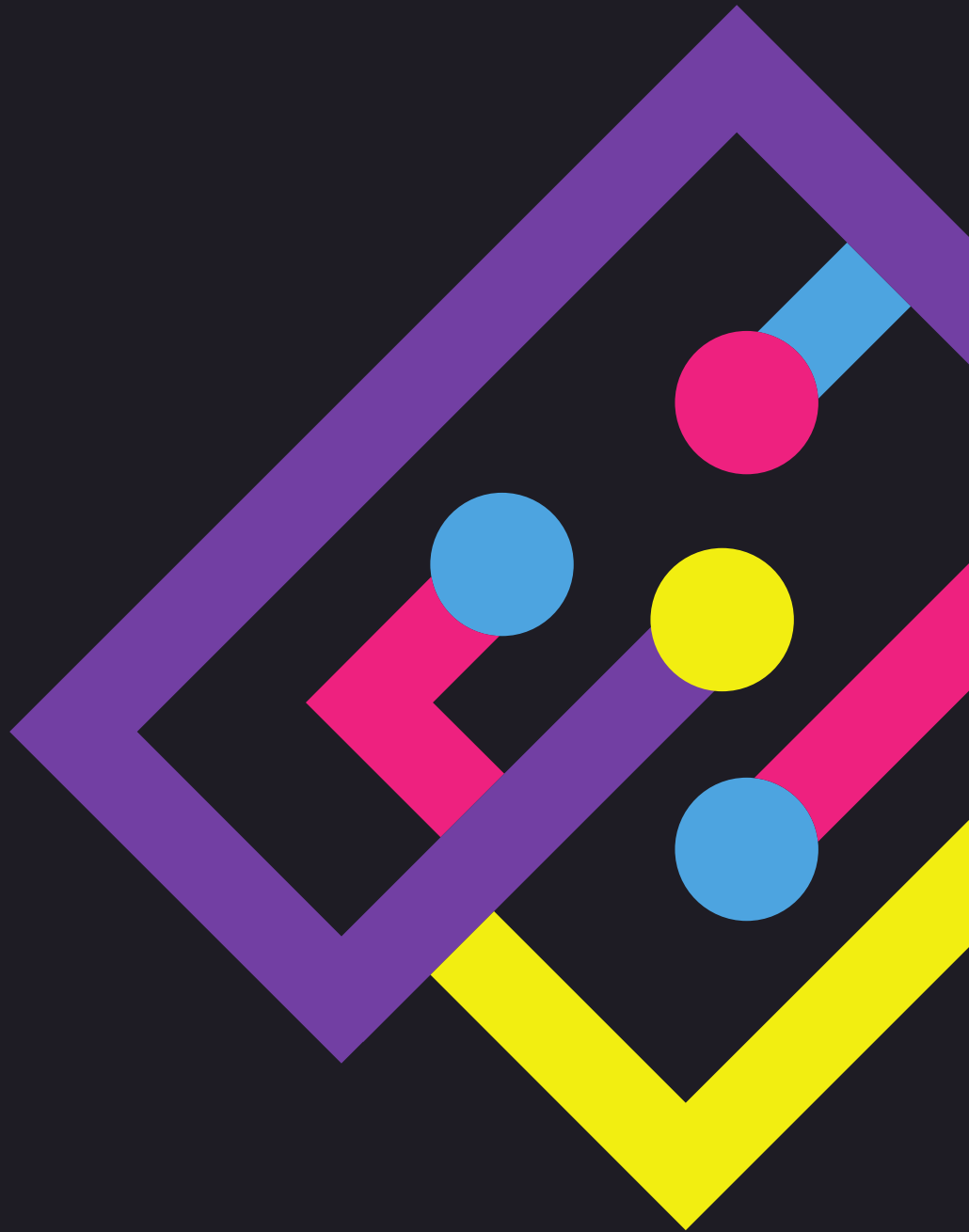


ADMINISTRASI UBUNTU VPS UNTUK WORDPRESS



MUSA AMIN

 **BITNESIA**

Administrasi Ubuntu VPS untuk WordPress

Musa Amin

BITNESIA

26 Juli 2023

DAFTAR ISI

DAFTAR ISI.....	i
DAFTAR GAMBAR.....	iv
DAFTAR TABEL.....	vi
BAGIAN 0 PENDAHULUAN.....	1
Pengguna Buku.....	1
Rancangan Server.....	1
Perangkat yang Digunakan.....	2
Pengetahuan Dasar.....	3
BAGIAN 1 SISTEM OPERASI LINUX.....	4
Distribusi Linux.....	4
Ubuntu.....	4
Struktur Direktori.....	5
Shell dan Perintah Dasar.....	7
Shell Prompt.....	8
Operasi File dan Folder.....	9
Kompresi File.....	12
Perintah Jaringan dan Internet.....	13
Manajemen User.....	15
Membuat User.....	15
Memberi Akses sudo.....	15
Menguji Akses sudo.....	15
Melepas Akses sudo.....	16
Mengubah Password.....	16
Menghapus User.....	17
Kepemilikan dan Izin Akses.....	17
Menampilkan Kepemilikan dan Izin Akses.....	17
Mengubah Kepemilikan.....	19
Mengubah Izin Akses.....	20
Text Editor.....	22
Vi/Vim.....	22
Nano.....	23
BAGIAN 2 VIRTUAL PRIVATE SERVER (VPS).....	25
Kelebihan VPS.....	26
Kapan Pakai VPS?.....	27
Tipe Virtualisasi.....	27
OpenVZ (Open Virtuozzo).....	27
KVM (Kernel-based Virtual Machine).....	28
Menyewa VPS.....	28
Menguji Kinerja (Benchmark) VPS.....	29
BAGIAN 3 DOMAIN NAME SYSTEM (DNS).....	32
Cloudflare.....	32
Cara Kerja Cloudflare.....	32
Daftarkan Domain di Cloudflare.....	34

BAGIAN 4 SECURE SHELL (SSH)	37
Remote VPS di Windows.....	37
Remote VPS di Linux.....	40
BAGIAN 5 KONFIGURASI AWAL	41
Mengatur Zona Waktu.....	41
Update dan Upgrade.....	42
Menambah User.....	43
Mengamankan SSH.....	44
Mengubah Nomor Port.....	44
Memblokir root Login SSH.....	46
Login SSH Memakai Key.....	46
BAGIAN 6 TRANSFER FILE	53
Transfer File di Xftp.....	53
Transfer File di Linux.....	54
BAGIAN 7 MARIADB DATABASE	55
Menginstal MariaDB.....	55
Mengamankan MariaDB.....	55
Membuat User dan Database.....	56
BAGIAN 8 APACHE WEB SERVER	58
Repository PPA Apache.....	58
Instalasi Apache.....	58
Konfigurasi Virtual Host.....	59
PHP di Apache.....	61
Repository PPA PHP.....	61
Instalasi PHP.....	62
Pengujian PHP.....	62
Konfigurasi php.ini untuk Apache.....	63
BAGIAN 9 NGINX WEB SERVER	64
Repository PPA Nginx.....	64
Instalasi Nginx.....	64
Server Block.....	65
PHP di Nginx.....	67
Repository PPA PHP.....	67
Instalasi PHP.....	67
Konfigurasi Server Block untuk PHP.....	68
Pengujian PHP.....	69
Konfigurasi php.ini untuk PHP-FPM.....	70
BAGIAN 10 SECURE SOCKETS LAYER (SSL)	71
SSL dari Cloudflare.....	71
Konfigurasi SSL Cloudflare.....	71
Konfigurasi SSL di Apache.....	74
Konfigurasi SSL di Nginx.....	76
BAGIAN 11 WORDPRESS	79
Instalasi WordPress dengan WP-CLI.....	79
Menguji URL Rewrite.....	81
Menguji Folder Permissions.....	82

