

Servidores VPS



Ribamar FS

Fortaleza, 21 de maio de 2018

Sumário

| | |
|--|-----|
| 1 – Cuidados Básicos..... | 5 |
| 1.1 - Alguns comandos do Linux, do FreeBSD e do OpenBSD..... | 5 |
| 1.2 - Crecar ISO..... | 17 |
| 1.3 - Compactar e Descompactar Arquivos no Terminal do Linux..... | 17 |
| 1.4 – Crontab..... | 20 |
| 1.5 - Procurar string s sobrescrever com outra em arquivo..... | 27 |
| 1.6 - Dica sobre a linguagem C:..... | 28 |
| 1.7 - DNS Gratuito de CloudFlare..... | 29 |
| 1.8 – Corrigir Erros de Locales..... | 29 |
| 1.9 - Procurando Arquivos pelo Terminal do UNIX com find e locate..... | 30 |
| 1.10 - Formatar pendrive..... | 32 |
| 1.11 - Criar um link simbólico..... | 33 |
| 1.12 - Editor de textos para o terminal/modo texto no Unix..... | 33 |
| 1.13 - Setando Permissões para o Servidor web..... | 35 |
| 1.14 – Configurações de Rede pela linha de comando..... | 36 |
| 1.15 – Usando o RSync..... | 46 |
| 2 – Desktop..... | 47 |
| 2.1 – Batchs ou Arquivos de Lote..... | 48 |
| 2.2 - Recuperação do Grub 2..... | 51 |
| 2.3 – Ajustar Relógio em Dualboot..... | 51 |
| 2.4 – Proteção de Roteador WiFi..... | 51 |
| 2.5 – SSH em Banda Larga ADSL..... | 52 |
| 2.6 - Upgrade do Debian..... | 52 |
| 2.7 – Upgrade Ubuntu..... | 52 |
| 2.8 - Configurar Hora em Servidor Debian e derivados..... | 54 |
| 2.9 - Ajustar o hostname..... | 54 |
| 2.10 - Para limpar o cache da RAM..... | 54 |
| 2.11 - MySQL..... | 55 |
| 2.12 – Adicionar partição de Swap ao Linux..... | 62 |
| 2.13 – Clamav..... | 62 |
| 3 – Hospedagem tipo VPS..... | 63 |
| 3.1 - Hospedagem na Digital Ocean..... | 63 |
| 3.1.1 – Snapshot..... | 90 |
| 3.1.2 – DNS na Digital Ocean..... | 92 |
| 3.2 – Servidores VPS na Vultr..... | 94 |
| 3.2.1 - Restauração de Snapshot na Vultr..... | 100 |
| 3.2.2 – DNS na Vultr..... | 101 |
| 4 – Melhorando a Segurança de um VPS com CentOS 7..... | 105 |
| 4.0. Cuidados Iniciais..... | 105 |
| 4.1. Habilitação e Configurar firewall com ufw..... | 108 |
| 4.2. Secure shared memory no fstab..... | 108 |
| 4.3. Reforçar a segurança do SSH..... | 108 |
| 4.4. Reforçar a segurança da rede configurando o sysctl..... | 110 |
| 4.5. Prevenir IP Spoofing..... | 111 |
| 4.6. Reforçar a segurança do PHP..... | 111 |
| 4.8. Instalar e Configurar ModSecurity e ModEvasive..... | 112 |

| | |
|---|-----|
| 4.9. Scannear logs e banir hosts suspeitos..... | 112 |
| 4.10. Detectar Intrusões – PSAD..... | 114 |
| 4.11. Checar por RootKits – RKHunter e CHKRootKit..... | 114 |
| 4.12 Varrendo portas abertas com Nmap..... | 115 |
| 4.13. Instalar e configurar o Apparmor..... | 115 |
| 4.14. Auditar segurança do sistema com Tiger e Tripwire..... | 116 |
| 4.15. Atualizar a distribuição..... | 117 |
| 4.16. Usar Senhas Fortes..... | 117 |
| 4.17. Melhorando a segurança de sites com Joomla..... | 117 |
| 4.18. Melhorar a segurança no Desktop..... | 118 |
| 4.19. Melhorando a Segurança do MySQL..... | 119 |
| 4.20. Melhorando a segurança com Lynis..... | 119 |
| 4.21. Cuidados Extras..... | 121 |
| 5 - Monitorando um servidor Linux Ubuntu 16.04..... | 122 |
| 5.1 - Varrendo portas abertas com Nmap..... | 123 |
| 5.2 - Auditar segurança do sistema com Tiger e Tripwire..... | 127 |
| 6 – Segurança em Servidores Linux..... | 129 |
| 6.1 - Atualizar automaticamente somente as atualizações de segurança..... | 130 |
| 6.2 – Remover serviços que não estão em uso..... | 130 |
| 6.3 – Senhas Fortes..... | 130 |
| 6.4 – Ferramentas..... | 131 |
| 6.5 – Desempenho do Servidor..... | 132 |
| 6.6 – Criptografia..... | 134 |
| 6.6 - Melhorar a segurança da memória compartilhada..... | 136 |
| 6.7 – Firewall..... | 136 |
| 6.7.1 – IPTables..... | 136 |
| 6.7.2 – ufw..... | 142 |
| 6.8 – Logs..... | 144 |
| 6.9 – Apache..... | 145 |
| 6.10 – PHP..... | 151 |
| 6.11 - Melhorando a Segurança do MySQL/MariaDB..... | 153 |
| 6.12 – Reforçando a Segurança do Joomla..... | 154 |
| 6.13 – SELinux..... | 163 |
| 6.14 – Rede..... | 184 |
| 6.15 - Mantendo Servidores web e de bancos de dados seguros..... | 188 |
| 6.16 – SSH..... | 189 |
| 6.17 – AppArmor..... | 198 |
| 6.18 – Bastille..... | 199 |
| 6.19 – fail2ban..... | 200 |
| 6.20 - RKHunter e CHKRootKit..... | 201 |
| 6.21 - Detectar Intrusões com PSAD..... | 202 |
| 6.22 - Advanced Intrusion Detection Environment (AIDE)..... | 202 |
| 6.23 - Usando DenyHosts..... | 203 |
| 6.24 - Melhorando a segurança com Lynis..... | 204 |
| 7 – Ferramentas..... | 209 |
| 7.1 – Backup..... | 209 |
| 7.3 - Soluções para Administração Web de Servidor..... | 216 |
| Cockpit..... | 217 |
| 7.4 – Testes de Stress para Servidor Web..... | 219 |
| 8 – Shell Scripts..... | 226 |

| | |
|----------------------------|-----|
| 9 – Servidores..... | 235 |
| 9.1 – CentOS EMP..... | 235 |
| 9.2 – CentOS LAMP..... | 248 |
| 9.3 – Debian com LEMP..... | 266 |
| 9.4 – Fedora..... | 278 |
| 9.5 – OpenBSD..... | 289 |
| 9.6 – Ubuntu com LAMP..... | 316 |
| 9.7 – Ubuntu com LEMP..... | 330 |
| 9.8 – FreeBSD..... | 340 |

