

VPS Debian 12

Usando Contabo



Ribamar FS

Abril/2024

<https://ribamar.net.br>

Sumário

Introdução.....	3
Público Alvo.....	3
Sobre o Autor.....	3
1 - Planejamento para o servidor e os sites.....	5
2 - Contratação do domínio.....	6
3 - Contratação da hospedagem.....	7
4 - Alerta de Problemas.....	9
5 - Configurar o servidor VPS.....	10
5.1 - Atualizar.....	10
5.2 - Alguns ajustes iniciais.....	10
5.3 - Configurar o SSH e o ufw.....	12
6 - Configurações do DNS.....	14
7 - Instalação e configurações do EMP.....	16
7.1 - Criação dos blocos do Nginx.....	17
8 - Permissões do /var/www.....	21
9 - SSL com Certbot.....	22
10 - Criação dos bancos de dados.....	24
11 - Backups.....	25
12 - Criação de scripts e aliases.....	27
13 - Recomendações Extras de segurança.....	28
14 - Monitoramento do Servidor.....	29
14.1 - Alguns comandos via terminal no servidor.....	29
14.2 - Lynis.....	29
14.3 - Fail2Ban.....	30
14.4 - Usando a ferramenta htop.....	31
15 - Criação e configuração dos sites.....	33
16 - Dicas sobre PHP.....	34
17 - Códigos deste e-book no Github.....	35
18 - Informações sobre a Contabo.....	36
19 - Ferramentas.....	38
19.1 - nano - Editor de texto para o terminal.....	38
19.2 - mc - Gerenciador de arquivos para o terminal.....	39
19.3 - Compactação de arquivos.....	41
19.4 - Gerenciamento de pacotes com apt.....	41
19.5 - Alguns comandos.....	41
19.6 - Atualizações de segurança automáticas.....	43
20 - Referências.....	44
21 - Conclusão.....	45

Introdução

O objetivo principal da elaboração deste e-book é fornecer, primeiro para mim (para servir de roteiro para meus projetos), e, depois de testado algumas vezes, também para outras pessoas interessadas, um roteiro prático para a criação de um servidor tipo VPS e nele criar alguns sites com o CMS Joomla usando boas práticas e tomando cuidado com a segurança, tanto do servidor quanto dos sites. Aqui estarei relatando os passos simples de cada atividade. Além do e-book, como PDF não guarda bem código a ser copiado e colado, então criei um repositório no Github (<https://github.com/ribafs2/vps>) para guardar todo o código do e-book. Também criei um vídeo, tendo como roteiro este e-book mostrando a criação do VPS em detalhes.

Público Alvo

Este pequeno manual destina-se a quem está usando uma hospedagem compartilhada e deseja ter mais liberdade e mais controle sobre seu servidor. Com um servidor tipo VPS temos praticamente controle total sobre o servidor. Se quisermos instalara Apache ou Nginx, instalar MySQL ou PostgreSQL, se quisermos instalar qualquer que seja a extensão e versão do PHP. É você quem decide. Mas é importante saber que todo o gerenciamento é por sua conta, instalar e configurar um firewall, configurar o SSH e numa porta desejada. O suporte oferecido pelo serviço que contratamos praticamente deve ser esquecido, você está por sua conta.

Isso que falei acima mostra que se você quer ter conforto deve ficar com as hospedagens compartilhadas, mas se tem disposição para aprender e quer pagar o preço para ter um grande controle sobre seu servidor, então estamos aqui para ajudá-lo. Se decidir usar VPS lembre-se que precisa ser um autodidata e estudar muito. Não desista nas primeiras dificuldades e se tornará um profissional melhor e mais valorizado no mercado.

Pra valer, público-alvo é qualquer pessoa interessada, pois está disponível para todos.

Sobre o Autor

Sou o ribafs/Ribamar FS, um apaixonado pela programação web com PHP, por Linux e pela administração de servidores linux.

Participo ativamente em diversos grupos de discussão no Facebook

Estudo e trabalho com TI há uns 30 anos.

Um currículo não atualizado

<https://ribafs.github.io/sobre/curriculo/>

Meu site atual, criado num VPS no Contabo. Meu pequeno laboratório criado com Joomla:

<https://ribamar.net.br/>

Outros livros meus (todos free)

<https://ribafs.github.io/sobre/livros/>

Este treinamento está sendo publicado de uma forma diferente. Inteiramente gratuito. Apenas com sugestão de doação. Mas, sinceramente, gostaria de receber doações somente de quem sentir vontade de fazê-lo, daqueles que perceberem que está sendo útil e está podendo fazê-lo. Este livro é bem prático, com receitas de bolo e pouca teoria.

Debian 12

Ao final de uma instalação básica percebo que o Debian ocupa um espaço menor em disco e consome menos memória RAM e isso me faz preferir o Debian, especialmente com servidor usando poucos recursos, mas não somente.

1 - Planejamento para o servidor e os sites

Esta etapa é bem importante. Pode ser feita num papel ou num arquivo texto do computador. Precisamos fazer um planejamento do domínio, do servidor, dos sites, dos aplicativos, etc. Este planejamento deve ser mais detalhado e organizado se o projeto for importante. Para um projeto pessoal este planejamento pode ser mais simples, mas também é importante.

Este planejamento também será importante para ser usado como roteiro na criação do servidor e dos sites. Caso esta primeira etapa seja elaborada com bastante critério e cuidado, não acontecerá no futuro que tenha esquecido algo importante e tenha que fazer um grande trabalho para resolver.

2 – Contratação do domínio

Registrar o domínio ou os domínios a serem usados nos sites é bom que seja a primeira providência. Precisamos ficar atentos e anotar as informações necessárias para gerenciar os domínios, pois quando mais a frente, contratar a hospedagem precisaremos voltar para a administração dos domínios para apontar os nameservers da hospedagem.

A minha sugestão vai para o serviço de registro de domínio brasileiro, registro.br. Porque pagamos uma anuidade e geralmente não temos surpresas ao renovar o domínio, visto que algumas empresas se aproveitam e aumentam exageradamente a anuidade.

3 - Contratação da hospedagem

Veja que este e-book está trabalhando com um VPS hospedado na Contabo.com. Praticamente qualquer outra empresa, que ofereça acesso via SSH, pode ser usada para seguir o roteiro deste livro. Nem vou citar as vantagens que vi na Contabo, pois sei que alguns colegas tem preferências diferentes e tá tudo bem.

Quando contratamos a Contabo recebemos um e-mail com os dados para acessar a administração.

Na administração podemos criar de fato o VPS já escolhendo a distribuição e entrando com uma senha para o usuário root. Com isso podemos acessar o servidor pelo nosso desktop via SSH.