BAGIAN 12 PHPMYADMIN.....	83
Download phpMyAdmin.....	83
Konfigurasi phpMyAdmin.....	83
Apache Virtual Host untuk phpMyAdmin.....	84
Nginx Server Block untuk phpMyAdmin.....	85
Enable-Disable phpMyAdmin.....	87
BAGIAN 13 TINY FILE MANAGER.....	89
Download Tiny File Manager.....	89
Konfigurasi Tiny File Manager.....	90
Apache Virtual Host untuk Tiny File Manager.....	91
Nginx Server Block untuk Tiny File Manager.....	92
Enable-Disable Tiny File Manager.....	94
BAGIAN 14 LOG FILE.....	96
Menampilkan Log.....	96
auth.log - Authorization Log.....	97
lastlog - Login Terakhir.....	97
Apache Log File.....	97
Nginx Log File.....	98
BAGIAN 15 SYSTEM MONITORING.....	99
htop - Interactive Process Viewer.....	99
HetrixTools - Uptime Monitor.....	100
Uptime Monitoring.....	100
Domain dan SSL Monitoring.....	100
Server Monitoring.....	101
Notifikasi ke Telegram.....	101
BAGIAN 16 FIREWALL.....	103
IPTables.....	103
Cloudflare Web Application Firewall.....	105
Firewall Rules.....	106
BAGIAN 17 BACKUP & RESTORE DATA.....	110
Backup ke Local Disk.....	110
Backup ke Google Drive.....	111
Install rclone.....	112
Script backup-gdrive.....	117
Automatic Backup.....	118
Backup Data ke Object Storage.....	119
Restore Data.....	120

DAFTAR GAMBAR

Gambar 1. Alur akses website dan server.....	2
Gambar 2. Time line masa dukungan Ubuntu.....	5
Gambar 3. Manual hier - filesystem hierarchy.....	7
Gambar 4. Izin akses file.....	18
Gambar 5. Vim berada dalam Command mode.....	22
Gambar 6. Vim berada dalam Insert mode.....	23
Gambar 7. Nano text editor.....	24
Gambar 8. Physical Server vs Virtual Machine.....	25
Gambar 9. Perbandingan kontrol layanan cloud.....	26
Gambar 10. Website dengan Cloudflare vs tanpa Cloudflare.....	33
Gambar 11. Statistik pemakaian bandwidth.....	33
Gambar 12. Form daftar akun Cloudflare.....	34
Gambar 13. Form Add site.....	34
Gambar 14. Paket Free layanan Cloudflare.....	34
Gambar 15. DNS records.....	35
Gambar 16. Pengaturan nameserver domain.....	35
Gambar 17. Perubahan nameserver.....	36
Gambar 18. Quick start guide.....	36
Gambar 19. New session Xshell.....	37
Gambar 20. Host key.....	38
Gambar 21. SSH User Name.....	38
Gambar 22. SSH User Authentication.....	39
Gambar 23. Remote SSH ke VPS dengan Xshell.....	39
Gambar 24. Remote SSH ke VPS dengan OpenSSH client.....	40
Gambar 25. Pesan permintaan restart.....	42
Gambar 26. File konfigurasi SSH server.....	44
Gambar 27. Status SSH service.....	45
Gambar 28. Nomor port di Xshell.....	45
Gambar 29. User Key Manager.....	46
Gambar 30. Key Generation Parameters.....	47
Gambar 31. Generate Public Key.....	47
Gambar 32. Key name.....	48
Gambar 33. Public Keys.....	48
Gambar 34. SSH User Authentication dengan Public Key.....	51
Gambar 35. Login SSH dengan nama host.....	52
Gambar 36. Lokasi shortcut Xftp di Xshell.....	53
Gambar 37. Koneksi SFTP di Xftp.....	54
Gambar 38. Status service MariaDB.....	55
Gambar 39. mysql command-line.....	57
Gambar 40. Status service apache2.....	59
Gambar 41. Apache default page.....	59
Gambar 42. Halaman index.html domain.....	61
Gambar 43. PHP Info dengan Apache.....	62

Gambar 44. Opsi upload_max_filesize di PHP Info.....	63
Gambar 45. Status service nginx.....	65
Gambar 46. Nginx default page.....	65
Gambar 47. Halaman index.html domain.....	67
Gambar 48. PHP Info dengan PHP-FPM.....	69
Gambar 49. Cloudflare SSL/TLS encryption mode.....	72
Gambar 50. Origin certificates.....	72
Gambar 51. Generate SSL di Cloudflare.....	72
Gambar 52. Origin Certificate.....	73
Gambar 53. Private Key.....	73
Gambar 54. Hasil instalasi WordPress.....	81
Gambar 55. Setting Permalinks.....	81
Gambar 56. URL postingan memakai judul post.....	82
Gambar 57. Theme Details.....	82
Gambar 58. Form login phpMyadmin.....	86
Gambar 59. Halaman home phpMyAdmin.....	87
Gambar 60. Password Hash Generator.....	90
Gambar 61. Halaman login Tiny File Manager.....	93
Gambar 62. Folder /var/www di Tiny File Manager.....	94
Gambar 63. Pemakaian CPU dan RAM di htop.....	99
Gambar 64. Process dan pemakaian CPU/RAM di htop.....	100
Gambar 65. HetrixTools Server Monitoring.....	101
Gambar 66. Notifikasi HetrixTools di Telegram.....	102
Gambar 67. Firewall Rules.....	106
Gambar 68. Rule Allow Known Bots.....	106
Gambar 69. Rule Block !Indonesia - wp-login_wp-admin.....	107
Gambar 70. Rule Block Rusia Cina Jerman.....	108
Gambar 71. Rule Block Files.....	109
Gambar 72. Folder Backup-VPS di Google Drive.....	112
Gambar 73. rclone meminta akses ke Google Account.....	115

DAFTAR TABEL

Tabel 1. Direktori di Linux.....	6
Tabel 2. Izin akses Numeric Mode.....	20
Tabel 3. Operator izin akses dengan Symbolic Mode.....	21
Tabel 4. Karakter untuk izin akses Symbolic Mode.....	21
Tabel 5. Tombol perintah yang sering digunakan di nano.....	24

BAGIAN 0

PENDAHULUAN

Virtual Private Server (VPS) semakin sering digunakan sebagai server untuk menjalankan website WordPress. Ada yang memilih upgrade dari shared hosting ke VPS karena memerlukan sumber daya yang lebih tinggi dan ada pula yang sedari awal sudah menggunakan VPS.

Namun ada kendala yang terjadi ketika memakai VPS yaitu dibutuhkan keterampilan dalam administrasi Linux server karena VPS menggunakan sistem operasi Linux. Untuk itu, buku ini hadir untuk memberikan panduan teknis yang berisi langkah-langkah bagaimana administrasi VPS dengan sistem operasi Linux (Ubuntu 20.04) untuk menjalankan website WordPress.

Pengguna Buku

Buku ini ditujukan untuk WordPress developer yang ingin mempelajari bagaimana cara melakukan administrasi Ubuntu Virtual Private Server (VPS) untuk operasional website WordPress tanpa menggunakan control panel yang semua proses instalasi dan konfigurasi berbasis command line.

Selain itu, buku ini juga dapat menjadi buku panduan dasar bagi seorang calon system administrator (sysadmin) yang bertugas mengelola server dengan sistem operasi Ubuntu dan aplikasi website berbasis PHP.

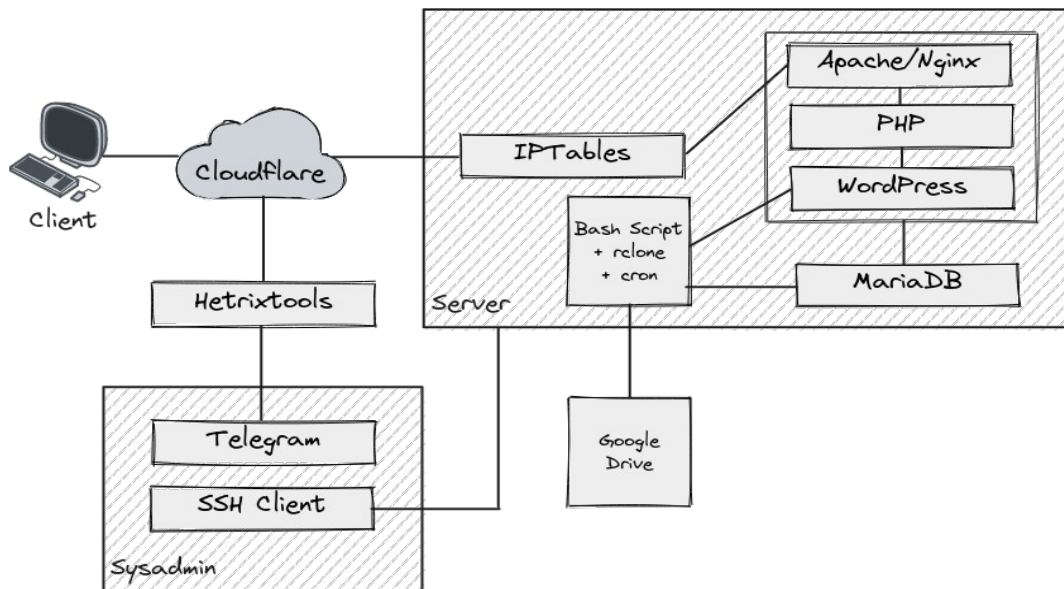
Rancangan Server

Alur akses website dan server yang dirancang dalam buku ini yaitu permintaan dari web browser (HTTP request) tidak direspon (HTTP response) secara langsung oleh web server (Apache atau Nginx) yang berada di VPS, tetapi dilayani oleh Cloudflare.