1 – Cuidados Básicos

1.1 - Alguns comandos do Linux, do FreeBSD e do OpenBSD

A maioria dos comandos funciona de forma idêntica em Linux e BSD
Mas existem pequenas variações especificamente em arquivos de configuração
Linux e OpenBSD geralmente armazenam os arquivos de configuração na pasta

/etc

E arquivos de usuários na pasta
/home

FreeBSD armazena o arquivos de configuração do sistema na pasta
/etc

Mas os arquivos de programas opcionais (aqueles instalados pelo usuário: Apache, PHP,
etc) na pasta:
/usr/local/etc

Arquivos de usuários na pasta
/usr/home

Instalação de Pacotes

As distribuições Linux cada uma tem seus gerenciadores de pacotes e comandos

FreeBSD usa

```
pkg install nome  
pkg update  
pkg upgrade  
pkg search
```

OpenBSD

```
pkg_add nome  
pkg_info nome  
pkg_add -u nome
```

Acertando a data e a hora (Linux e BSD)

```
date  
[MMDDhhmm[[CC]YY][.ss]]
```

16/03/2018 13:23

```
sudo date 031613232018
16/03/2018 13:23
sudo date 03161323
16/03/2018 13:23
```

SSH (Linux e BSD)

```
ssh ribafs@ribafs.org
```

Com porta diferente
ssh -p 25522 ribafs@ribafs.sub.es

Copiar para fora
scp -P 25522 arquivo.zip user@ip_ou_dominio:/home/ribafs

Copiar para cá
scp -P 25522 user@ip_ou_dominio:/home/user/arquivo.zip /home/ribafs

Download continuando caso caia com wget (Linux e BSD)

O wget é um software para fazer download com muitos recursos, inclusive continuar caso seja interrompido

Continuar caso seja interrompido

```
wget -c http://joomla.org/download/joomla3.5.2.tar.gz
```

Baixar arquivo com wget em certo diretório

```
sudo wget "http://www.adminer.org/latest.php" -O /usr/share/adminer/latest.php
```

Navegador web em modo texto (Linux e BSD)

```
lynx http://site.com.br
```

Gerenciador de arquivos modo texto (Linux e BSD)

```
mc /pasta1 /pasta2
```

history - mostra o histórico de comandos digitados (Linux e OpenBSD)

Muitos são comuns a todos os sabores Unix

uname - mostra informações sobre o sistema.
uptime - informa há quanto tempo sua máquina está ligada sem reiniciar.
arch - informa a arquitetura do computador (ex.: i386, i586, etc).
free - exibe informações sobre a utilização de memória da máquina.
free -m

cal - mostra calendário
cal 2010
cal -d 2013-05

`pwd` - mostra qual é o diretório onde estou agora

`ls` - listagem de arquivos e diretórios

`ls -la` - inclusive ocultos

`ls -lh` - mostra com respectivos tamanhos

`mkdir` - criar diretório

`mkdir -p` - criar recursivo

`mkdir -p /home/ribafs/dir1/dir2/dir3` - cria todos, mesmo que dir1 e dir2 não existam

Criar dois diretórios

`mkdir -p /etc/nginx/sites-{enabled,available}`

Criar Vários de uma vez só

`mkdir -p diretorio/{1..100}`

`mkdir -p Retroarch/{core/,save/}`

`cd` - muda para o diretório fornecido. `cd /etc`

`cd -` - volta para o diretório que estava anteriormente

`cd ..` - desce um nível abaixo na árvore de diretórios

`cd ../../` - desce dois níveis

clear - limpar a tela (Linux e BSD)

mv origem destino - move arquivo/diretório (Linux e BSD)

rm nome - remove arquivo

`rm -rf nomedir` - remove diretório

Copiar arquivo/diretório da origem para o destino (Linux e BSD)

`cp` origem destino

Copiar recursivamente com todo o conteúdo

`cp -Ra` origem destino

Para copiar arquivos ou diretórios preservando suas permissões, atributos, links, basta utilizar o comando "`cp`" com a opção "`-p`":

Exemplo de comando (Copiando Arquivos):

`cp -p /home/User/teste.txt /etc`

Exemplo de comando (Copiando Diretórios recursivamente):

`cp -rp /home/User/ /etc`

Obs: A opção "`-r`" copia recursivamente os diretórios, arquivos, links

Mais informações digite: "`man cp`"

Cria arquivo vazio (Linux e BSD)

touch arquivo.txt

ou

> arquivo.txt - cria o arquivo

Mostra informações sobre todas as placas de rede, IP, máscara, etc (Linux e BSD)

ifconfig

last - histórico de usuários que acessam o sistema nome

Localizar arquivos (Linux e BSD)

Para atualizar o banco de dados do locate:

Linux - sudo updatedb

BSD - sudo /usr/libexec/locate.updatedb

locate nome

find /etc -name 'php' -printlo

locate arquivo

Antes execute updatedb para atualizar seu banco de dados

find /var/www/html -type f -name "config.php"

Procura um arquivos por um padrão, sendo um filtro muito útil e usado, por exemplo um cat a.txt | grep ola irá mostrar-nos apenas as linhas do ficheiro a.txt que contenham a palavra "ola"

grep

Lista as localizações de programas binários, fontes e documentações.

Procurar path de arquivos binários/comandos

whereis comando_binario

Criptografar arquivos facilmente

Criptografar

gpg -c arquivo.txt

Pedirá uma senha e gerará o arquivo arquivo.txt.gpg

Guardar arquivo.txt fora ou remover

Descriptografar

gpg arquivo.txt.gpg

Trará de volta o arquivo.txt

Criar arquivo com certo tamanho. Gerará um arquivo de 10MB

dd if=/dev/zero of=teste_arquivo.txt bs=1M count=10

Criar 100 arquivos arq1, arq2, ... arq100
touch diretorio/arq{1..100}

Apagar arquivos com mais de 7 dias
find /tmp/ -type f -mtime +7 -exec rm -f {} \;

Apagar diretórios antigos

```
find /tmp/ -type d -mtime +7 -exec rm -f {} \;
```

Lista todos os comandos do sistema

```
compgen -c
```

```
compgen -c | grep find
```

Nome da distribuição

```
lsb_release -a
```

```
ou cat /etc/issue
```

Criar arquivo com listagem do hardware

```
sudo lshw -short -html > info.txt && xdg-open info.txt
```