Contratar o plano VPS 1 no Contabo. Características:

- 4 vCPU cores
- 6 GB de RAM
- 100 GB de disco NVMe ou 400 GB SSD
- 1 Snapshot
- 32 TB de tráfego

Criar server com Debian 12

Após atualizar criar um Snapshot e ficar atualizando a cada atualização do servidor

<https://my.contabo.com/>

VPS Control

Snapshot

Clicar no botão abaixo

Create Snapshot

Debian12-07042024-7h

Sublinhado não vale

Em caso de problema podemos restaurar

<https://my.contabo.com/>

VPS Control

Snapshot

Clicar no botão abaixo

Clicar em Rollback

VPS Control

Install/Reinstall

Após contratar um plano de VPS na Contabo e receber o acesso ao site de administração, podemos então cadastrar cada um dos domínios que iremos usar em nossos sites, como também os sub-domínios:

<https://my.contabo.com>

Clicar em
DNS Zone Management

Exemplo

Domain – ribamar.net.br

Target IP address – Selecionar o IP que foi reservado para seu VPS

Clicar em Create zone

Com isso ele mostra acima os nameservers da Contabo

ns1.contabo.net (79.143.182.242, 2a02:c205:0:0882::1)

ns2.contabo.net (178.238.234.231, 2a02:c205:0:0891::1)

ns3.contabo.net (5.189.191.29, 2a02:c207:0:0842::1)

Precisamos anotar estes e levar para a administração do domínio para apontar para eles.

Abaixo aparece o domínio que está registrado agora no Contabo. Então podemos adicionar registros ao DNS. Para isso, abaixo, clicamos no botão com um lápis à direita do nome do domínio.

Importante Lembre que para implementar o SSL precisa esperar que o domínio seja propagado. Detalhes mais a frente.

Precisamos repetir os passos acima para cada domínio adicional e também para todos os subdomínios. Lembrando, que os subdomínios não precisam ser registrados na administração do domínio, mas apenas aqui na administração da Contabo e também no Nginx.

Registros do DNS

Criar os registros necessários: CNAME para criar www para cada domínio, Registro A para cada domínio.

4 – Alerta de Problemas

Dois grandes problemas que tenho encontrado com VPS

Uso de chaves SSH para acesso ao Servidor

Perdi alguns servidores por conta disso, por usar chaves do SSH para configurar o SSH na hospedagem.

Uma beleza de solução e bem confiável. Mas quando eu fazia algo de que gosto de fazer, formatar o micro e instalar uma nova versão da distribuição Linux em meu desktop, então perdia o acesso ao servidor. Continuava tudo funcionando, mas eu não mais acessava o servidor.

Nenhuma vez o suporte me ajudou em relação a isso. Pesquisando descobri que existe como fazer um backup da chave do SSH para poder usar no novo sistema do desktop, mas cancei de procurar e desisti.

Restringir acesso somente ao seu IP no firewall

Com a intenção de melhorar a segurança do servidor, acabo de configurar o firewall para que somente aceite conexão em certa porta e somente do meu IP externo.

Acontece que uso internet do tipo ADSL, que muda o IP de vez em quando e sem aviso. Acabo de perder o acesso ao meu servidor. Então, para quem usa uma internet cujo IP pode mudar não pode usar este reforço da segurança no firewall.

Ainda bem que tenho backup de tudo e um roteiro para a reinstalação.

5 - Configurar o servidor VPS

5.1 – Atualizar

Pelo seu desktop acesse o servidor via SSH

```
ssh root@IP
```

Após receber o prompt da Contabo, execute:

```
apt update
```

```
apt upgrade -y
```

```
reboot
```

Geralmente não existe a necessidade de reiniciarmos um linux, mas geralmente acontece de atualizarmos e instalarmos novos kernels. Então, para que o novo kernel instalado seja usado, precisamos reiniciar o servidor.

Aguarde alguns segundos antes de conectar novamente...

5.2 – Alguns ajustes iniciais

Acessar com

```
ssh root@IP
```

Checar versão do SO

```
cat /etc/issue - Debian 12
```

Ajuste do timezone

```
timedatectl set-timezone "America/Fortaleza"
```

Verificar espaço livre e total

```
df -h  
96G 2.0G 90G 3% /
```

Verificar a memória

```
free -m  
Mem:      5924      258      5757      7      75      5665  
Swap:      0          0          0
```

Criação da swap

```
fallocate -l 1G /swapfile  
chmod 600 /swapfile  
mkswap /swapfile  
swapon /swapfile
```

```
nano /etc/fstab
```

Adicione ao final
/swapfile swap swap defaults 0 0

Verificar novamente

```
free -m  
Mem:      5924    260    5753     7     78    5663  
Swap:     1023     0    1023
```

Criar user regular

```
adduser ribafs
```

Instalar sudo e ufw (firewall)

```
apt install sudo ufw -y
```

Adicionar meu user ao grupo do sudo, para que seja privilegiado

```
adduser ribafs sudo
```

Testar

```
su - ribafs  
sudo clear  
exit
```

Adicionar meu user para o grupo do Nginx

```
adduser ribafs www-data
```

5.3 – Configurar o SSH e o ufw

É importante configurar SSH e ufw sem reiniciar o SSH, pois se mudarmos a porta do SSH e reiniciar o SSH perderemos o acesso ao servidor, então mudamos a porta, permitimos essa porta no ufw e assim estamos bem. Já aconteceu comigo de mudar a porta do SSH, reiniciar o mesmo antes de ajustar as portas no UFW e assim perder o acesso ao VPS.

Execute as configurações do SSH e do ufw com bastante atenção. Caso contrário perderá o acesso ao servidor.

Configurar o SSH

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

```
Port 60222
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 3
X11Forwarding no
AllowUsers ribafs
```

Configurar o firewall

Abrir somente estas 3 portas, todas as demais ficarão fechadas.

```
ufw allow 60522
ufw allow 80
ufw allow 443
```

```
ufw enable
y
ufw status verbose
```

```
Status: active
Logging: on (low) - iniciar no boot
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
--	-----	----
60222	ALLOW IN	Anywhere
80	ALLOW IN	Anywhere
443	ALLOW IN	Anywhere
60222	ALLOW IN	177.37.233.89
60222 (v6)	ALLOW IN	Anywhere (v6)
80 (v6)	ALLOW IN	Anywhere (v6)
443 (v6)	ALLOW IN	Anywhere (v6)

Importante: podemos melhorar a segurança através do firewall, mas somente se usarmos um IP externo que seja fixo:

```
ufw allow from 177.37.233.89 to any port 60222
```

Assim somente podemos acessar o servidor via SSH se estivermos com o referido IP

```
service ssh restart
```

Caso queira remover regras do ufw

```
sudo ufw status numbered
```

```
sudo ufw delete 4
```

```
exit
```

6 – Configurações do DNS

Registrar cada domínio na hospedagem e com os nameservers do Contabo apontá-los na administração dos domínios.

Criação dos registros A no DNS para cada subdomínio na hospedagem

Como criar um registro A para um subdomínio no Contabo

Como saber se o domínio propagou?

No linux eu gosto de usar um comando `host` no terminal para saber se o domínio já propagou:

```
host ribamar.net.br
```

Caso já tenha propagado ele me mostra o domínio e o IP associado a ele.
`ribamar.net.br has address 64.23.165.38`

Também existem alguns serviços online que mostram ainda mais detalhes.
O que mais uso é este:

<https://www.whatsmydns.net/>

Você digita o domínio e clica em Search. Veja que o registro tipo A já está selecionado.
Obs: Para que configuremos o SSL com o Certbot, há necessidade de o domínio já ter propagado.

- Acessar o admin
 - DNS Zone Management
- Abaixo, à direita do nome do domínio, clicar no bloco de notas

Abaixo

```
Name - frangomontese.com.br
Type - A
Data - 84.247.172.72
```

```
Name - www.frangomontese.com.br
Type - CNAME
Data - frangomontese.com.br
```

```
Name - blog.ribamar.net.br
Type - A
Data - 84.247.172.72
Create record
blog.ribamar.net.br 86400 A 0 84.247.172.72
```

Name - www.blog.ribamar.net.br
Type - CNAME
Data - blog.ribamar.net.br

Name - material.ribamar.net.br
Type - A
Data - 84.247.172.72
(Este é criado somente para abrigar um redirecionamento para o site no GH)

Name - eletrotekcellfortaleza.ribamar.net.br
Type - A
Data - 84.247.172.72

Name - testes.ribamar.net.br
Type - A
Data - 84.247.172.72

7 – Instalação e configurações do EMP

Instalação e configurações do EMP (Nginx, MariaDb, PHP e cia).

Conectar ao servidor, agora com o user regular e por uma outra porta, diferente da 22, que é a default

```
ssh -p 60222 ribamarfs@84.247.172.72
```

```
sudo apt update  
sudo apt upgrade -y
```

Instalar o Nginx

```
sudo apt install nginx -y
```

Testar no navegador

<http://IP>

Instalar MariaDb

```
sudo apt install mariadb-server -y
```

Melhorar a segurança do MariaDb

```
sudo mysql_secure_installation
```

Testando

```
mysql -uroot -p
```

Para adicionar suporte ao PHP no Nginx

Instalar e usar o PHP-FPM para executar arquivos PHP

```
sudo apt install aptitude git composer mc curl phpunit ssh imagemagick zip unzip -y  
sudo apt install php-fpm php-mysql php-gd php-cli php-curl php-mbstring php-zip php-opcache  
php-xml php-bcmath php-pear php-imagick php-tidy php-xmlrpc php-intl php-xdebug php-apcu php-redis -y  
sudo mkdir -p /etc/apt/keyrings
```

```
NODE_MAJOR=20
```

```
echo "deb [signed-by=/etc/apt/keyrings/nodesource.gpg]
```

```
https://deb.nodesource.com/node_${NODE_MAJOR}.x nodistro main" | sudo tee  
/etc/apt/sources.list.d/nodesource.list
```

```
sudo apt update
```

```
sudo apt install nodejs -y
```

```
sudo apt update && sudo apt install -y yarn
```

7.1 – Criação dos blocos do Nginx

Para os sites com domínios e subdomínios

default - /var/www/html – ribamar.net.br e www.ribamar.net.br

blog - /var/www/blog – blog.ribamar.net.br e www.blog.ribamar.net.br

material - /var/www/material – material.ribamar.net.br (redirecionar para o GH)

eletro - /var/www/eletro - eletro.ribamar.net.br

```
cd /etc/nginx/sites-available
```

```
sudo rm default
```

```
sudo nano default
```

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/html;
    index index.html index.php;
    server_name ribamar.net.br www.ribamar.net.br;

    location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    }
}
```

Para o default não há necessidade de criar o link simbólico

```
sudo nano blog
```

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/blog;
    index index.html index.php;
    server_name blog.ribamar.net.br www.blog.ribamar.net.br;

    location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    }
}
```

```
sudo ln -s /etc/nginx/sites-available/blog /etc/nginx/sites-enabled/blog
```

Observe que o default não precisa de link simbólico.

```
sudo nano eletro
```

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/eletro;
    index index.html index.php;
    server_name eletro.ribamar.net.br www.eletro.ribamar.net.br ;

    location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    }
}
```

```
sudo ln -s /etc/nginx/sites-available/eletro /etc/nginx/sites-enabled/eletro
```

```
sudo nano material
```

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/material;
    index index.html index.php;
    server_name material.ribamar.net.br www.material.ribamar.net.br ;

    location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    }
}
```

```
sudo ln -s /etc/nginx/sites-available/material /etc/nginx/sites-enabled/material
```

Adicionar um novo domínio

Caso queira adicionar um segundo domínio neste mesmo servidor, precisa adicionar seus dois registros ao DNS da hospedagem e adicionar o bloco/subdomínio ao Nginx, como a seguir:

```
sudo nano frango
```

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/frango;
    index index.html index.php;
    server_name frangomontese.com.br www.frangomontese.com.br;

    location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
    }
}
```

```
sudo ln -s /etc/nginx/sites-available/frango /etc/nginx/sites-enabled/frango
```

Testar a sintaxe dos blocos

```
sudo nginx -t
```

Reiniciar o Nginx

```
sudo systemctl restart php8.2-fpm nginx
```

Criar pastas

```
sudo mkdir /var/www/blog  
sudo mkdir /var/www/eletro  
sudo mkdir /var/www/material
```

Configurar material para o redirecionamento

```
cd /var/www/material
```

Criar arquivo que redirecionará todos os acessos de material.ribamar.net.br para o Github. Acontece que o site material esteve algum tempo no ar e pode ser que alguém o procure, no caso será redirecionado para o GH.

```
sudo nano index.php
```

```
<?php  
header('location: https://ribafs2.github.io/material/');
```

Se tudo correr bem não mostra nenhuma mensagem na tela. Antes de acessar ajuste as permissões e implemente o SSL.

8 - Permissões do /var/www

É muito importante ter um bom ajuste das permissões da pasta web.

Setar as permissões dos arquivos da pasta /var/www

Ao copiar ou criar arquivos/pastas dentro da pasta (exemplo: /var/www/html) o(s) arquivos herdarão as permissões da pasta.

Evite mover arquivos para o /var/www, pois assim eles herdam as permissões originais e precisará executar o script perms.

```
sudo nano /usr/local/bin/perms
```

```
#!/bin/sh
clear;
echo "Aguarde enquanto configuro as permissões do /var/www/$1";
echo "";
chown -R www-data:www-data /var/www/$1;
find /var/www/$1 -type d -exec chmod 775 {} \;
find /var/www/$1 -type f -exec chmod 664 {} \;
find /var/www/$1 -type d -exec chmod g+s {} \;
echo "";
echo "Concluído!";
```

```
sudo chmod +x /usr/local/bin/perms
```

Usando

```
sudo perms (varre toda a /var/www)
sudo perms html(varre /var/www/html)
```

9 - SSL com Certbot

Atualmente é muito importante usar SSL em nossos sites. Especialmente em páginas que autenticam os usuários, sem SSL a senha trafegará pela internet, do seu desktop até o servidor, em texto claro. Com SSL ela irá criptografada.