Cloudflare yang menjadi perantara antara web browser dengan VPS bertujuan untuk melakukan pengamanan (proxy, firewall dan SSL) terhadap VPS dan kemudahan dalam manajemen DNS record. VPS hanya dapat diakses secara langsung oleh system administrator melalui protokol SSH.

Untuk memantau apakah website sedang aktif atau tidak (uptime monitoring) menggunakan layanan dari HetrixTools yang tetap melalui Cloudflare. Jika website tidak aktif (down), HetrixTools mengirimkan

notifikasi ke Telegram, begitu pula ketikan website sudah aktif kembali (up). Selain itu, HetrixTools juga digunakan sebagai system monitoring, memantau kinerja server, agent (HetrixTools client) mengirimkan data dari server ke HetrixTools.



Gambar 1. Alur akses website dan server

Perangkat yang Digunakan

Perangkat lunak dan tool yang digunakan di dalam buku ini:

1. VPS dengan sistem operasi Ubuntu 20.04
2. Nama domain
3. Akun [Cloudflare](#), [HetrixTools](#), dan [Google](#)
4. SSH Client [Xshell](#) (Windows)
5. SFTP Client [Xftp](#) (Windows)
6. Text Editor [Sublime Text](#)
7. Web Browser [Mozilla Firefox](#) atau [Google Chrome](#)
8. Jaringan internet yang stabil

Pengetahuan Dasar

Pengetahuan dasar yang dibutuhkan agar dapat mempermudah dalam mempraktikkan langkah-langkah teknis di dalam buku ini:

- Jaringan komputer seperti protokol jaringan
- Struktur direktori pada sistem operasi Linux
- Ownership dan permission file di Linux
- Perintah Linux dasar
- Text editor berbasis command-line seperti nano atau vim

BAGIAN 1

SISTEM OPERASI LINUX

Sistem operasi Linux merupakan sistem operasi free software yang salah satu unsur kebebasannya yaitu bebas digunakan untuk tujuan apapun termasuk untuk tujuan bisnis. Selain itu kode sumbernya tersedia bagi siapa saja untuk dipelajari, dikembangkan, dan didistribusikan ulang.

Umumnya website diakses di internet setiap hari mulai dari blog, media online, e-commerce, sampai media sosial di belakangnya ada komputer server yang menjalankan sistem operasi Linux. Penyedia layanan Virtual Private Server (VPS) juga umumnya menyediakan Linux sebagai pilihan sistem operasinya.

Selain sifatnya yang free dan open source, beberapa faktor lain yang menjadi alasan mengapa memilih Linux sebagai sistem operasi terbaik untuk server antara lain bebas biaya lisensi, stabilitas, keandalan, keamanan, fleksibilitas, dan hemat dalam pemakaian resources (sumber daya CPU, RAM, disk).

Distribusi Linux

Linux mengadopsi lisensi free software membuatnya terbuka. Hal tersebut memungkinkan siapa saja boleh ikut berkontribusi dalam pengembangannya, bahkan dapat mengembangkannya menjadi varian lain sesuai dengan kebutuhan atau tujuan komputasi tertentu.

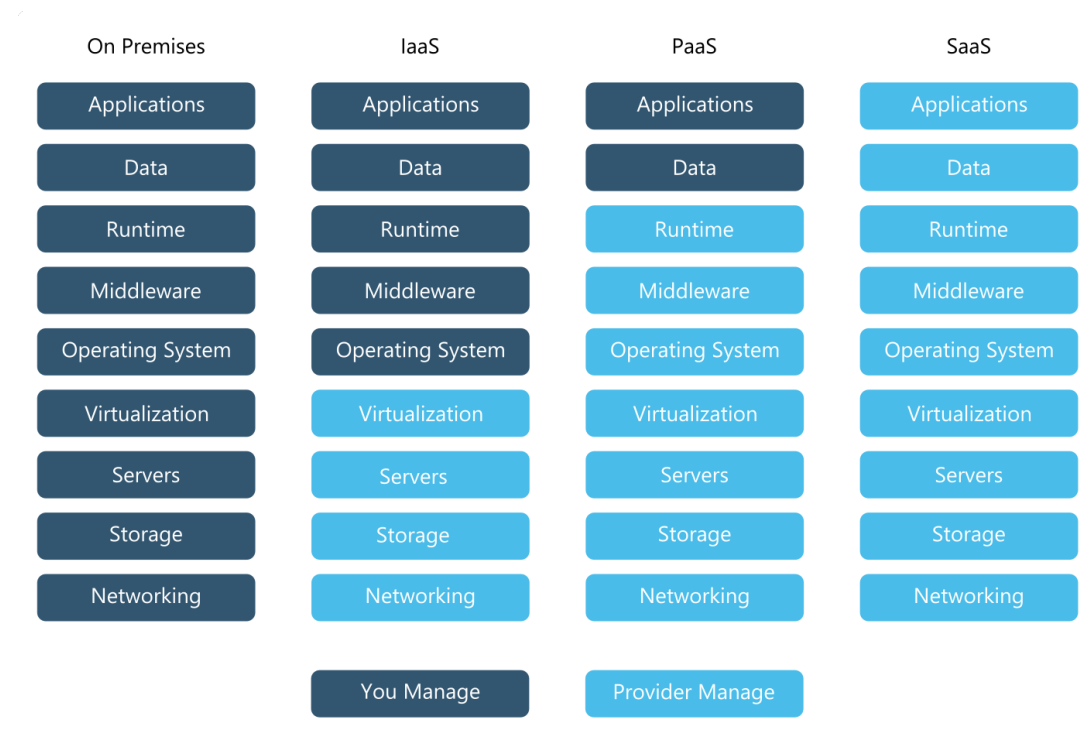
Berbagai varian Linux disebut sebagai Linux distro (distribution) atau distribusi Linux. Daftar varian Linux dapat dilihat di distrowatch.com yang jumlahnya telah mencapai lebih dari 250 distribusi Linux.

Distribusi Linux yang umumnya digunakan sebagai sistem operasi server antara lain, Red Hat, CentOS, openSUSE, SUSE Linux, Debian, dan Ubuntu. Dalam buku ini distribusi Linux yang digunakan adalah Ubuntu.

Ubuntu

[Ubuntu](#) adalah salah satu distribusi Linux populer yang dapat digunakan untuk memenuhi kebutuhan komputasi baik itu untuk desktop maupun server. Ubuntu merupakan turunan dari Debian yang berarti manajemen

dikeluarkan lebih besar dibandingkan dengan web hosting, pengguna VPS harus memiliki keterampilan administrasi Linux server. VPS yang harus dikelola sendiri disebut sebagai VPS Unmanaged, sedangkan kebalikannya VPS yang konfigurasinya dibantu oleh penyedia disebut sebagai VPS Managed.



Gambar 9. Perbandingan kontrol layanan cloud

Kelebihan VPS

Kelebihan VPS jika dibandingkan dengan web hosting:

- Ketersediaan sumber daya memori (RAM) dan prosesor (CPU) yang lebih baik, tidak perlu berbagi dengan pengguna lain.
- Kapasitas penyimpanan lebih besar (Disk), bahkan di beberapa penyedia cloud server dapat meningkatkan kapasitas disk atau menambah disk baru.
- Kinerja server lebih baik, mengurangi kemungkinan terjadinya website lambat atau tidak dapat diakses (down) akibat dari meningkatnya trafik pengunjung website.
- Keamanan dan privasi data lebih terjamin, karena pengguna lain tidak dapat mengaksesnya.