Mostra arquivo texto na tela

```
cat arquivo.txt
```

Alterar permissão de arquivos e diretórios

```
chmod dgo
```

d - permissão do dono

g - permissão de todo o grupo

o - permissão dos outros/público

Exemplos:

```
chmod 664 arquivo.html
```

```
chmod -R 644 /var/www/html
```

Dono de arquivos e diretórios

```
chown u:g
```

u - usuário

g - grupo

Exemplo

```
chown -R ribafs:www-data /var/www/html
```

Criar arquivo vazio

```
touch arquivo.txt
```

ou

```
> arquivo.txt
```

Editores de texto

```
vi ou vim
```

mcedit - editor de texto parte do pacote mc

nano - editor de texto

Ver números de linhas no nano

nano -c arquivo.txt

Comandos do nano:

Ctrl+O - salvar

Ctrl+X - sair

Busca interna - F6

Shift + Insert - colar texto que está na memória

Ctrl+K - apagar a linha atual

df - mostra informações das partições

df -h - informações e espaço em MB

free - informações sobre memória RAM e swap (apenas no Linux)

free -m - mostrando em MB

du - mostra arquivos e diretórios com seus respectivos tamanhos

du -sh - mostra o tamanho total do diretório atual ou indicado de forma silenciosa, sem listar

Mostrar processos

ps ax

kill -9 numero_processo # Número da esquerda

Restartar serviço sem derrubá-lo

sudo killall -HUP apache2

Trocar a senha do usuário

passwd ribafs

Reiniciar computador

reboot

shutdown -r now

Desligar agora

shutdown -h now

Mostrar informações de uso dos recursos de hardware: cpu, RAM, etc
top

Informações sobre o sistema operacional

uname -a

Informações sobre o usuário atual

who

Nome do usuário atual

whoami

Pacotes Debian e derivadas

sudo su

apt update - Atualizar repositórios

apt upgrade - atualizar os pacotes

apt install nome - instalar um pacote

apt remove nome - remover um pacote

apt remove --purge nome - remover apagando configurações

aptitude search nomeouparte - busca por pacotes instalados e não instalados. Os instalados são listados com i à esquerda

Listagem de arquivos texto:

more - lista todo o arquivo de uma vez

less - lista pro página, podendo passar com pgdn e voltar com pgup

pstree - mostra os processos do sistema em árvore

Bom uso do less:

pstree | more

fdisk -l - mostra partições

Saber informações sobre um comando:

comando --help

man comando

Lista de comandos - <http://comandoslinux.com/>

Comandos do Apache

a2enmod nome_modulo => habilita módulo

a2dismod nome_modulo => desabilita módulo

a2ensite nome_site (existentes no diretório /etc/apache2/sites-available) => habilita site

a2dissite

a2enconf => habilita configuração

a2disconf

Gerenciamento do serviço

systemctl start apache2

```
systemctl status apache2.service  
journalctl -xn  
Verificar sintaxe da configuração  
apachectl -t
```

Usuários e grupos

```
adduser nome  
addgroup nome  
userdel nome  
groupdel nome  
adduser user group
```

chown Mudar o dono ou grupo de um ficheiro ou directoria, vem de change owner
chgrp Mudar o grupo de um ficheiro ou directoria

ifconfig - informações sobre placas de rede

passwd nome - trocar a senha de um usuário

pwd - mostra diretório atual

who - mostra informações sobre o usuário atual

whoami - mostra usuário atual

reboot - reiniciar servidor

Hardware

```
dmidecode -t memory
```

```
free -m
```

```
du -f
```

Referências

<http://comandoslinux.com/>

<https://www.infowester.com/comandoslinux.php>

<https://www.vivaolinux.com.br/dicas/impressora.php?codigo=6935>

<http://www.linuxdevcenter.com/cmd/>

<https://linuxconfig.org/linux-commands>

<https://www.mediacollege.com/linux/command/linux-command.htm> |

<https://sempreupdate.com.br/5-administracao-de-sistemas-linux-comandos-uteis/>

<https://sempreupdate.com.br/6-administracao-de-sistemas-linux-comandos-uteis-parte-2/>

<https://sempreupdate.com.br/7-administracao-de-sistemas-linux-comandos-uteis-parte-3/>

<https://sempreupdate.com.br/8-administracao-de-sistemas-linux-comandos-uteis-parte-4/>

<https://sempreupdate.com.br/9-administracao-de-sistemas-linux-comandos-uteis-parte-5/>

<https://sempreupdate.com.br/10-administracao-de-sistemas-linux-comandos-uteis-parte-6/>

1.2 - Checar ISO

```
sha512sum /dev/sr0 /tmp/file.iso
```

```
md5sum file.iso
```

1.3 - Compactar e Descompactar Arquivos no Terminal do Linux

Instalar compactadores para Linux:

```
sudo apt-get install unace zip unzip p7zip-full p7zip-rar sharutils uudeview mpack arj unrar  
rar lzma lha lzma-dev rar unrar-free ark ncompress
```

Compactação zip

```
zip pacote.zip arquivoa.txt arquivos.txt arquivos.odt  
zip pacote.zip *.txt  
zip -r documentos.zip /usr/*.txt
```

Opções:

- r recursivo
- 1 rápido
- 9 maior compactação
- D compactar somente arquivos, nada de diretório
- x arquivos - excluir da compactação alguns arquivos

Descompactação

```
unzip nome.zip
```

Em diretório específico

```
unzip nome.zip -d /tmp
```

Compactar arj

```
arj a pacote.arj arquivo.odt
```

Descompactar

```
arj x pacote.arj
```

Compactar tar

```
tar -czpvf pacote.tar arquivo1.gif memorando.htm carta.doc  
tar -czpvf pacote.tar pasta
```


Descompactar:

```
tar -zxpvf nomedoarq.tar
```

Compactar tar.gz

```
tar -czpvf pacote.tar.gz arquivo1.gif memorando.htm carta.doc  
tar -czpvf pacote.tar.gz pasta
```

Descompactar num certo diretório

```
tar -zxpvf pacote.tar.gz -C /tmp
```

```
tar.bz2
```

```
tar -jxpvf pacote.tar.bz2
```

Descompactar apenas um arquivo de dentro do pacote

```
tar -xvf pacote.tar.gz foto1.png
```

Lista de parâmetros do tar:

- c – cria um novo arquivo tar;
- M – cria, lista ou extrai um arquivo multivolume;
- p – mantém as permissões originais do(s) arquivo(s);
- r – acrescenta arquivos a um arquivo tar;
- t – exhibe o conteúdo de um arquivo tar;
- v – exhibe detalhes da operação;
- w – pede confirmação antes de cada ação;
- x – extrai arquivos de um arquivo tar;
- z – comprime ou extrai arquivos tar resultante com o gzip;
- j – comprime ou extrai arquivos tar resultante com o bz2;
- f – especifica o arquivo tar a ser usado;
- C – especifica o diretório dos arquivos a serem armazenados.

