx” agar dapat menguji coba layanan server HTTP.

```
# dnf -y install lynx
```

Seperti terlihat pada cuplikan gambar berikut:

```
[root@server ~]# dnf -y install lynx
Last metadata expiration check: 1:09:46 ago on Sat 16 Sep 2023 02:22:06 AM UTC.
Dependencies resolved.
=====
Package                Architecture Version                Repository              Size
=====
Installing:
lynx                    x86_64                2.8.9-19.el9           appstream               1.6 M
```

Tunggu hingga proses instalasi selesai dilakukan.

7. Mengakses layanan HTTP menggunakan *browser lynx*.

```
# lynx localhost
```

Hasilnya terlihat seperti gambar berikut:

```

HTTP Server Test Page powered by CentOS (p1 of 3)
HTTP Server Test Page

This page is used to test the proper operation of the HTTP server after
it has been installed. If you can read this page it means that this
site is working properly. This server is powered by CentOS.

-----

If you are a member of the general public:

The website you just visited is either experiencing problems or is
undergoing routine maintenance.

If you would like to let the administrators of this website know that
you've seen this page instead of the page you expected, you should send
them e-mail. In general, mail sent to the name "webmaster" and directed
to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting
www.example.com, you should send e-mail to "webmaster@example.com".

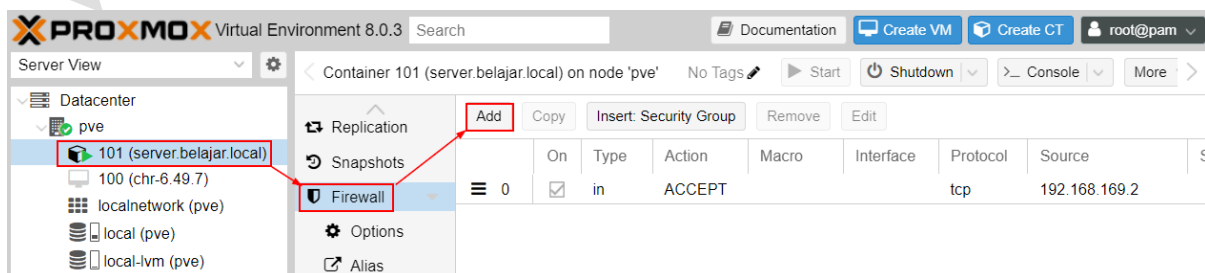
If you are the website administrator:

You may now add content to the webroot directory. Note that until you
do so, people visiting your website will see this page, and not your
-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
    
```

Terlihat menampilkan halaman **HTTP Server Test Page**.

Tekan tombol *q* untuk keluar (**quit**) dari **browser lynx** maka akan tampil pesan konfirmasi “*Are you sure you want to quit? (y)*”. Tekan tombol *y* untuk keluar.

8. Membuat aturan (*rule*) *firewall* untuk **mengijinkan akses SSH dari Windows dengan alamat IP 192.168.169.2 ke CT ID 101 melalui WEBGUI Proxmox VE** yang dapat diakses melalui *browser* pada alamat <https://192.168.169.1:8006>. Pada WEBGUI dari Proxmox VE, akses menu **Datacenter > PVE** pada panel sebelah kiri dari *Server View* *PVE* dan di bawah *node pve*, pilih **container “101 (server.belajar.local)”** menu **Firewall** pada panel sebelah kanan serta memilih tombol **Add**, seperti terlihat pada gambar berikut:



Tampil kotak dialog **Add: Rule**. Terdapat beberapa parameter yang diatur, seperti terlihat pada gambar berikut:

Penjelasan parameter:

- Direction*., digunakan untuk menentukan arah pemfilteran trafik yaitu **IN** (paket yang masuk).
- Action*., digunakan untuk menentukan aksi atau tindakan yang diambil ketika terdapat trafik dengan nilai parameter yang sesuai dengan *rule* yaitu **ACCEPT** (diterima).
- Source*., digunakan untuk menentukan alamat IP sumber yang diijinkan untuk mengakses layanan SSH yaitu **192.168.169.2**.
- Enable*., digunakan untuk mengaktifkan rule firewall. Pastikan tercentang (✓).
- Protocol*., digunakan untuk menentukan protokol yang difilter yaitu **tcp**.
- Dest. Port*., digunakan untuk menentukan nomor port tujuan yaitu **80**.
- Comment*., digunakan untuk menentukan deskripsi singkat terkait *rule firewall* yang dibuat yaitu **Allow HTTP access from Windows**.