- Kontrol secara penuh, diberikan user root untuk dapat melakukan instalasi dan konfigurasi server. Bebas memasang layanan apa yang ingin dijalankan.

Kapan Pakai VPS?

Meskipun VPS memiliki banyak kelebihan, tapi sebagai calon pengguna harus tahu juga kapan waktu yang tepat untuk memakai VPS.

- Ketika membutuhkan kustomisasi konfigurasi, bahasa pemrograman, dan database.
- Ketika membutuhkan resources server yang lebih besar, karena trafik pengunjung website atau pengguna aplikasi yang semakin meningkat.
- Ketika membutuhkan akses root ke server.
- Ketika membutuhkan server untuk development environment (lingkungan pengembangan) atau testing environment (lingkungan pengujian) .
- Ketika memproses data transaksi keuangan dan data sensitif.

Tipe Virtualisasi

Terdapat dua tipe virtualisasi yang digunakan oleh penyedia dalam membangun VPS yaitu OpenVZ dan KVM. Tiap tipe virtualisasi tersebut memiliki kelebihan dan kekurangan masing-masing yang perlu diketahui sebelum memutuskan untuk memilih tipe VPS.

OpenVZ (Open Virtuozzo)

OpenVZ merupakan virtualisasi yang berbasis container pada sistem operasi Linux. Tipe virtualisasi ini menggunakan Linux kernel dari host-OS sehingga hanya dapat menjalankan sistem operasi Linux saja.

Selain hanya dapat menjalankan Linux, keterbatasan lainnya yaitu tidak mendukung swap (menggantikan disk sebagai virtual memory untuk membantu RAM), sementara beberapa aplikasi mengharuskan adanya swap.

Kelebihan dari VPS dengan virtualisasi OpenVZ yaitu biaya sewa yang lebih murah. Selain itu, konfigurasi resources dapat dilakukan tanpa perlu restart.

VPS dengan OpenVZ cocok digunakan untuk menjalankan website dan tidak membutuhkan adanya kustomisasi kernel.

KVM (Kernel-based Virtual Machine)

KVM merupakan teknologi virtualisasi yang full hardware, dikembangkan dan dijalankan di atas sistem operasi Linux, diinstal langsung di atas server fisik (bare metal).

Dengan KVM, pengguna dapat menggunakan sistem operasi apa saja pada virtual machine termasuk Windows. VPS dengan virtualisasi KVM sering juga disebut semi dedicated server karena performa yang baik dan andal.

Kelebihan lainnya yaitu mendukung partisi swap, masing-masing VPS memiliki RAM dan CPU tersendiri, dan biasanya sudah disertai VNC remote. Tetapi untuk mendapatkan segala kelebihan tersebut harus mengeluarkan biaya yang lebih mahal.

VPS dengan virtualisasi KVM cocok digunakan untuk menjalankan website atau aplikasi yang memerlukan sumber daya yang tinggi.

Menyewa VPS

VPS bisa didapatkan dengan menyewa dari perusahaan penyedia VPS. Terdapat dua model penyewaan VPS yaitu bayar per bulan atau bayar sesuai dengan pemakaian (Pay-as-you-go).

Ketika menggunakan VPS dengan model Pay-as-you-go pengguna harus terlebih dahulu mengisi saldo ke dalam akun agar dapat melakukan pembuatan VPS. Saldo akan terpotong secara otomatis berdasarkan berapa lama pemakaian dan spesifikasinya.

Spesifikasi VPS

Spesifikasi VPS secara umum ada empat yaitu CPU, memory, disk, dan bandwidth. Spesifikasi paling rendah 1 CPU, 1GB RAM, 25GB disk, dan 1TB bandwidth. Dengan spesifikasi tersebut harga sewa di provider lokal mulai dari Rp50.000/bulan dan harga sewa di provider luar negeri mulai dari \$5/bulan.

Informasi Akses VPS

Jika VPS sudah siap, catat informasi yang dibutuhkan untuk mengakses VPS (SSH remote) yaitu username yang biasanya adalah root, password, dan IP address. IP address nantinya juga dibutuhkan untuk konfigurasi di DNS records (menghubungkan domain ke VPS).

Menguji Kinerja (Benchmark) VPS

Benchmark VPS adalah proses pengujian dan pengukuran kinerja dari sebuah VPS. Tujuannya untuk mendapatkan informasi tentang seberapa baik VPS tersebut bekerja dalam berbagai aspek, seperti kecepatan CPU, kecepatan disk, kestabilan jaringan, dan penggunaan sumber daya. Salah satu tool yang dapat digunakan untuk benchmark VPS yaitu [Bench.sh](#).

Menjalankan Bench.sh.

```
# wget -qO- bench.sh | bash
```

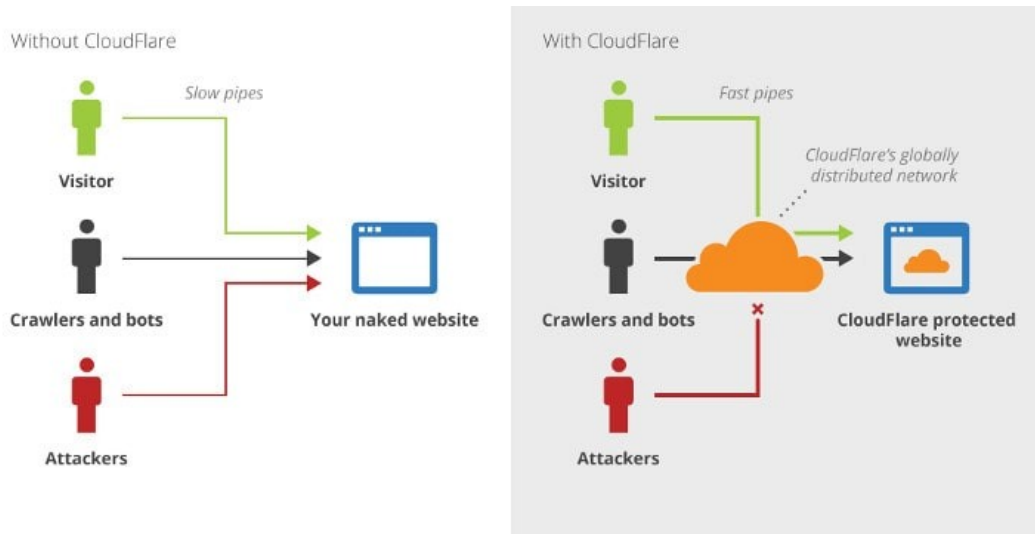
Contoh potongan hasil benchmark dari Bench.sh.

```
CPU Model      : AMD EPYC 7542 32-Core Processor
CPU Cores      : 1 @ 2894.558 MHz
CPU Cache      : 512 KB
AES-NI         : Enabled
VM-x/AMD-V     : Disabled
Total Disk     : 24.5 GB (2.8 GB Used)
Total Mem      : 870.3 MB (270.7 MB Used)
System uptime  : 0 days, 0 hour 0 min
Load average   : 0.99, 0.25, 0.09
OS             : Ubuntu 22.04.1 LTS
Arch           : x86_64 (64 Bit)
Kernel        : 5.15.0-53-generic
TCP CC        : cubic
Virtualization : KVM
IPv4/IPv6     : OnLine / OnLine

-----

I/O Speed(1st run) : 418 MB/s
I/O Speed(2nd run) : 424 MB/s
I/O Speed(3rd run) : 295 MB/s
I/O Speed(average) : 379.0 MB/s

-----
```

Gambar 10. Website dengan Cloudflare vs tanpa Cloudflare

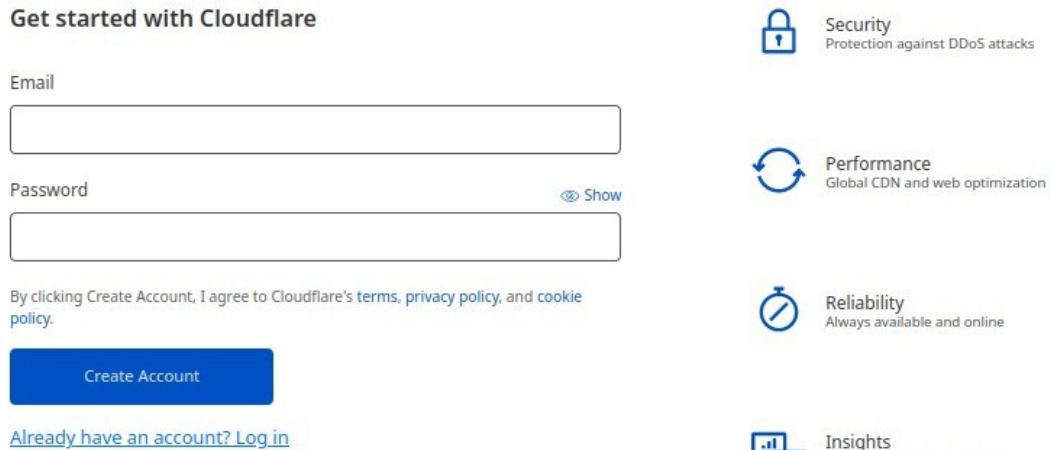
Faktor lain yang menjadi pertimbangan dalam menggunakan Cloudflare yaitu dapat menghemat bandwidth karena Cloudflare membuat cache dari file statis website. Penghematan bandwidth ini sangat membantu bagi pemilik website dengan trafik tinggi.