Compactar gzip

```
gzip documentos.odt
```

Descompactar

```
gunzip documentos.odt.gz
```

Compactar bzip2

```
bzip2 pacote.gz
```

Descompactar

```
bunzip2 pacote.bz2  
bunzip2 pacote.tar.bz2
```

Compactar rar

rar a pacote.rar arquivoa arquivob

rar a pacote.rar /pasta

Descompactar

unrar x pacote.rar

Compactar 7z

7za a pacote.7z arquivoa arquivob

Descompactar

7za x pacote.7z

Compactar lha

lha a pacote.lha arquivoa arquivob

Descompactar

lha x pacote.lha

Compactar zoo

zoo a pacote.zoo arquivoa arquivob

Descompactar

zoo x pacote.zoo

Ajuda sobre um dos compactadores acima:

man nome_compactador

Ex:

man arj

Referências:

<http://blog.kolaborativa.com/2011/10/compactar-e-descompactar-arquivos-zip-rar-tar-gz-bz2-tar-tar-bz2-pelo-terminal/>

<https://linuxdicasuporte.blogspot.com.br/2015/03/compactacao-de-arquivos-para-debian.html>

1.4 – Crontab

CRONTAB – o agendador de tarefas do linux e BSD
4 de janeiro de 2012 By Ubuntu Dicas 15 Comentários

por Rodolfo Silveira

Olá pessoal, estou aqui de volta fazendo um pequeno tutorial sobre o crontab o agendador de tarefas do Linux, lembrando que o crontab existe em qualquer versão do linux.

Com o crontab é possível especificar horários como “todos os dias às 5 da manhã” ou “a cada meia hora”, “de dez em dez minutos”.

Para a maioria das tarefas pouco importa a hora que vai ocorrer mas sim a frequência em que ela vai ser executada, como diariamente ou semanalmente. Para isso já existe 4 diretórios especiais, que basta o administrador botar o script lá dentro, eles já serão executados na periodicidade desejada.

```
/etc/cron.daily diário
/etc/cron.hourly a cada hora
/etc/cron.monthly mensal
/etc/cron.weekly semanal
```

Mas caso você mesmo queira fazer um período específico, com hora e tudo mais, basta editar o arquivo:

```
/etc/crontab
```

Então vamos lá. Escolha um editor de sua escolha, no meu caso o VIM e abra um terminal e digite:

```
sudo vim /etc/crontab
```

Notem no conteúdo:

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
```

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
# m h dom mon dow user command
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

Notem que já existe algumas entradas justamente dos diretórios especiais, para adicionar sua própria tarefa temos que seguir o seguinte padrão de linha:

```
minuto hora dia domês mês diadasemana usuário comando
```

Notem que para cada espaço, se avança um campo e os campos seguem o padrão existente que conhecemos, por exemplo no campo mês não pode ter 15 pois temos de 1-12 e o campo da semana usamos de 0 a 7 onde zero e 7 é domingo 1 é segunda-feira, 2 terça-feira e assim por diante.

Temos também alguns caracteres que facilitam a vida:

| Caractere | Exemplo | Significado |
|-----------|---------|---------------------------|
| Hífen | 2-4 | intervalo de 2 a 4 |
| virgula | 2,4,6,8 | os números 2,4,6 e 8 |
| barra | */10 | de dez em dez |
| asterisco | * | todas as opções possíveis |

Vamos botar a mão na massa:

Imagine que temos uma rotina de backup que comprime o o /home e o /var/log e queremos que esta rotina aconteça diariamente as 23:35;

Se usarmos o tar por exemplo, poderíamos usar duas linhas de comando ou não, por isso recomendo que crie um script e no arquivo do CRON nós vamos apontar para o script. Criando o script:

```
vim /scriptbkp.sh
```

O conteúdo do script, onde comprime a pasta home e a pasta log no hd externo de modo que o nome do arquivo fique com a data do dia da execução e ainda criando um arquivo de log localizado no /scriptbkplog.log para posterior análise:

```
#!/bin/sh
tar -cvzf /media/hdexterno/bkphome$(date +%Y_%m_%d).tar.gz /home >>
/scriptbkplog.log
tar -cvzf /media/hdexterno/bkplog$(date +%Y_%m_%d).tar.gz /var/log >>
/scriptbkplog.log
```

Salve e saia.

Vamos dar permissão de execução também:

```
sudo chmod 755 /scriptbkp.sh
```

Agora vamos lá no crontab:

```
sudo vim /etc/crontab
```

Adicione a seguinte linha:

```
35 23 * * * root sh /scriptbkp.sh
```

Salve e saia. Pronto, todos os dias da semana, todos os meses, todos os dias do mês, na hora 23 e minuto 35 ele vai executar o script e enviar o backup para o hd externo do exemplo.

Mas e se quisermos a atividade de segunda e sábado as 09:27. A linha ficará assim:

```
27 09 * * 1,6 root sh /scriptbkp.sh
```

Se quisermos toda hora, de 08 as 18 de segunda a sexta:

```
00 8-18 * * 1-5 root sh /scriptbkp.sh
```

Se quisermos fazer mensalmente independente da hora, feche o crontab e mova o arquivo para a pasta especial, com o seguinte comando:

```
sudo mv /scriptbkp.sh /etc/cron.monthly
```

FIM! Se tiverem dúvida podem entrar em contato valeu!

Rodolfo Silveira
@rodolfo_tec
e-mail: ro_dolfo14@hotmail.com

Crédito

<https://www.ubuntudicas.com.br/2012/01/crontab-o-agendador-de-tarefas-do-linux/>

Agendando tarefas em Linux/Unix usando o cron

Autor: Ricardo Souza Silveira <rikrdosilveira at gmail.com>

Data: 27/03/2008

Cron - Resumo e introdução

Resumo: Este artigo trás informações sobre o comando cron. Alguns comandos e parâmetros que poderão ser utilizados também estarão citados neste artigo, assim como alguns exemplos de como poderá ser utilizado.

Abstract: This article back information on the command cron. Some command and parameters that could be used also will be cited in this article as well as some examples of how it may be used.

Introdução

O cron é uma ferramenta de sistemas Linux e Unix que permite a execução de comandos ou programas, agendados para um determinado dia/mês/ano/hora.

Para demonstrar melhor a utilidade de comando cron no Linux, suponhamos que por questões de segurança você precisa fazer um backup de alguns arquivos de uma aplicação, que é acessada por clientes diariamente. Neste caso você poderá utilizar o cron para fazer esse backup automaticamente em horários programados.

Como utilizar o cron

O agendamento das tarefas é feita através do arquivo de configuração localizado no diretório `/etc/crontab` ou em arquivos de usuários localizados em `/var/spool/cron/crontabs/[nome do usuário]`.

Para adicionar uma tarefa ao cron é preciso que você abra com um editor de texto qualquer (se estiver usando interface gráfica Gnome, e se tiver instalado, poderá utilizar o `gedit`, ou se estiver em moda caracter o `vim`, `vim`, `nano`, `pipe` como preferir) o arquivo `/etc/crontab` e agendar, definindo o mês/dia/hora em que o comando devera ser executado. Para que a ferramenta cron funcione não é necessário reiniciá-la.

Para que o agendamento funcione é necessário que siga um padrão, um formato ao qual deve se respeitar. Veja o exemplo abaixo:

[minutos] [horas] [dias do mês] [mês] [dias da semana] [usuário] [comando]