Configuração do SSL com Certbot

O Certbot é uma ótima opção para adicionar SSL free no Servidor. Ótimo não somente por ser free mas por ser bem prático de instalar.

Acessamos o site

<https://certbot.eff.org/>

Rolamos um pouco a tela e em Software selecionamos Nginx System selecionamos Debian Testing

Rolar a tela e seguir os passos.

<https://certbot.eff.org/instructions?ws=nginx&os=debiantesting>

Já tenho aqui os comandos então

```
sudo apt update
sudo apt install snapd -y
sudo snap install --classic certbot
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

Configurar o SSL

```
sudo certbot --nginx
```

Entre com seu e-mail

Y

Y

Enter

para todos

Deploying certificate

Successfully deployed certificate for frangomontese.com.br to /etc/nginx/sites-enabled/frango

Successfully deployed certificate for www.frangomontese.com.br to /etc/nginx/sites-enabled/frango

Successfully deployed certificate for ribamar.net.br to /etc/nginx/sites-enabled/default

Successfully deployed certificate for blog.ribamar.net.br to /etc/nginx/sites-enabled/blog

Successfully deployed certificate for www.blog.ribamar.net.br to /etc/nginx/sites-enabled/blog

Successfully deployed certificate for material.ribamar.net.br to /etc/nginx/sites-enabled/material

Successfully deployed certificate for www.ribamar.net.br to /etc/nginx/sites-enabled/default

Congratulations! You have successfully enabled HTTPS on <https://frangomontese.com.br>, <https://www.frangomontese.com.br>, <https://ribamar.net.br>, <https://blog.ribamar.net.br>, <https://www.blog.ribamar.net.br>, <https://material.ribamar.net.br>, and <https://www.ribamar.net.br>

If you like Certbot, please consider supporting our work by:

** Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>*

** Donating to EFF: <https://eff.org/donate-le>*

Renovação automática

```
sudo certbot renew --dry-run
```

Testar a sintaxe dos blocos do Nginx

```
sudo nginx -t
```

Reiniciar

```
sudo systemctl restart php8.2-fpm nginx
```

Adicionar novo domínio

Caso venha a adicionar novo domínio ou subdomínio precisa executar

```
sudo certbot --nginx
```

Quando perguntado sobre se (E)xpand ou (C)ancela

Digite E e Enter para expandir

Então execute

```
sudo certbot renew --dry-run
```

Para evitar isso, é melhor que faça um bom planejamento de que domínios e subs irá usar no início.

10 – Criação dos bancos de dados

Por uma questão de organização e também para reforçar a segurança dos sites, eu sempre crio um banco de dados e um usuário que é o dono do banco para cada site.

Minhas regras para melhor memorizar. nome_db, nome_us, onde nome é o nome da pasta do site.

Criaremos 5 bancos e seus 5 respectivos usuários:

```
sudo mysql
```

```
create database ribamar_db CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'ribamar_us'@'localhost' IDENTIFIED BY 'zmxn1029R@';
GRANT ALL PRIVILEGES ON ribamar_db.* TO 'ribamar_us'@'localhost' WITH GRANT
OPTION;
```

```
create database blog_db CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'blog_us'@'localhost' IDENTIFIED BY 'zmxn1029B@';
GRANT ALL PRIVILEGES ON blog_db.* TO 'blog_us'@'localhost' WITH GRANT OPTION;
```

```
create database eletro_db CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'eletro_us'@'localhost' IDENTIFIED BY 'zmxn1029E@';
GRANT ALL PRIVILEGES ON eletro_db.* TO 'eletro_us'@'localhost' WITH GRANT OPTION;
```

```
create database material_db CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'material_us'@'localhost' IDENTIFIED BY 'zmxn1029M@';
GRANT ALL PRIVILEGES ON material_db.* TO 'material_us'@'localhost' WITH GRANT
OPTION;
```

```
create database frango_db CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'frango_us'@'localhost' IDENTIFIED BY 'zmxn1029F@';
GRANT ALL PRIVILEGES ON frango_db.* TO 'frango_us'@'localhost' WITH GRANT OPTION;
```

```
\q
```

11 – Backups

Uma das medidas de segurança mais importantes. Lembre que além de criar o backup também deve se certificar de que ele está funcionando. Para isso restaure em seu desktop.

Backups são imprescindíveis para eventuais restauração

Uma das providências mais importantes em termos de segurança na web, backup dos arquivos e do banco de dados. A frequência deve ser diretamente proporcional à importância do site ou aplicativo.

Um exemplo de script que uso para efetuar backup de um site:

```
mkdir /home/ribafs/backups
```

```
nano /home/ribafs/backup.sh
```

```
mysqldump -uroot -pzmxn1029M@ ribamar_db > /home/ribafs/backups/ribamar_$(date +"%Y_%m_%d").sql
mysqldump -uroot -pzmxn1029M@ blog_db > /home/ribafs/backups/blog_$(date +"%Y_%m_%d").sql
mysqldump -uroot -pzmxn1029M@ eletro_db > /home/ribafs/backups/eletro_$(date +"%Y_%m_%d").sql
mysqldump -uroot -pzmxn1029M@ material_db > /home/ribafs/backups/material_$(date +"%Y_%m_%d").sql
cd /var/www/
zip -rq /home/ribafs/backups/ribamar_$(date +"%Y_%m_%d").zip html
zip -rq /home/ribafs/backups/blog_$(date +"%Y_%m_%d").zip blog
zip -rq /home/ribafs/backups/eletro_$(date +"%Y_%m_%d").zip eletro
zip -rq /home/ribafs/backups/material_$(date +"%Y_%m_%d").zip material
```

Veja que eu salvo na pasta /home/ribafs/backups e depois baixo dela para o meu desktop.

Com este sufixo

```
_$(date +"%Y_%m_%d")
```

Temos um backup por dia. Caso queira uma frequência maior, use algo como:

```
_$(date +"%Y_%m_%d:%H:%i")
```

Backup diário e automático

Para isso podemos usar o cron e criar um script para backup em

Dar permissão de execução para ele:

```
chmod +x /home/ribafs/backup.sh
```

```
crontab -e
```

Adicionar ao final:

```
0 2 * * * /home/ribafs/backup.sh
```

Assim ele fará automaticamente o backup todos os dias as 2 horas da manhã.

O script backupdia deve conter tudo que desejamos fazer o backup diariamente. Depois veremos como copiar o conteúdo da pasta backup para o desktop.

Importância do Backup

Ao meu ver o backup é uma das providências mais importantes em termos de segurança, pois se por algum motivo perder o site, poderá então restaurar um backup recente e confiável. Mesmo que não consiga acesso ao servidor poderá restaurar em outro.

Lembre de manter pelo menos umas 3 cópias dos sites e aplicativos e é muito importante que teste o restore em seu desktop e em outra pasta do servidor.

12 - Criação de scripts e aliases

Com a intenção de otimizar a administração do VPS gosto de criar alguns aliases e alguns scripts, tanto para o servidor quanto para o desktop.

Aliases