Gambar 11. Statistik pemakaian bandwidth

Daftarkan Domain di Cloudflare

1. Membuat akun Cloudflare, klik [Sign Up](#) di cloudflare.com. Jika sudah punya akun, bisa langsung [Login](#).



Get started with Cloudflare

Email

Password Show

By clicking Create Account, I agree to Cloudflare's [terms](#), [privacy policy](#), and [cookie policy](#).

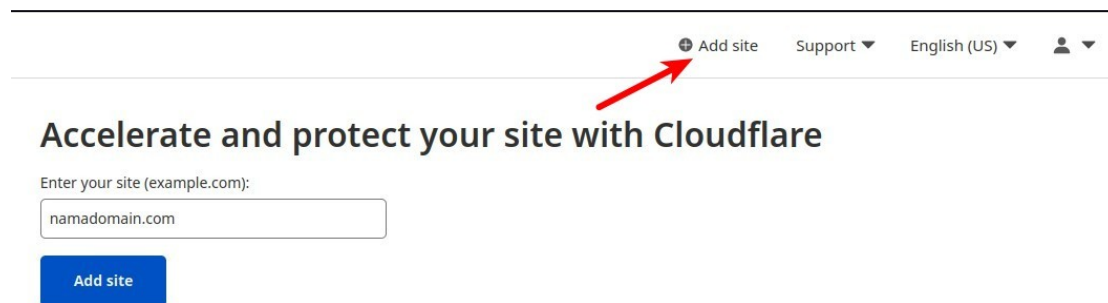
[Create Account](#)

[Already have an account? Log in](#)

- Security**
Protection against DDoS attacks
- Performance**
Global CDN and web optimization
- Reliability**
Always available and online
- Insights**
Built in analytics and more

Gambar 12. Form daftar akun Cloudflare

2. Login Cloudflare, klik menu **Add Site**, masukkan nama domain, lalu klik tombol **Add site**.



Accelerate and protect your site with Cloudflare

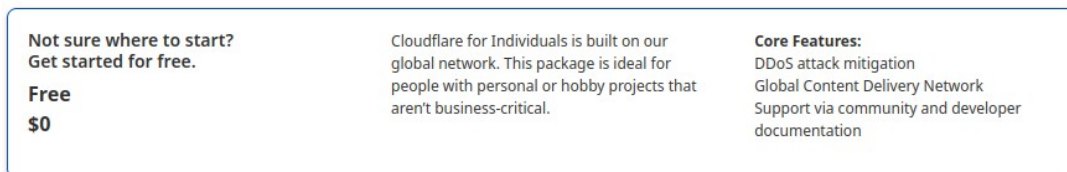
Enter your site (example.com):

[Add site](#)

[Add site](#) Support English (US) User

Gambar 13. Form Add site

3. Memilih paket (Plan), pilih **Free \$0**, lalu **Continue**.



Not sure where to start? Get started for free.

Free \$0

Cloudflare for Individuals is built on our global network. This package is ideal for people with personal or hobby projects that aren't business-critical.

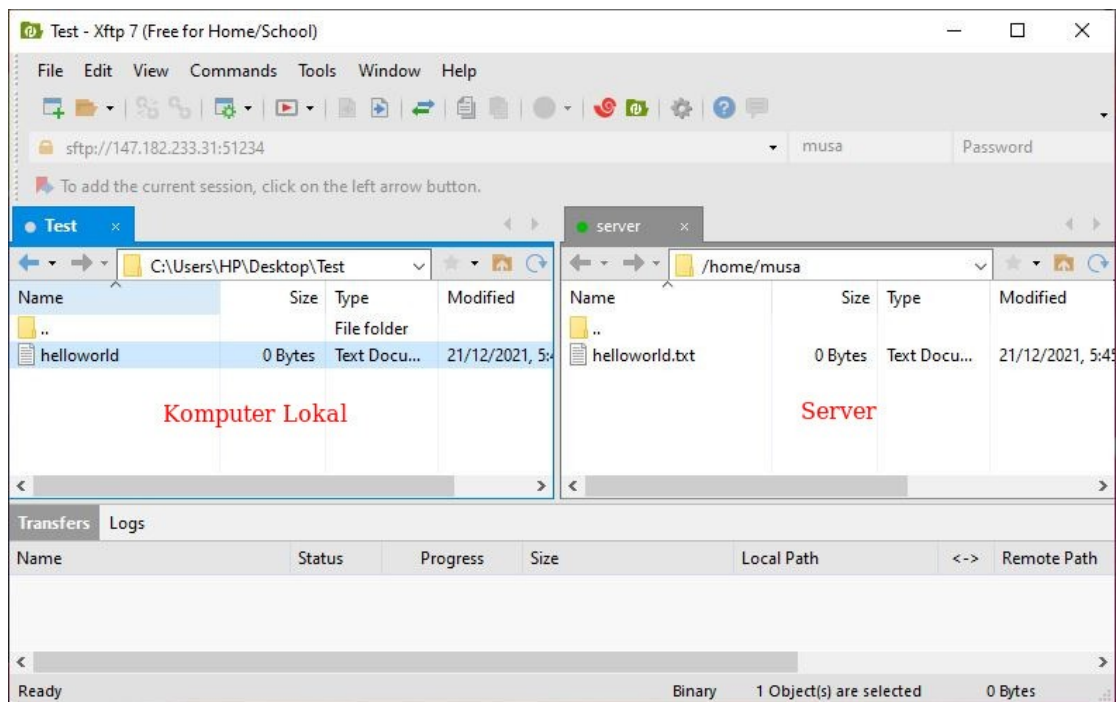
Core Features:
DDoS attack mitigation
Global Content Delivery Network
Support via community and developer documentation

Which plan is right for you? [Learn more](#).

[Continue](#)

Gambar 14. Paket Free layanan Cloudflare

3. Xftp terbuka dan login ke server sesuai dengan akses SSH yang digunakan di Xshell. Kolom sebelah kiri adalah data yang berada di lokal. Kolom sebelah kanan adalah data yang berada di server.
4. Untuk transfer file dari lokal ke server, klik kanan pada file yang ada di lokal yang ingin ditransfer dan pilih menu Transfer. Begitu juga sebaliknya untuk transfer file dari server ke lokal.



Gambar 37. Koneksi SFTP di Xftp

5. File yang ditransfer ke server tersimpan di folder home. File tersebut dapat dipindahkan ke folder lain sesuai dengan kebutuhan melalui SSH.