```
31 18 1 * * root run-parts --report /etc/cron.monthly
```

```
| | | | | | |
| | | | | | | \_ Comando que será executado
| | | | | | | \_ UID que executará o comando
| | | | | | |
| | | | | | | \_ Dia da semana (0-7)
| | | | | | |
| | | | | | | \_ Mês (1-12)
| | | | | | |
| | | | | | | \_ Dia do Mês (1-31)
| | | | | | |
| | | | | | | \_ Hora (0-23)
| | | | | | |
| | | | | | | \_ Minuto (0-59)
```

Onde corresponde:

Exemplo:

Executar todos os dias, as 0 horas, 0 minutos, todo dia da semana como root o comando `backup`

```
0 0 * * * root /usr/local/bin/backup --report
```

Outras considerações

Na opção que corresponde ao dia da semana pode ser utilizado as 3 primeiras letras em inglês (`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`).

Você pode executar tarefas de hora em hora, diariamente, semanalmente e mensalmente, simplesmente colocando seus arquivos dentro dos diretório respectivos `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`.

Veja um exemplo: dentro de `/etc/cron.daily/` tenho um arquivo backup, onde tenho o script de backup do meu sistema, ou seja, no meu caso ele ira fazer backup todos os dias as 12:20. Obs.: é necessário que esse arquivo tenha permissão para execução, e para isso basta executar o comando: `chmod +x /etc/cron.daily/backup`.

Os campos que não for se importar, pode ser colocado um `"*"`, como se tivesse selecionado "todas as possibilidades", sendo que podem ser colocado `"-"` (hífen) para determinar os intervalos de execução. A `","` (vírgula) define uma lista valores, lista de opções com os números (1,3,5).

O arquivo que é gerado pelo cron em no diretório do usuário `/var/spool/cron/crontabs/[usuário]` pelo crontab tem o mesmo formato do `/etc/crontab`, exceto por não possuir o campo 'usuário (UID)', pois o nome do arquivo já identifica o usuário no sistema. Caso você queira editar um arquivo de usuário feito pelo cron, basta utilizar o comando `"crontab -e"`, ele irá abrir o que foi agendado para aquele usuário.

Cuidado, caso você edite o "crontab", certifique-se para que haja uma linha em branco no final do arquivo, caso esta linha não exista o ultimo comando não se executará. E tenha muita atenção ao colocar qualquer texto após o programa que será executado será considerado comentário e não será interpretado pelo cron.

Alguns exemplos de comandos

Para rodar todo dia de hora em hora:

```
00 * * * * script
```

Para rodar de dez em dez minutos todos os dias:

```
00-59/10 * * * * script
```

Note a divisão por 5 do intervalo 00-59.

Para rodar uma sequência de horas:

```
20 10,12,16,18,22 * * * * script
```

Para rodar numa sequência de dias do mês às 14:00:

```
00 14 03-15 * * script
```

Para rodar ao meio-dia e a meia-noite de terça a sábado:

```
00 00, 12 * * 2-6 script
```

Para enviar um e-mail as 20:20 no dia 23/03 para Pedro dizendo "Viva o Linux porque nós amamos a liberdade!":

```
20 20 23 3 * root echo "Viva o Linux porque nós amamos a liberdade!"|mail Pedro
```

Conclusão

Com a utilização da ferramenta cron, concluí que no agendamento de tarefas em sistemas Linux/Unix pode ser feito perfeitamente com o comando cron, sendo um ferramenta fácil de implementar. É ótima para fazer backup automáticos, agendamento de tarefas diárias economizando tempo e trabalho repetitivos.

Referências

1. Agendando tarefas e rotinas com o Cron:

<http://www.guiadohardware.net/dicas/agendando-tarefas-rotinas-cron.html>

Acessado pela última vez no dia 05/03/2008 às 14:00 horas

2. Usando cron e crontab para agendar tarefas

<http://www.infowester.com/linuxcron.php>

Acessado pela última vez no dia 05/03/2008 às 14:30 horas

3. Utilizando o crontab

<http://www.devin.com.br/eitch/crontab/>

Acessado pela última vez no dia 05/03/2008 às 15:30 horas

4. Crontab

<http://pt.wikipedia.org/wiki/Crontab>

Acessado pela última vez no dia 05/03/2008 às 15:45 horas

<https://www.vivaolinux.com.br/artigos/impressora.php?codigo=7965>

```
=====
```

```
* * * * * env DISPLAY=:0.0 /home/x/Documents/MyScripts/Cron/BeepAlarm "Wake Up"
```

```
# Example of job definition:
```

```
# .----- minute (0 - 59)
```

```
# | .----- hour (0 - 23)
```

```
# | | .----- day of month (1 - 31)
```

```
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
```

```
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7)
```

```
# | | | | |
```

```
# * * * * * command to be executed
```

```
* * * * * command to be executed
```

```
- - - - -
```

```
||| |
```

```
||| | ---- Day of week (0 - 7) (Sunday=0 or 7)
```

```
|| | ---- Month (1 - 12)
```

```
|| ---- Day of month (1 - 31)
```

```
| ---- Hour (0 - 23)
```

```
----- Minute (0 - 59)
```

```
# Minute Hour Day of Month Month Day of Week User Command
```

```
# (0-59) (0-23) (1-31) (1-12 or Jan-Dec) (0-6 or Sun-Sat)
```

```
0 2 * * * root /usr/bin/find
```

```
MAILTO=user@somehost.tld
1 2 * * * /path/to/your/command
```

Provide the full path to your command.