```
cd /home/ribafs
```

```
nano .bashrc
```

```
alias c="clear"
```

```
alias e="exit"
```

```
alias cw="cd /var/www"
```

```
alias nr="sudo systemctl restart php8.2-fpm nginx"
```

```
# Executar o backup manualmente
```

```
alias backup="sh /home/ribamarfs/backupdiario"
```

```
alias s="sudo su"
```

```
alias rc="nano .bashrc"
```

```
alias rcs="source ~/.bashrc"
```

```
alias phpi="sudo nano /etc/php/8.2/fpm/php.ini;nr"
```

```
source .bashrc
```

Aliases no desktop que agem com o servidor

```
# Trazer para a pasta atual do desktop todos os arquivos da pasta /home/ribamarfs/backups do servidor
```

```
# Acessar o servidor via SSH
```

```
alias s="ssh -p 60222 ribamarfs@ribamar.net.br"
```

```
# Mostrar maiores arquivos da pasta atual em ordem decrescente
```

```
alias maiores="du -h | egrep -v "\\.+/" | sort -hr"
```

Enviar e receber arquivos para/do servidor por scp no desktop

```
sudo nano /usr/local/bin/scpe
```

```
scp -P 60522 $1 ribafs@ribamar.net.br:/var/www
```

```
sudo chmod +x /usr/local/bin/scpe
```

```
sudo nano /usr/local/bin/scpr
```

```
scp -P 60522 ribafs@ribamar.net.br:$1 .
```

```
sudo chmod +x /usr/local/bin/scpr
```

13 - Recomendações Extras de segurança

- Instalar e usar o firewall (ufw) o máximo restritivo e dando acesso somente ao meu IP
- Usar fail2ban e outras similares
- Usar SSL no site e admin
- Sempre criar uns 3 usuários super
- Usar senhas complexas e grandes tanto para joomla quanto para o user do SO
- Cada site com uma senha própria
- Renomear a pasta administrator por padrão.
- Voltar para administrator somente quando for usar ou uma extensão que proteja o administrator
- Backup, backup, e testar em recovery local
- Muito importante: se desapegue, pois não existe segurança perfeita e pode acontecer de ser invadido
- Evite usar programas de FTP (com estes a senha navega em texto claro), ao invés disso use scp, sftp como o Filezilla.

14 – Monitoramento do Servidor

14.1 - Alguns comandos via terminal no servidor

Verificar o espaço em disco

```
df -h
```

Verificar a memória RAM e o swap

```
free -m
```

Verificar o espaço ocupado por uma pasta

```
du -sh pasta
```

Verificar todas subpastas da pasta atual em tamanho e ordem decrescente

```
cd pasta
```

```
maiores
```

O monitoramento do servidor precisa ser contínuo quando temos interesse em sua segurança.

Ao empregar monitoramento proativo e testes de segurança rigorosos, você pode identificar vulnerabilidades antes que agentes mal-intencionados tenham a chance de explorá-las.

Monitorar a performance e estabilidade de funcionamento são importantes para serem monitorados.

14.2 - Lynis

Lynis é uma ferramenta de segurança testada em batalha para sistemas que executam Linux, macOS ou sistema operacional baseado em Unix. Ele executa uma extensa verificação de integridade de seus sistemas para oferecer suporte ao fortalecimento do sistema e aos testes de conformidade. O projeto é um software de código aberto com licença GPL e disponível desde 2007.

<https://cisofy.com/lynis/>

```
sudo apt update  
sudo apt install lynis -y
```

Scan

```
sudo lynis audit system
```

Lynis irá inspecionar várias facetas do seu sistema, incluindo contas de usuário, permissões do sistema de arquivos e configurações de rede. Após a conclusão, ele gera um relatório abrangente detalhando as vulnerabilidades descobertas e as etapas de correção sugeridas. Por exemplo, se Lynis identificar um pacote de software desatualizado, recomendará atualizá-lo para mitigar riscos potenciais. Ao incorporar o Lynis ao seu regime de segurança, você pode reforçar proativamente as defesas do seu servidor e desfrutar de tranquilidade diante de ameaças emergentes.

14.3 - Fail2Ban

Introdução a uma estrutura proativa de prevenção de intrusões

O Fail2Ban está na vanguarda no domínio da prevenção de invasões, fornecendo uma estrutura poderosa projetada para repelir acessos não autorizados e impedir ataques de força bruta. Através do monitoramento vigilante dos arquivos de log, esta ferramenta identifica padrões de comportamento suspeito e responde prontamente impondo restrições de acesso. Um fiel guardião da segurança do seu servidor, o Fail2Ban opera como uma sentinela proativa contra ameaças emergentes.

```
sudo apt update
sudo apt install fail2ban -y
```

Proteger SSH

```
sudo nano /etc/fail2ban/jail.conf
```

```
[sshd]
```

```
enabled = true
```

```
port = ssh
```

```
filter = sshd
```

```
#logpath = /var/log/auth.log
```

```
maxretry = 3
```

```
bantime = 5m
```

```
sudo service fail2ban restart
```

Ver status

```
sudo fail2ban-client status
```

Ver logs

```
sudo cat /var/log/fail2ban.log | grep Ban
```

```
sudo apt update
```

```
sudo apt upgrade fail2ban
```

Diretrizes de configuração e uso para proteção aprimorada

A força do Fail2Ban reside na sua natureza configurável. Exige a criação de arquivos de configuração personalizados para definir regras que detectem e neutralizem o acesso não autorizado. Notavelmente, esta ferramenta encontra aplicação em serviços de proteção como SSH, Mastodon e Nextcloud, entre outros. Ao personalizar essas configurações, você pode estipular parâmetros como o número de tentativas de login malsucedidas permitidas antes de acionar um banimento e a duração do banimento subsequente.

Por exemplo, para proteger o SSH no Ubuntu 20.04, modifique o arquivo `/etc/fail2ban/jail.local` conforme demonstrado anteriormente. Esta abordagem adaptável estende-se à salvaguarda de outros serviços, erguendo assim defesas robustas contra agentes maliciosos que tentam acesso não autorizado.

14.4 - Usando a ferramenta htop

```
sudo apt install htop
```

O htop nos mostra boas informações sobre o servidor em tempo real, como processos rodando, informações sobre a memória, o processador, sobre o swap, uptime, load average. É uma alternativa ao comando top, com uma interface mais amigável, usando cores e oferecendo a possibilidade de uso do mouse

Executar