Transfer File di Linux

Transfer file di Linux dapat menggunakan SCP melalui command line. Misalnya transfer file.txt ke server dan dapat langsung memanfaatkan config dari SSH client. File yang ditransfer tersimpan di folder home.

```
scp file.txt server:~/
```

Untuk transfer direktori perlu menambahkan opsi `-r` untuk `recursive`.

```
scp -r folder-data server:~/
```

BAGIAN 6

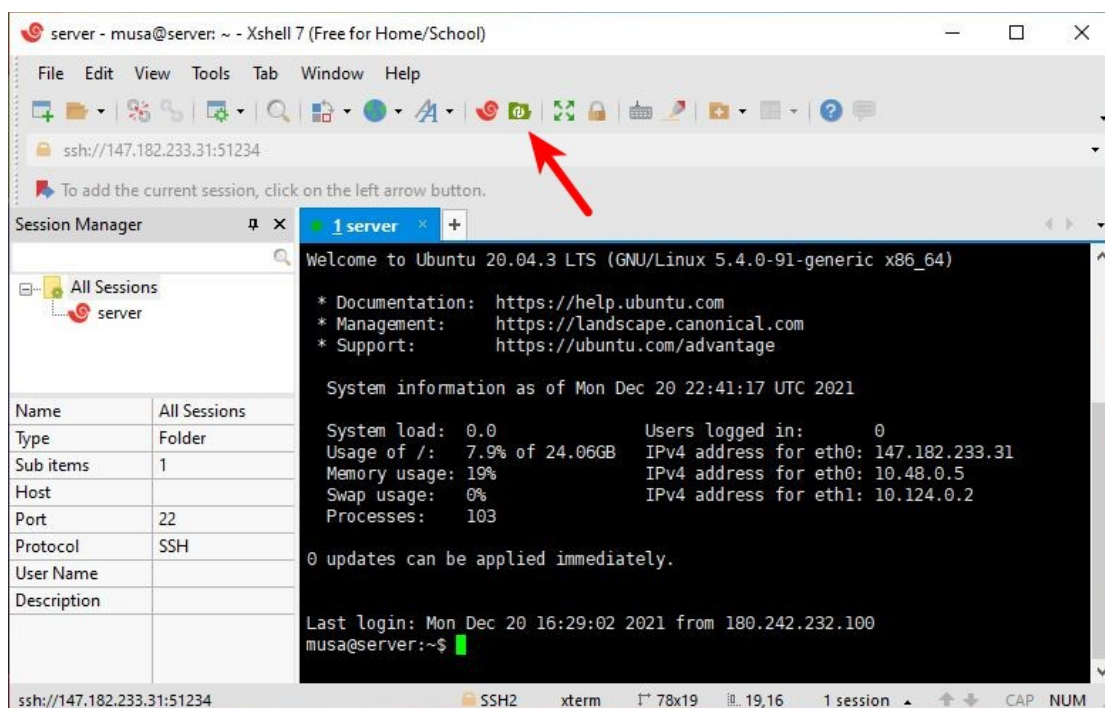
TRANSFER FILE

Fungsi utama dari SSH adalah untuk remote server, tetapi selain itu dapat berfungsi juga untuk melakukan transfer file antara komputer lokal (client) dengan server. Transfer file melalui SSH dapat dilakukan dengan menggunakan dua protokol yaitu SFTP (SSH File Transfer Protocol) dan SCP (Secure Copy Protocol).

Transfer File di Xftp

Xftp merupakan aplikasi FTP/SFTP client untuk Windows yang juga bagian dari produk NetSarang. Xshell dapat dikombinasikan dengan Xftp untuk memudahkan proses transfer file.

1. Buka Xshell dan login ke server.
2. Klik icon Xftp pada toolbar Xshell atau CTRL+ALT+F (New File Transfer) untuk membuka aplikasi Xftp dan langsung melakukan login ke server, siap untuk transfer file.



Gambar 36. Lokasi shortcut Xftp di Xshell

```
musa@laptop:~$ ssh server
```

```
musa@laptop:~$ ssh server
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

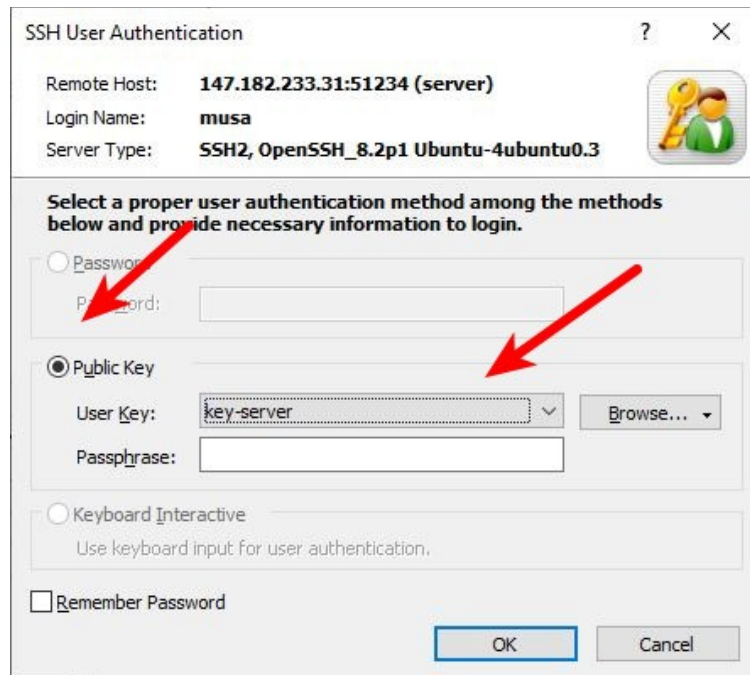
System information as of Mon Dec 20 16:29:01 UTC 2021

System load:  0.13           Users logged in:      1
Usage of /:   7.9% of 24.06GB IPv4 address for eth0: 147.182.233.31
Memory usage: 20%           IPv4 address for eth0: 10.48.0.5
Swap usage:   0%            IPv4 address for eth1: 10.124.0.2
Processes:   109

0 updates can be applied immediately.

Last login: Mon Dec 20 16:28:45 2021 from 180.242.232.100
musa@server:~$
```

Gambar 35. Login SSH dengan nama host



Gambar 34. SSH User Authentication dengan Public Key

Login SSH dengan Key di Linux

Untuk memudahkan login SSH dengan key di Linux tanpa harus mengetik perintah yang cukup panjang, gunakan file config SSH client.

1. Membuat file config di client.

```
musa@laptop:~$ nano .ssh/config
```

2. Masukkan konfigurasi yang berisi nama host, IP address, file private key, nomor port, dan user yang digunakan.

```
Host server
HostName 147.182.233.31
IdentityFile /home/musa/.ssh/key-server
IdentitiesOnly=yes
Port 51234
User musa
```

3. Login dengan perintah ssh diikuti dengan nama host sesuai yang telah dibuat di dalam file config.

Mengirim Public Key Secara Otomatis

Cara ini digunakan di Linux dan masih bisa login dengan memakai password. Jangan lupa tambahkan opsi `-p` jika sudah mengubah nomor port SSH.

```
ssh-copy-id -i ~/.ssh/key-server musa@147.182.233.31 -p 51234
```

Mengaktifkan Login SSH dengan Key

1. Buka file konfigurasi SSH server.

```
sudo nano /etc/ssh/sshd_config
```

2. Ubah nilai `PasswordAuthentication` menjadi `no`.

```
PasswordAuthentication no
```

3. Simpan.
4. Restart SSH service.

```
sudo systemctl restart ssh
```

Login SSH dengan Key di Xshell

Klik nama session server yang ingin di-remote, Xshell secara otomatis mendeteksi apakah metode authentication bisa menggunakan password atau harus menggunakan key. Pilih key yang telah dibuat dan telah dimasukkan ke server.

Membuat Key di Linux

1. Jalankan perintah `ssh-keygen`.
2. Masukkan path folder yang akan menjadi tempat penyimpanan file key. Defaultnya di `/home/user/.ssh` lalu diikuti dengan nama file key misalnya `key-server`.

```
musa@laptop:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/musa/.ssh/id_rsa):
/home/musa/.ssh/key-server
```

3. Tidak harus mengisi passphrase, Enter.
4. Hasil generate akan membuat dua buah file key yaitu private key (`key-server`) dan public key (`key-server.pub`). Tampilkan isi file public key dengan perintah `cat` dan copy isinya jika ingin menggunakan cara manual mengirim file public key ke server.

```
musa@laptop:~$ cat ~/.ssh/key-server.pub
```

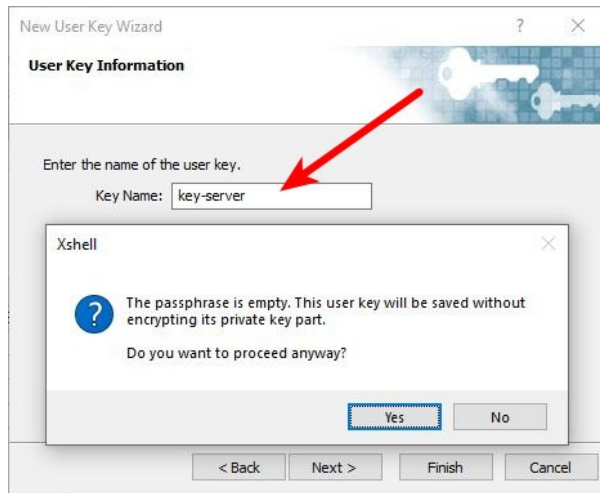
Mengirim Public Key Secara Manual

Public key harus dikirim atau disimpan di server, tepatnya di dalam folder `/home/user/.ssh` dengan nama file `authorized_keys`. Cara manual mengirim public key yaitu dengan membuat folder dan file yang dibutuhkan lalu paste public key yang telah di-copy sebelumnya. Cara ini digunakan jika memakai Windows client atau sudah tidak bisa lagi login dengan password.