```
1 2 * * * /path/to/your/command
```

Testar se está rodando
pgrep cron
Deve aparecer o número do PID

```
grep CRON /var/log/syslog
```

```
grep -i cron /var/log/syslog|tail -2
sudo crontab -e
```

```
0 13 * * * /usr/local/bin/transf.sh
```

```
SOME_DIR=/var/log
MY_LOG_FILE=/var/log/some_file.log
```

```
BIN_DIR=/usr/local/bin
MY_EXE=/usr/local/bin/some_executable_file
```

```
0 10 * * * ${MY_EXE} some_param >> ${MY_LOG_FILE}
```

crontab -u username -e (to edit) -l(to list) -r(to remove) 10(minutes) 8-15(hours) *(Day of month) *(month) 1,3,5(days of week) /path/to/script/script_name.sh

```
* 14 * * * home/hacks/notify.sh >/dev/null 2>&1
```

```
service cron start /stop /restart
```

<https://askubuntu.com/questions/23009/why-crontab-scripts-are-not-working>

1.5 - Procurar string s sobrescrever com outra em arquivo

```
sed -i 's/PasswordAuthentication no/PasswordAuthentication yes/g' /etc/ssh/sshd_config;
```

1.6 - Dica sobre a linguagem C:

Precisei criar uma máquina virtual com o Windows dentro do VirtualBox no Linux para minha esposa usar o MS Office.

Então para facilitar seu acesso criei um script shell que abre a máquina virtual e o coloquei na área de trabalho.

Acontece que ao clicar no script abre-se uma janela com 4 opções. Eu gostaria de que ao clicar já abrisse o VirtualBox com a VM.

Lembrei de criar um executável que chamasse o script e então fui pesquisar em como fazer isso na Linguagem C.

Criei o script shell

```
nano win7.sh
```

```
vboxmanage startvm Windows7  
chmod +x win7.sh
```

Criar o fonte em C:

```
nano windows7.c
```

```
#include <stdio.h>  
#include <stdlib.h>  
int main(int argc, char const *argv[])  
{  
    puts("Executar o seguinte script :");  
    puts("/home/ribafs/win7.sh");  
    puts("Iniciando agora...");  
    system("/home/ribafs/win7.sh"); //it will run the script inside the c code.  
    return 0;  
}
```

Compilando

```
g++ windows7.c -o windows7
```

Executando:

```
./windows7
```

Ou com um clique na área de trabalho.

Beleza. Assim ele já abre com um único clique sem abrir janela de confirmação.

Obs.: abre com um único clique porque configurei o nemo para abrir com clique único.

1.7 - DNS Gratuito de CloudFlare

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

Caso deseje utilizar o DNS da CloudFlare faça o seguinte:

Abra as configurações de sua conexão com a internet em seu sistema operacional. Vá ao menu que configura IPv4;

Nele você verá um campo semelhante a "Servidor DNS"

Coloque estes numeros:

Primário: 1.1.1.1
Secundário: 1.0.0.1

No Ubuntu por exemplo, existe um campo no menu de redes que pede "servidores DNS", os numeros devem ser colocados ordenadamente, assim:
1.1.1.1, 1.0.0.1

O plano grátis inclui
Esses grandes recursos:

- Proteção DDoS limitada
- CDN Global
- Certificado SSL compartilhado
- Modo "Estou sob ataque" (I'm Under Attack™)
- Regras para 3 páginas incluídas
- Regras adicionais disponíveis para compra através do painel

<https://www.cloudflare.com/a/sign-up>

1.8 – Corrigir Erros de Locales

```
locale-gen "en_US.UTF-8"
```

```
Generating locales...  
  en_US.UTF-8... done  
Generation complete.
```

```
dpkg-reconfigure locales
```

```
Generating locales...  
  en_US.UTF-8... up-to-date  
Generation complete.
```

1.9 - Procurando Arquivos pelo Terminal do UNIX com find e locate

Procurar arquivo no diretório atual:

```
find -name "arquivo.zip"
```

Procurar arquivo ignorando o case:

```
find -iname "Arquivo.zip"
```

Procurar arquivos que não tenham um nome:

```
find -not -name "nome-a-ignorar"
```

Procurar arquivo pelo tipo:

```
find -type tipo_descritor arquivo.txt
```

tipo_descritor:

- f: regular file

- d: directory

- l: symbolic link

- c: character devices

- b: block devices

Procurar todos os arquivos tipo caractere no raiz:

```
find / -type c
```

Procurar todos os arquivos terminados com .conf:

```
find / -type f -name "*.conf"
```

Procurando por tamanho/size:

- c: bytes

- k: Kilobytes

- M: Megabytes

- G: Gigabytes

- b: 512-byte blocks

```
find / -size 50c
```

Procurar todos os arquivos menores que 50 bytes:

```
find / -size -50c
```

Procurar todos os arquivos maiores que 700MB:

```
find / -size +700M
```

Procurar arquivos de acordo com o tempo:

Access Time: Last time a file was read or written to. (-atime)

Modification Time: Last time the contents of the file were modified.(-mtime)

Change Time: Last time the file's inode meta-data was changed.(-ctime)

Procurar arquivos que foram modificados há 1 dia:

```
find / -mtime 1
```

Procurar arquivos que foram acessados há menos de 1 dia:

```
find / -atime -1
```

Procurar arquivos que tiveram suas metainformações mudadas há mais de 3 dias:

```
find / -ctime +3
```

Arquivos que foram modificados há menos de 1 minuto:

```
find / -mmin -1
```

Procurar arquivos que tenham como dono o user syslog:

```
find / -user syslog
```

Procurar arquivos do grupo shadown:

```
find / -group shadow
```

Procurar arquivos com permissão 777:

```
find . -type f -perm 0777 -print
```

Procurar arquivos com permissão diferente de 777:

```
find / -type f ! -perm 777
```

Procurar todos os arquivos executáveis:

```
find / -perm /a=x
```

Procurar todos os arquivos com permissão 777 e mudar para 644:

```
find / -type f -perm 0777 -print -exec chmod 644 {} \;
```

Procurar diretórios com permissão 777 e mudar para 755:

```
find / -type d -perm 777 -print -exec chmod 755 {} \;
```

Procurar o arquivo tecmint.txt e removê-lo:

```
find . -type f -name "tecmint.txt" -exec rm -f {} \;
```

Procurar todos os arquivos .mp3 e removê-los:

```
find . -type f -name "*.mp3" -exec rm -f {} \;
```

Procurar todos os arquivos vazios:

```
find /tmp -type f -empty
```

Procurar todos os diretórios vazios:

```
find /tmp -type d -empty
```

Procurar todos os arquivos ocultos:

```
find /tmp -type f -name ".*"
```

Procurar todos os arquivos do usuário ribafs no diretório /home/ribafs:

```
find /home/ribafs -user ribafs
```

Procurar arquivos que tenham permissão igual a 666:

```
find / -perm 666
```

Procurar arquivos que tenham permissão igual a 777:

```
find / -perm 777
```

Contar os arquivos com certo nome no diretório atual:

```
find -name file1 | wc -l
```

Mudar as permissões do diretório /var/www/html recursivamente para 755 e de todos os arquivos para 644:

```
find /var/www/html -type d -exec chmod 755 {} \;
```

```
find /var/www/html -type f -exec chmod 644 {} \;
```

Procurando com locate

```
sudo apt-get update
```

```
sudo apt-get install mlocate
```

```
sudo updatedb
```

```
locate nomearquivo
```

Referências:

<https://www.digitalocean.com/community/tutorials/how-to-use-find-and-locate-to-search-for-files-on-a-linux-vps>

<https://www.tecmint.com/35-practical-examples-of-linux-find-command/>

1.10 - Formatar pendrive

```
su
```

```
fdisk -l
```

Se preciso remover todas as partições com

```
fdisk /dev/sdb
```

```
d
```

```
1
```

```
d
2
n
p
Enter
Enter
w
```

```
umount /dev/sdb1
```

```
mkfs.vfat /dev/sdb1
```

```
mkfs.ntfs /dev/sdb1
```

```
mkfs.ext4 /dev/sdb1
```

Mudar o label

```
e2label /dev/sdb1 RibaFS
```

Deixar com leitura e escrita

```
chown -R ribafs:ribafs /media/ribafs/RibaFS
```

Reiniciar computador após isso para que o pendrive tenha permissão de escrita.

1.11 - Criar um link simbólico

Na pasta `/var/www/html` para a pasta `/var/www/local/joomla`

```
cd /var/www/html
```

```
ln -s /var/www/local/joomla joomla
```

```
ls -la
```

```
drwxrwxr-x 3 ribafs www-data 4096 Set 29 08:24 .
```

```
drwxr-xr-x 6 root root 4096 Set 20 09:01 ..
```

```
-rw-rw-r-- 1 ribafs www-data 21414 Ago 31 10:28 adminer.css
```

```
-rw-rw-r-- 1 ribafs www-data 436227 Ago 31 10:28 adminer.php
```

```
-rw-rw-r-- 1 ribafs www-data 11321 Ago 31 09:42 index.html
```

```
lrwxrwxrwx 1 ribafs ribafs 24 Set 29 08:24 joomla -> /var/www/local/joomla
```

1.12 - Editor de textos para o terminal/modo texto no Unix

Resumo

nano arquivo_texto

Ctrl+O ou F3 - salvar o arquivo

Ctrl+X - sair do nano

Ctrl+G - Help

Mover o cursor na horizontal para a esquerda e para a direita - Ctrl+F e Ctrl+B

Mover o cursor na vertical para cima e para baixo - Ctrl+P e Ctrl+N

Também podemos usar as setas do teclado.

Ctrl+W ou F6 - Procurar por parte do texto

Alt+\ - para a primeira linha do texto

Alt+/ - para a última linha

F7 - uma tela acima

F8 - uma tela abaixo

Ctrl+K - apaga a linha atual, melhor, recorta para a memória

Ctrl+U - cola o que está na memória. O conteúdo recortado por Ctrl+K

Ctrl+6 - Inicia a seleção de um texto. Arraste até o final.

No final tecle Ctrl+K para recortar

Mova o cursor para onde deseja colar e tecle Ctrl+U

Para selecionar todo o arquivo

Alt+\

Ctrl+6

Alt+/

Alt+6 - copiar o texto selecionado

Ctrl+U - colar

Mostrar abaixo o número da linha num arquivo

nano -c arquivo

Ctrl+\ - Sobrescrever um trecho de texto/string

Ctrl+J - justifica um parágrafo

Ctrl+C - mostra abaixo a posição atual do cursor

Ctrl+/ - mudar o cursor para uma linha e coluna. Ex: 10.0

Ctrl+- - reduz o tamanho da fonte

Ctrl+0 - volta a fonte ao tamanho normal. São atalhos do teclado e não do nano

1.13 - Setando Permissões para o Servidor web

Para trabalho em equipe no servidor web

Num Debian e derivadas

Criar um grupo
addgroup webdevel

Adicionar cada um dos integrantes da equipe ao grupo webdevel
addgroup ribafs webdevel

sudo nano /usr/local/bin/perms

```
sudo clear;
echo "Aguarde enquanto configuro as permissões do /var/www/html/$1";
echo "";
chown -R www-data:webdevel /var/www/html/$1;
chgrp -R webdevel /var/www/html/$1
find /var/www/html/$1 -type d -exec chmod 2775 {} ;
find /var/www/html/$1 -type f -exec chmod 2664 {} ;
echo "";
echo "Concluído!";
```

chmod +x /usr/local/bin/perms;;

Num RedHat/CentOS

Antes instalar o Apache

```
addgroup webdevel
usermod -a -G webdevel apache
usermod -a -G webdevel ribafs
```

Usando Permissões

```
sudo clear;
echo "Aguarde enquanto configuro as permissões do /var/www/html/$1";
echo "";
chown -R apache:webdevel /var/www/html/$1;
chgrp -R webdevel /var/www/html/$1
```

```
find /var/www/html/$1 -type d -exec chmod 2775 {} ;
find /var/www/html/$1 -type f -exec chmod 2664 {} ;
if [-d "/var/www/html/$1/bin"]
then
    chmod +x /var/www/html/$1/bin/cake
fi
echo "";
echo "Concluído!";

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

1.14 – Configurações de Rede pela linha de comando

Configurações do serviço da Vultr para seus servidores

CentOS, RHEL

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=45.63.104.148
NETMASK=255.255.254.0
GATEWAY=45.63.104.1
DNS1=108.61.10.10
```

/etc/sysconfig/network-scripts/route-eth0

```
169.254.0.0/16 dev eth0
```

Ubuntu 12.xx - 15.xx

```
/etc/network/interfaces
```

```
auto lo
iface lo inet loopback
```

```
auto eth0
iface eth0 inet static
    address 45.63.104.148
    netmask 255.255.254.0
    gateway 45.63.104.1
    dns-nameservers 108.61.10.10
    post-up ip route add 169.254.0.0/16 dev eth0
```

DHCP

```
auto eth0
iface eth0 inet dhcp
```

Ubuntu 16.xx, Ubuntu 17.04

```
/etc/network/interfaces
```

```
auto lo
iface lo inet loopback
```

```
auto ens3
iface ens3 inet static
    address 45.63.104.148
    netmask 255.255.254.0
    gateway 45.63.104.1
    dns-nameservers 108.61.10.10
    post-up ip route add 169.254.0.0/16 dev ens3
```

Ubuntu 17.10