```
htop
```

Menu abaixo com informações/ações importantes

Informações importantes ao início: load average, swap, memória

Podemos selecionar com o mouse

Clicar em MEM% inverte os processos pelo tamanho

Clicar em CPU% é parecido

Assim também nas demais colunas

Matar processos

Selecionar o processo clicando em sua linha - Teclar F9

Reiniciar processo

selecionar e F7

Mudando prioridade de processos

Selecionar processo com as setas

Teclar F7 ou F8 para ajustar o valor

Uptime

Tempo que faz desde que o servidor foi desligado ou reiniciado.

Comandos suportados:

Arrows, PgUP, PgDn, Home, End ⇒ Percorra a lista de processos.

Espaço ⇒ “Marca”: marca de um processo. Comandos que podem operar para “matar” um processo.

U ⇒ “desmarcar” todos os processos (remover todas as tags adicionadas com a tecla Espaço).

F1, h ⇒ Ajuda

F2, S ⇒ Configuração. Lá você pode configurar metros exibido no topo lado da tela, bem como definir várias opções de tela, escolha entre os esquemas de cores e escolha o layout do exibido colunas.

F3, / ⇒ Processo de pesquisa: digite parte de uma linha de comando do processo e destaque da seleção será transferida para ele. Enquanto na pesquisa modo, pressionar esta tecla irá percorrer as ocorrências correspondentes.

F4, I ⇒ Inverter a ordem de classificação

F5, t ⇒ Organize os processos de paternidade, e o layout mostrado como uma árvore.

F7,], – ⇒ Aumentar a prioridade do processo selecionado. Isso pode ser feito apenas para o superusuário.

F8, [+ ⇒ Diminua a prioridade do processo selecionado.

F9, k ⇒ “Matar o processo”: envia um sinal que é selecionado em um menu, para um ou um grupo de processos. Se os processos foram marcados.

F10, q ⇒ Sair

u ⇒ mostra os processos pertencentes a um usuário especificado.

M ⇒ Ordenar por uso de memória.

P ⇒ Ordenar por uso de processador.

T ⇒ Ordenar por hora.

<https://blog.remontti.com.br/728>

15 – Criação e configuração dos sites

Todos os sites aqui, exceto material (este é apenas um arquivo de redirecionamento), foram criados restaurando backups que eu tinha em meu desktop.

Restaurando Backup de site Joomla

- Crio o bloco no Nginx
- Crio o banco e o usuário no servidor
- Importo usando scp o backup (um zip contendo arquivos e sql) para a pasta /var/www
- Descompacto frango.zip assim:

```
unzip frango.zip -d frango
```

```
Assim ele extrai tudo em /var/www/ frango
```

```
cd /var/www/ frango
```

```
mysql -uroot -psenha frango_db < frango.sql
```

```
Ainda em /var/www/ frango
```

```
nano configuration.php
```

Ajusto os dados do banco e user e tmp e logs

Abro em meu desktop o administrador pelo navegador

<https://frangomontese.com.br/administrator>

Assim eu recupero todos os sites.

Testar tudo, sites e administração e efetuar ajustes se necessário

Ajustes nas Extensões

- idioma pt-br - * (veja abaixo)

- Template T4 com blank bs5 - <https://www.joomlart.com/t4-framework>

- Busca e indexação pelo componente

- Novidades

- Populares

- Bíblia em pt, es e en - <http://backup/materialjs/devel/backend/CMS/Joomla/biblia-joomla-master.zip>

- Pensamento do dia - <http://backup/materialjs/devel/backend/CMS/Joomla/pensamento-do-dia-master.zip>

- Comentários - <https://compojoom.com/downloads/official-releases-stable/ccomment>

- Instalar o plugin Block Access para proteger o administrador e também para o site (All) de todos os sites. - https://github.com/alve89/j_plg_hrz_block_access/releases

* Caso a tradução oficial do Joomla 5.0.3 ainda não tenha saído para o pt-BR e queira uma boa alternativa para instalar o ptbr, veja:

<https://ribamar.net.br/joomla/pt-br-para-joomla-5-0-3>

16 – Dicas sobre PHP

Geralmente precisamos ajustar alguns parâmetros no php.ini e no nginx.conf para poder instalar alguma extensão. Seguem algumas dicas para isso.

Aumentar tamanho do upload do PHP

php.ini

```
post_max_size - 16  
upload_max = 16
```

Nginx – quando recebemos o erro

413 Request Entity Too Large

```
sudo nano /etc/nginx/nginx.conf
```

```
# set client body size to 16M #  
client_max_body_size 16M;
```

```
nginx -s reload
```

```
sudo systemctl restart php8.2-fpm nginx
```

Pasta temporária do PHP

```
upload_tmp_dir = /tmp
```

17 – Códigos deste e-book no Github

Caso tenha alguma dificuldade em copiar e colar o código deste PDF, então veja este arquivo texto no Github:

<https://github.com/ribafs2/vps/blob/main/codigos.txt>

18 – Informações sobre a Contabo

Site de administração

<https://my.contabo.com/>

E-mail do suporte

support@contabo.com

Que sistemas operacionais/distribuições/versões são suportadas (16/04/2024)

- AlmaLinux 8 e 9
- CentOS 7
- Debian 11 e 12
- Fedora 35
- OpenSuSE 15.3
- Rocky Linux 9
- Ubuntu 20.04 e 22.04

Alguns recursos

Your services - Muitas informações sobre o nosso VPS e gerenciamento (Manage)

Customer details - dados sobre quem contratou o Contabo

Unpaid Orders - pagamentos em aberto

Billing - informações sobre pagamento

Payment Method - mudar forma de pagamento

VPS control - onde está a maioria das ferramentas de administração do VPS:

restart

start

stop

Reinstall

Snapshot

No botão Manage tem um assistente caso não esteja conseguindo conectar ao servidor

Reset password - caso queira trocar a senha do root

Move to other region - lembre que outras regiões são pagas

Reinstall

Criamos snapshot para que, em caso de problema fatal, possamos voltar o servidor ao estado em que criamos o snapshot. Para isso usamos a ferramenta Reinstall.

Após reinstalar o status fica pending (observe). Aguarde até que mude para running, para somente então acessar o servidor.

Após reinstalar deve acessar com

```
ssh root@IP
```

Caso no desktop apareça uma mensagem contendo:

```
ssh-keygen -f "/home/ribafs/.ssh/known_hosts" -R "84.247.172.72"
```

Execute esta linha no prompt, aguarde um pouco então repita para acessar