1. Buat folder `.ssh` di dalam folder home.
2. Buat file `authorized_keys` dengan nano.
3. Paste public key lalu simpan dan keluar dari nano.
4. Ubah permission folder `.ssh` menjadi `700`.
5. Ubah permission file `authorized_keys` menjadi `600`.

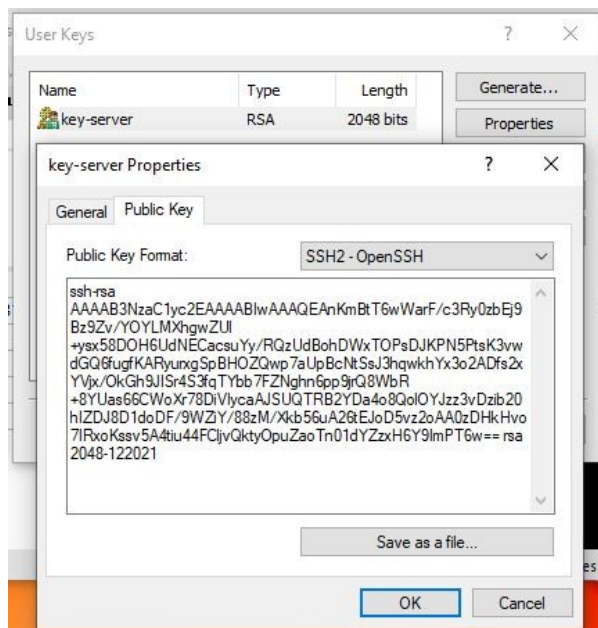
```
mkdir ~/.ssh
nano ~/.ssh/authorized_keys
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```


4. Berikan Key Name misal key-server, lalu Finish, Yes.



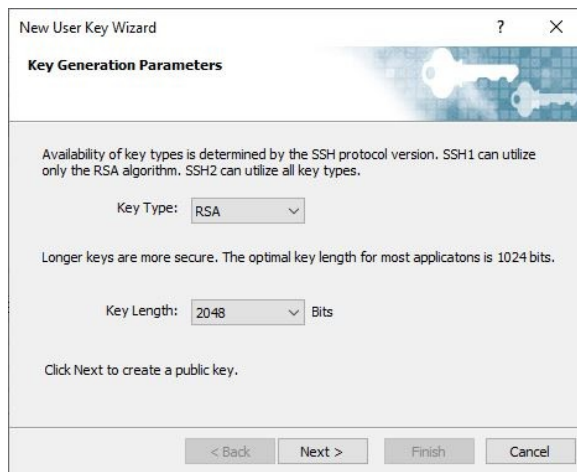
Gambar 32. Key name

5. Klik nama key, lalu Properties.
6. Klik tab Public Key, lalu copy key yang ada di kolom. Lalu OK, Close.



Gambar 33. Public Keys

2. Lalu Key Type dan Key Length pakai default saja, klik Next.



Gambar 30. Key Generation Parameters

3. Akan di-generate RSA key, setelah selesai klik Next.



Gambar 31. Generate Public Key

Membuat file konfigurasi WordPress `wp-config.php` yang memuat koneksi ke database.

```
sudo wp config create \  
--dbname="nama_db" \  
--dbuser="user_db" \  
--dbpass="pass_db" \  
--dbhost="localhost" \  
--allow-root
```

Menjalankan perintah instalasi, mendefinisikan URL akses WordPress, admin user, admin password, admin email, dan title website.

```
sudo wp core install \  
--url="https://www.domain.com" \  
--title="Judul Website" \  
--admin_user="admin_user" \  
--admin_password="admin_password" \  
--admin_email="admin@email.com" \  
--allow-root
```

Menghapus file `index.html` yang sebelumnya dibuat untuk pengujian virtual host.

```
sudo rm index.html
```

Mengubah ownership folder document root.

```
sudo chown -R www-data:www-data /var/www/domain.com
```

Menguji hasil instalasi WordPress, browse `http://domain.com`.

BAGIAN 11

WORDPRESS

[WordPress](#) adalah Content Management System (CMS) yang paling populer di dunia, dikembangkan dengan menggunakan bahasa pemrograman PHP dan MySQL/MariaDB database. WordPress dapat dimanfaatkan untuk berbagai kebutuhan jenis website seperti blog, media online, website profil perusahaan atau profil institusi pendidikan, sampai menjadi toko online.

Instalasi WordPress dengan WP-CLI

Semua kebutuhan untuk instalasi WordPress sudah terpasang, yaitu web server, database, PHP engine, dan domain yang dilengkapi dengan sertifikat SSL (HTTPS). Langkah selanjutnya adalah instalasi WordPress dengan menggunakan command line tool untuk WordPress yaitu WP-CLI.

[WP-CLI](#) adalah aplikasi tool WordPress berbasis command line interface yang berfungsi untuk melakukan setting WordPress, seperti install WordPress, manajemen plugin dan theme. WP-CLI dikembangkan dengan tujuan untuk membantu mempercepat alur kerja dari seorang WordPress developer.

Download `wp-cli.phar`.

```
sudo curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

Memberikan permission execute dan memindahkannya ke folder bin.

```
sudo chmod +x wp-cli.phar
sudo mv wp-cli.phar /usr/local/bin/wp
```

Berpindah ke folder document root.

```
cd /var/www/domain.com
```

Download WordPress core.

```
sudo wp core download --allow-root
```

```
server {  
    listen 80;  
    server_name www.domain.com domain.com;  
    return 301 https://www.domain.com$request_uri;  
}
```

Restart service Nginx.

```
sudo systemctl restart nginx
```

Browse <http://domain.com>, secara otomatis redirect ke <https://domain.com>.

Mengubah konfigurasi dengan menambahkan SSL dan redirect HTTP ke HTTPS.

```
server {  
    listen 443 ssl;  
    server_name www.domain.com domain.com;  
  
    ssl_certificate /etc/ssl/domain/domain.com-cert.pem;  
    ssl_certificate_key /etc/ssl/domain/domain.com-key.pem;  
    include /etc/ssl/options-ssl-nginx.conf;  
  
    root /var/www/domain.com;  
    index index.php index.html index.htm;  
  
    location / {  
        try_files $uri $uri/ /index.php?$query_string;  
    }  
  
    location ~ \.php$ {  
        try_files $fastcgi_script_name =404;  
        include fastcgi_params;  
        fastcgi_pass    unix:/run/php/php7.4-fpm.sock;  
        fastcgi_index  index.php;  
        fastcgi_param  DOCUMENT_ROOT    $realpath_root;  
        fastcgi_param  SCRIPT_FILENAME  $realpath_root$fastcgi_script_name;  
    }  
  
    access_log /var/log/nginx/domain.com_access.log;  
    error_log /var/log/nginx/domain.com_error.log;  
}
```

```
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI}
[END,NE,R=permanent]
</VirtualHost>
```

Mengaktifkan module SSL, rewrite, virtual host, dan restart Apache.

```
sudo a2enmod ssl rewrite
sudo a2ensite domain.com-ssl.conf
sudo systemctl restart apache2
```

Browse <http://domain.com>, secara otomatis redirect ke <https://domain.com>.