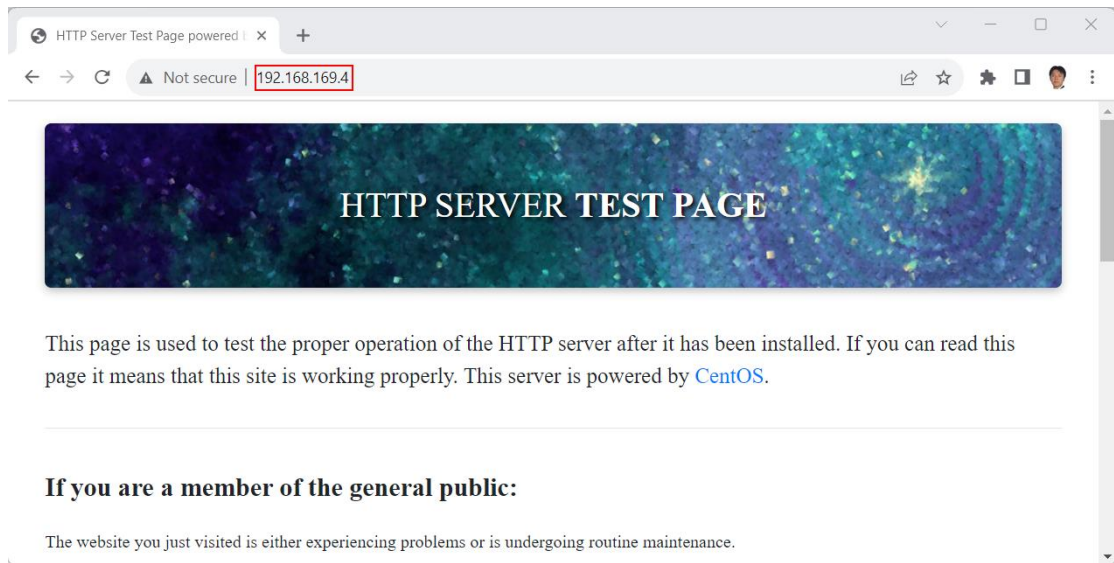
Klik tombol **Add** untuk memproses pembuatan *rule firewall*. Hasil dari penambahan *rule* tersebut, seperti terlihat pada gambar berikut:

Container 101 (server.belajar.local) on node 'pve' No Tags

Start Shutdown Console More

	On	Type	Action	Macro	Interface	Protocol	Source	S...	Destination	D.Port	Lo...	Comment
0	✓	in	ACCEPT			tcp	192.168.169.2			80	no...	Allow HTTP access from Windows
1	✓	in	ACCEPT			tcp	192.168.169.2			22	no...	Allow SSH From Windows

- Lakukan pengaksesan melalui *browser* di *Windows 10* ke alamat <http://192.168.169.4> maka hasilnya akan terlihat seperti berikut:



DAFTAR REFERENSI

Proxmox, Proxmox VE Administration Guide, 2023

Proxmox, Proxmox VE Wiki, 2023, https://pve.proxmox.com/wiki/Main_Page

Mikrotik, Mikrotik Documentation, 2023, https://wiki.mikrotik.com/wiki/Main_Page

Fail2ban Website, 2023, https://www.fail2ban.org/wiki/index.php/Main_Page

www.iputuhariyadi.net

TENTANG PENULIS



I Putu Hariyadi

adalah dosen di program studi Ilmu Komputer, [Universitas Bumigora](#), Mataram, Nusa Tenggara Barat (NTB). Penulis sangat antusias untuk mendalami dunia Teknologi Informasi & Komunikasi (TIK). Memiliki ketertarikan pada bidang Jaringan Komputer, *Network Programmability*, *Cloud Computing*, *Pemrograman Web* dan Keamanan Sistem Informasi serta Sistem Temu Kembali Informasi (*Information Retrieval*).

Sebagian besar pengalaman penulis ketika mengeksplorasi bidang tersebut dituangkan pada situs pribadi yang beralamat di <https://www.iputuhariyadi.net>. Untuk korespondensi dapat menghubungi penulis melalui email di alamat: admin@iputuhariyadi.net atau putu.hariyadi@universitasbumigora.ac.id.