```
ssh root@IP
```

Operating system reinstallations

Esta página fornece uma visão geral das tarefas de reinstalação atualmente pendentes, em execução e concluídas recentemente para seus servidores. Por favor observe o seguinte:

O progresso é baseado no tempo médio necessário para instalar o sistema operacional escolhido.

Dependendo do modelo do seu servidor, a instalação pode demorar um pouco mais do que a barra de progresso sugere. Após o início da instalação, aguarde pelo menos 90 minutos para ver se ela termina.

Se a instalação não for concluída após 90 minutos, provavelmente a instalação falhou. Portanto, recomendamos que você reinicie a instalação ou entre em contato com nosso suporte e forneça o nome do servidor ou endereço IP mostrado na lista para que possamos verificar o estado atual em seu nome.

O campo de status contém os seguintes estados:

pendente: A instalação foi planejada e começará quando o servidor for reinicializado.

running: A instalação está em execução. A barra de progresso mostra uma estimativa de quanto do processo foi concluído.

falhou: A instalação foi assumida como falhada. Portanto, recomendamos que você reinicie a instalação.

iniciado: O sistema de resgate foi iniciado e agora está acessível.

finalizado: A instalação foi relatada como concluída e seu servidor deverá estar online após uma reinicialização final.

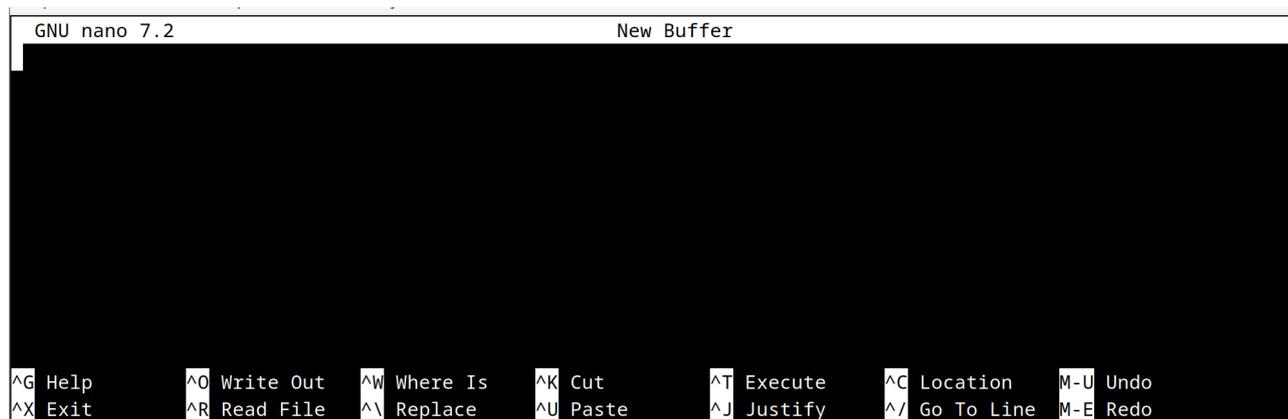
Server	Operating System	Starttime (CEST)	Status	Progress
vmi1612885	(84.247.172.72)	Debian 12 Image	07.04.2024 06:49	pending

19 – Ferramentas

19.1 – nano - Editor de texto para o terminal

O editor de texto para o terminal, nano, é muito utilizado no linux, tanto que o Debian já o traz instalado em um VPS da Contabo.

Ele é bem amigável



```

GNU nano 7.2                               New Buffer
-----
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo
  
```

Veja que para facilitar um pouco ele traz um menu na parte inferior, com boa parte dos principais comandos.

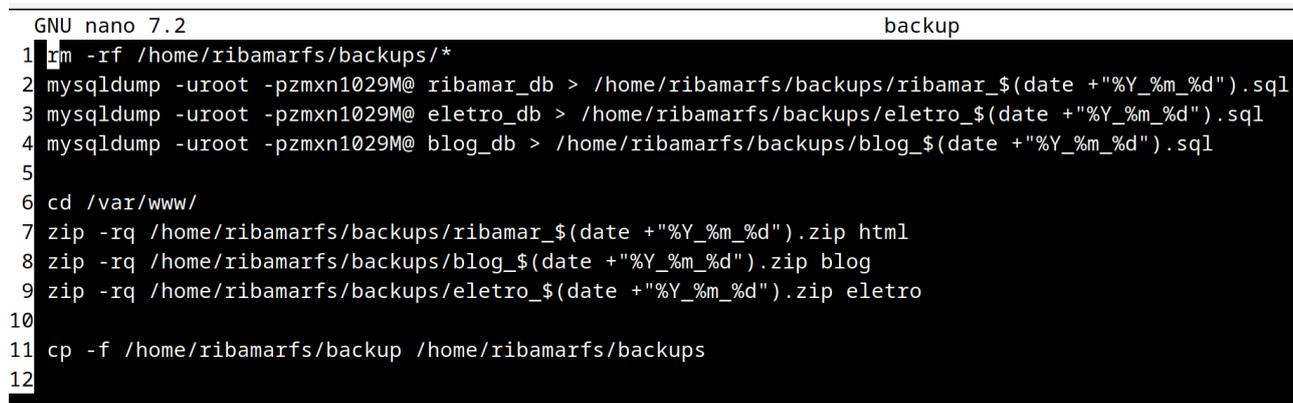
Alguns dos comandos que utilizo.

Abrir um arquivo

```
nano nomearq
```

Abrir um arquivo mostrando os números de linha

```
nano -l nomearq
```



```

GNU nano 7.2                               backup
-----
1 rm -rf /home/ribamarfs/backups/*
2 mysqldump -uroot -pzmxn1029M@ ribamar_db > /home/ribamarfs/backups/ribamar_$(date +"%Y_%m_%d").sql
3 mysqldump -uroot -pzmxn1029M@ eletro_db > /home/ribamarfs/backups/eletro_$(date +"%Y_%m_%d").sql
4 mysqldump -uroot -pzmxn1029M@ blog_db > /home/ribamarfs/backups/blog_$(date +"%Y_%m_%d").sql
5
6 cd /var/www/
7 zip -rq /home/ribamarfs/backups/ribamar_$(date +"%Y_%m_%d").zip html
8 zip -rq /home/ribamarfs/backups/blog_$(date +"%Y_%m_%d").zip blog
9 zip -rq /home/ribamarfs/backups/eletro_$(date +"%Y_%m_%d").zip eletro
10
11 cp -f /home/ribamarfs/backup /home/ribamarfs/backups
12
  
```

Veja que os números de linha são mostrados à esquerda.

Salvar um arquivo

Após criar ou alterar um arquivo para salvar:

Ctrl+O - salvar

Ctrl+X - sair

Copiar e colar

Copiar – Selecione a linha e Alt + 6

Colar – Coloque o cursor onde deseja colar e tecle Ctrl+U

Busca

Tecele F6 e digite o termo

Desfazer a última ação

Alt+U

19.2 – mc - Gerenciador de arquivos para o terminal

Instalei um gerenciador de arquivos para o modo texto, que é o

mc – midnight commander

Mesmo sendo no terminal ele tem muitos bons recursos e já vem com dois peineis, um ao lado do outro, para que possamos copiar da esquerda para a direita e outras operações. Suporta o uso do teclado e do mouse.

Veja sua interface