Konfigurasi SSL di Nginx

Membuat file `options-ssl-nginx.conf`.

```
sudo nano /etc/ssl/options-ssl-nginx.conf
```

Masukkan konfigurasi berikut.

```
ssl_session_cache shared:nginx_SSL:10m;
ssl_session_timeout 1440m;
ssl_session_tickets off;
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers off;

ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-
SHA384:ECDHE-RSA-AES128-SHA";
ssl_dhparam /etc/ssl/dhparam.pem;
```

Membuka file konfigurasi server block `domain.com.conf`.

```
sudo nano /etc/nginx/sites-available/domain.com.conf
```

Masukkan konfigurasi berikut.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName www.domain.com
    ServerAlias domain.com
    DocumentRoot /var/www/domain.com
    <Directory /var/www/domain.com>
        Options -Indexes +FollowSymLinks +MultiViews
        AllowOverride All
        Require all granted
    </Directory>
    ErrorLog /var/log/apache2/domain.com_error.log
    CustomLog /var/log/apache2/domain.com_access.log combined

    SSLCertificateFile /etc/ssl/domain.com/domain.com-cert.pem
    SSLCertificateKeyFile /etc/ssl/domain.com/domain.com-key.pem
    Include /etc/ssl/options-ssl-apache.conf
</VirtualHost>
</IfModule>
```

Membuka file konfigurasi virtual host port 80 (HTTP).

```
sudo nano /etc/apache2/sites-available/domain.com.conf
```

Menambahkan konfigurasi redirect HTTP ke HTTPS.

```
<VirtualHost *:80>
    ServerName www.domain.com
    ServerAlias domain.com

    RewriteEngine on
    RewriteCond %{SERVER_NAME} =www.domain.com
```


Di server, membuat file untuk Private Key, lalu paste keynya.

```
sudo nano /etc/ssl/domain.com/domain.com-key.pem
```

Di Cloudflare, klik OK.

Di server, generate dhparam.pem.

```
sudo openssl dhparam -out /etc/ssl/dhparam.pem 2048
```

Konfigurasi SSL di Apache

Membuat file options-ssl-apache.conf.

```
sudo nano /etc/ssl/options-ssl-apache.conf
```

Masukkan konfigurasi berikut.

```
SSL Engine on
SSLProtocol          all -SSLv2 -SSLv3
SSLCipherSuite       ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-
CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-
AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-
AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-
AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-
RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-
SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
SSLHonorCipherOrder  on
SSLCompression       off
SSLOptions +StrictRequire
SSLOpenSSLConfCmd    DHParameters "/etc/ssl/dhparam.pem"
```

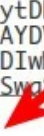
Membuat file konfigurasi virtual host untuk port 443 (HTTPS).

```
sudo nano /etc/apache2/sites-available/domain.com-ssl.conf
```

Lalu copy Origin Certificate dengan mengklik Click to copy.

Origin Certificate

```
-----BEGIN CERTIFICATE-----
MIIEqDCCA5CgAwIBAgIU50cMF2IcIsVPKHCUSqixasn900wDQYJKoZIhvcNAQEL
BQAwYsxCzAJBgNVBAYTA1VTMRkwFwYDVQQKEwBDbG91ZEZsYXJlLCBjb20wMTQw
MgYDVQQLZy9DbG91ZEZsYXJlIE9yaWdpbiBTU0wgQ2VydG1maWNhdGUgQXV0aG9y
aXR5MRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRMwEQYDVQIEwPDYXpZm9ybmlh
MB4XDTEyMDIwMzA0MjUwMjUwMjUwMjUwMjUwMjUwMjUwMjUwMjUwMjUwMjUwMjUw
dWRGbGFvZS9wS15iLiEdMBSGA1UECXMUO2xvdWRGbGFvZS9wS15iLiEdMBSGA1
UEChMQQ2xv
```

Click to copy 

Gambar 52. Origin Certificate

Di server, membuat folder untuk menyimpan SSL.

```
sudo mkdir /etc/ssl/domain.com
```

Lalu membuat file dengan nano, paste Origin Certificate.

```
sudo nano /etc/ssl/domain.com/domain.com-cert.pem
```

Di Cloudflare, copy Private Key.

Private Key

Copy the contents of your private key below to your web server and set file permissions such that only your http server can access it. Additionally, you can optionally encrypt this file and provide a password to decrypt it during your origin web server startup. The private key data will not be stored at Cloudflare and will no longer be accessible once the creation is complete. Please make sure you have a local copy of this key.

```
-----BEGIN PRIVATE KEY-----
0mCnqSQ5sDuwRGEjsQBzuMRX7zscFRJZYjxG5q0x+0xwGUBK1J9neDpLQpIeGZ6Z
0cOR/qB4g04AEY5bJ0w/wURmvU/U1PEECuQ/sMafAoGAJ7dzewsT4HeS0D8fJ0kp
3JjhIcjpRSmvCtfxk7w/nGLqFaGxboP06aGzyByoDTLp41mPE08CUA8Sd0Bo8exq
6U4IwXWG/irPavj86ORL3yMA2o1JpCod2iwX1h9FnZYGxsLL50fKbHphH/5Vshz
rvzDqJjirv+YQDakIpzW65s=
-----END PRIVATE KEY-----
```

Click to copy 

Web Server for Installation

For installation instructions specific to your type of origin web server, visit our support guide on [managing Origin CA certificates](#).

OK 

Gambar 53. Private Key

Masukkan scriptnya.

```
#!/bin/bash
clear
cd /var/www
tar czvf /backup/domain.com/domain.com-$(date +%d%m%Y).tar.gz
domain.com
mysqldump --defaults-extra-file=/backup/nama_db.cnf nama_db | gzip
> /backup/domain.com/nama_db-$(date +%d%m%Y).sql.gz
find /backup/domain.com -type f -mtime +1 -delete
```

Proses yang dikerjakan oleh script di atas adalah membuat backup file website dan database dalam format kompresi .tar.gz. Nama filenya ditambahkan tanggal backup sehingga tidak tertimpa file backup sebelumnya, misalnya mau backup per hari. Baris paling akhir, menghapus file backup yang umurnya sudah lewat satu hari agar tidak terlalu banyak menyimpan file backup yang dapat mengakibatkan disk kepenuhan.

Mengubah permission backup-local.sh.

```
chmod 700 /backup/backup-local.sh
```

Menjalankan backup-local.sh.

```
/backup/backup-local.sh
```

Memverifikasi hasil backup dengan cara menampilkan isi folder backup.

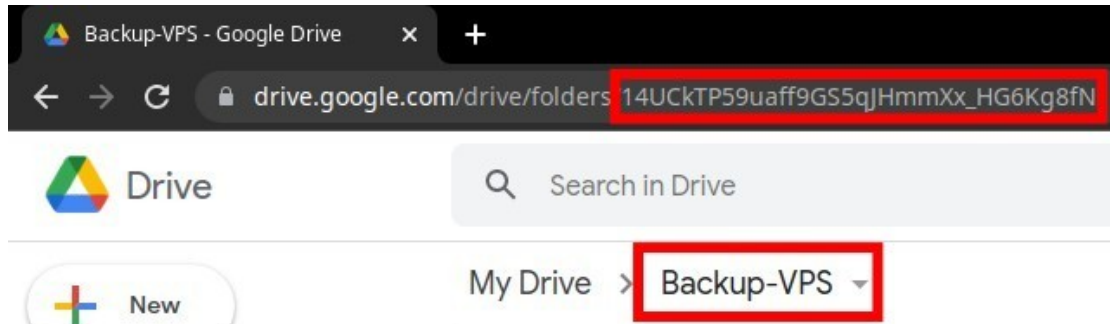
```
ls -lh /backup/domain.com
```

Backup ke Google Drive

Setelah backup ke local disk berhasil, selanjutnya mentransfer file hasil backup ke Google Drive. Untuk backup ke Google Drive menggunakan [rclone](#) dan bash script.

Install rclone

1. Browse [Google Drive](#), buat folder misal Backup-VPS.
2. Masuk ke folder Backup-VPS, lihat folder ID di address bar. Folder ID tersebut nantinya dibutuhkan pada saat konfigurasi rclone.



Gambar 72. Folder Backup-VPS di Google Drive

3. Install rclone di server

```
curl https://rclone.org/install.sh | sudo bash
```

4. Install juga rclone di PC desktop untuk kebutuhan authorize ke Google Drive.
5. Membuat konfigurasi rclone.

```
rclone config
```

5. Hasilnya seperti di bawah ini. Jawab n untuk membuat New remote.

```
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
```

6. Masukkan nama remotenya, misal my-gdrive.

```
name> my-gdrive
```

7. Memilih cloud storage provider, masukkan 17 untuk Google Drive. Nomor ini dapat berubah, tergantung versi rclone yang digunakan.