```

Left      File      Command  Options  Right
<- ~ . [^]> <- ~ . [^]>
.n        Name      Size     Modify   time    .n        Name      Size     Modify   time
/..       UP--DIR   Apr 7 15:10 /..       UP--DIR   Apr 7 15:10
/.cache   4096     Apr 7 16:39 /.cache   4096     Apr 7 16:39
/.config  4096     Apr 8 17:04 /.config  4096     Apr 8 17:04
/.local   4096     Apr 7 15:56 /.local   4096     Apr 7 15:56
/backups  4096     Apr 10 09:44 /backups  4096     Apr 10 09:44
.bash_history 7951    Apr 10 18:16 .bash_history 7951    Apr 10 18:16
.bash_logout 220     Apr 7 15:10 .bash_logout 220     Apr 7 15:10
.bashrc   3926     Apr 10 18:12 .bashrc   3926     Apr 10 18:12
.lesshst 20       Apr 8 17:06 .lesshst 20       Apr 8 17:06
.mysql_history 1650    Apr 9 14:46 .mysql_history 1650    Apr 9 14:46
.profile  807     Apr 7 15:10 .profile  807     Apr 7 15:10
.selected_editor 68     Apr 8 13:49 .selected_editor 68     Apr 8 13:49
.sudo_as_admin_successful 0      Apr 7 15:11 .sudo_as_admin_successful 0      Apr 7 15:11
.wget-hsts 165     Apr 8 04:12 .wget-hsts 165     Apr 8 04:12
backup    595     Apr 7 19:30 backup    595     Apr 7 19:30
*backupdayly 596    Apr 8 13:44 *backupdayly 596    Apr 8 13:44

UP--DIR                                     77G / 96G (80%)
UP--DIR                                     77G / 96G (80%)

Hint: Tab changes your current panel.
~--Serv -> [^]
1Help 2Menu 3View 4Edit 5Copy 6RenMov 7Mkdir 8Delete 9PullDn 10Quit
  
```

O menu inferior oferece a maioria das suas funcionalidades podendo ser ativados com as teclas F1 a F10 ou com o mouse.

Se usarmos assim:

mc pastaesq pastadir

Ele abrrirá no painel da esquerda a pastaesq e na direita a pastadir.

Ele já vem com um editor integrado, que é o mcedit e é usado para visualizar arquivos texto. Para editar um arquivo texto, selecione-o e teclre F4. Na primeira vez ele perguntará com qual editor deverá ficar editando os arquivos texto. Como eu já uso o nano, o escolho para usar sempre o nano.

Veja que podemos mover um arquivo/pasta do painel da esquerda para a direita, selecionando e teclando em F6.

Para excluir arquivos/pastas, selecionar e teclar F8,

Assim podemos fazer muita coisa com mais praticidade que pela linha de comando.

19.3 – Compactação de arquivos

Alguns poucos comandos que utilizo para descompactar arquivos no terminal do Linux.

Descompactar um arquivo zip em certa pasta

```
unzip nome -d pasta
```

Descompactar um arquivo .tar.gz em certa pasta

```
tar xzpvf nome.tar.gz -C pasta
```

19.4 – Gerenciamento de pacotes com apt

Atualizar repositórios

```
sudo apt update
```

Atualizar todos os pacotes da distribuição, inclusive os de terceiros

```
sudo apt upgrade
```

```
sudo apt upgrade -y (sem pedir confirmação)
```

Instalar um pacote

```
sudo apt install ufw
```

Remover um pacote

```
sudo apt remove ufw
```

Minha busca preferida

```
sudo aptitude search nome
```

Na listagem de retorno os que aparecem na coluna da esquerda com i é porque estão instalados.

19.5 – Alguns comandos

ls -la – mostra os arquivos da pasta atual, inclusive os ocultos

ls -lh – lista os arquivos mostra o tamanho de cada um

`sudo chown ribamarfs:ribamarfs arquivo` – Torna o user ribamarfs o dono do arquivo e o arquivo pertencerá ao grupo ribamarfs

`sudo chmod +x /usr/local/bin/arq` – Torna arq um arquivo executável.

`sudo chmod -R 775 /home/teste` – Torna a pasta /home/teste, recursivamente dizendo que o dono dos arquivos podem tudo (7), que os do grupo também podem tudo, segundo 7 e que os outros podem acessar e ler somente.

`pwd` – mostra a pasta atual

`whoami` – mostra quem é o user que está logado

Calculadora

`expr 6 + 4`

Espaços antes e após o sinal

scp – copia de arquivos usando SSH

Copiar um arquivo arqa local da pasta atual para o servidor na pasta /var/www

`scp -P porta arqa usuario@IPouDominio:/var/www`

Copiar um arquivo /var/www/teste.zip do servidor para a pasta atualizado

`scp -P porta usuario@IP:/var/www/teste.zip .`

rsync

Usando rsync para fazer uma cópia incremental do servidor para o desktop. No caso trazer somente os arquivos que não estão no desktop. Quando a pasta requer uso do sudo

`rsync -av --ignore-existing --progress -e 'ssh -p 60222' ribamarfs@ribamar.net.br:/home/backups/* /teste/"`

Trará de /home/backups no servidor para a pasta /teste no desktop, mas baixará somente os que não estejam ainda em /teste (incremental)

Quando a pasta não requer uso do sudo

`rsync -av --ignore-existing --progress ribamarfs@ribamar.net.br:/home/backups/* /teste/"`

19.6 – Atualizações de segurança automáticas

```
sudo apt update
sudo apt install unattended-upgrades apt-listchanges -y
```

```
sudo nano /etc/apt/apt.conf.d/50unattended-upgrades
```

Certifique-se de que o arquivo inclua as seguintes linhas para permitir que o pacote atualize automaticamente todos os pacotes do repositório de segurança:

```
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}-security";
};
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:00";
```

Criar

```
sudo nano /etc/apt/apt.conf.d/20auto-upgrades
```

Adicione as seguintes linhas para garantir que a lista de pacotes de atualização e a atualização automática sejam executadas diariamente:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Testar

```
sudo unattended-upgrades --dry-run --debug
```

Crédito

<https://reintech.io/blog/configure-automatic-security-updates-debian-12>

No meu desktop

No packages found that can be upgraded unattended and no pending auto-removals
The list of kept packages can't be calculated in dry-run mode.

20 – Referências

<https://contabo.com/en/vps/>

<https://my.contabo.com/>

<https://www.digitalocean.com/>

<https://www.vultr.com/>

<https://www.linode.com/>

<https://www.hostgator.com.br/servidor-vps>

Testes grátis por um ano

https://cloud.google.com/?hl=pt_br

<https://aws.amazon.com/pt/free>

<https://azure.microsoft.com/pt-br/free/>

21 – Conclusão

Gostaria de alertar para o fato de que este pequeno e-book é apenas um resumo prático de como eu trabalho e portanto se desejar se aprofundar na área deverá continuar estudando, pois existe muito mais.