```
/etc/netplan/10-ens3.yaml
```

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens3:
      dhcp4: no
      addresses: [45.63.104.148/23]
      gateway4: 45.63.104.1
      nameservers:
        addresses: [108.61.10.10]
      routes:
        - to: 169.254.0.0/16
```

```
via: 45.63.104.1
```

```
metric: 100
```

Debian 7, Debian 8

```
/etc/network/interfaces
```

```
auto lo
```

```
iface lo inet loopback
```

```
auto eth0
```

```
iface eth0 inet static
```

```
address 45.63.104.148
```

```
netmask 255.255.254.0
```

```
gateway 45.63.104.1
```

```
dns-nameservers 108.61.10.10
```

```
post-up ip route add 169.254.0.0/16 dev eth0
```

Debian 9

```
/etc/network/interfaces
```

```
auto lo
```

```
iface lo inet loopback
```

```
auto ens3
```

```
iface ens3 inet static
```

```
address 45.63.104.148
```

```
netmask 255.255.254.0
```

```
gateway 45.63.104.1
```

```
dns-nameservers 108.61.10.10
```

```
post-up ip route add 169.254.0.0/16 dev ens3
```

FreeBSD

```
/etc/rc.conf
```

```
static_routes="linklocal"
```

```
route_linklocal="-net 169.254.0.0/16 -interface vtnet0"
```

```
ifconfig_vtnet0="inet 45.63.104.148 netmask 255.255.254.0"
```

```
defaultrouter="45.63.104.1"
```

OpenBSD

```
/etc/mygate
```

```
45.63.104.1
```

```
/etc/hostname.vio0
```

```
inet 45.63.104.148 255.255.254.0 NONE
```

```
/etc/resolv.conf
```

```
nameserver 108.61.10.10
```

```
lookup file bind
```

Fedora 24-27

```
/etc/sysconfig/network-scripts/ifcfg-ens3
```

```
DEVICE=ens3
```

```
ONBOOT=yes
```

```
NM_CONTROLLED=no
```

```
BOOTPROTO=static
```

```
NOZEROCONF=yes
```

```
IPADDR=45.63.104.148
```

```
NETMASK=255.255.254.0
```

```
GATEWAY=45.63.104.1
```

```
DNS1=108.61.10.10
```

```
/etc/sysconfig/network-scripts/route-ens3
```

```
169.254.0.0/16 dev ens3
```

Windows Server

To configure the main IPv4 manually:

Open the windows control panel. You can access it from the start menu.

Click "Network and Internet".

Click "Network and Sharing Center".

Click "Change adapter settings".

Right click on the primary ethernet adapter, and click "Properties". The "Ethernet Properties" window will open.

Select "Internet Protocol Version 4 (TCP/IPv4)", then click the "Properties" button. The "Internet Protocol Version 4 (TCP/IPv4) Properties" window will open.

Check the box that reads "Use the following IP address:". Populate the fields:

IP address: 45.63.104.148

Subnet mask: 255.255.254.0

Default gateway: 45.63.104.1

Check the box that reads "Use the following DNS server addresses:". Populate the fields

Preferred DNS server: 108.61.10.10

Alternate DNS server: (blank)

Click "OK". Then click "OK" on the "Ethernet Properties" window. The main IPv4 has been configured manually. Note that it is normal for the connection to hiccup after pressing "OK".

Máscara Explicada

Apenas para iluminar um pouco, aquele número que vem depois da barra "/" significa o número de bits que ele vai utilizar na mascara. Vejamos.

Suponha que voce deixe 189.0.0.0/24, o que vai acontecer?

- 1) Voce vai tentar conectar no IP do seu servidor a partir de seu IP de origem IP
- 2) Seu servidor vai pegar o seu IP de origem e fazer um calculo de mascara usando 24 bits, numa comparação XOR bit-a-bit que vai resultar em 189.22.33.0
- 3) Ele vai pegar o resultado do calculo acima e comparar com seu arquivo e vai identificar que 189.22.33.0 NÃO É IGUAL A 189.0.0.0.

Portanto você tem que utilizar 189.0.0.0/8, pois assim ele vai pegar o seu IP IP, vai fazer uma comparacao XOR bit-a-bit e vai ter como resultado 189.0.0.0, com esse resultado ele vai comprar com o 189.0.0.0 e vai reconhecer a IGUALDADE entre eles e vai aceitar.

Em resumo.

IP/8 => IP/255.0.0.0 = 192.0.0.0
 IP/16 => IP/255.255.0.0 = 192.168.0.0
 IP/24 => IP/255.255.255.0 = 192.168.1.0
 IP/32 => IP/255.255.255.255 = 192.168.1.12

Outras mascaras são possíveis através de deslocamento de bit do parte da rede para o host, obtendo-se sub-redes, mas ai ja acabamos fungindo do escopo da lista.

--

Dickson S. Guedes

Comandos

tracert ip

ip route

Acessar página info.php internamente em modo texto
 curl http://127.0.0.1/info.php

Ver

sudo netstat -plutn

PING

O comando PING foi desenvolvido para identificar se um dispositivo na rede está respondendo ou não. O computador de origem envia um pacote de dados e através do protocolo ICMP, o servidor de destino devolve com uma resposta.

A partir de então, é possível verificar outros dados como tempo de resposta, a famosa "latência" de dados que é o tempo que leva para o dado ir e voltar.

Traceroute

```
traceroute ip_dominio
```

Traça a rota daqui até o ip_dominio mostrando os nós por onde passa

MTR (My traceroute ou também conhecido antigamente por Matt's traceroute)

O que vem à ser o MTR? Simples: A combinação do PING e do TRACERT em uma só ferramenta.

Ao mesmo tempo que você realiza o PING, você também realiza o TRACERT, e com a diferença de que: ele continua sendo executado para que você possa conferir o status atual da rede naquele exato momento.

Verificar Serviços em Execução

```
netstat -tap | grep serviço  
netstat -tap | grep apache2
```

Ver serviços rodando

```
netstat -nltp
```

Levantar

```
ip link set ifname up
```

Derrubar

```
ip link set ifname down
```

```
ifconfig eth0
```

```
ifconfig eth0 up
```

```
ifconfig eth0 down
```

```
ifconfig eth0 172.16.25.125
```

```
ifconfig eth0 192.168.50.5 netmask 255.255.255.0
```

```
ifconfig eth0 broadcast 172.16.25.63
```

```
ifconfig eth0 172.16.25.125 netmask 255.255.255.224 broadcast 172.16.25.63
```

```
ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF
```

```
ifup eth0
```

```
ifdown eth0
```

```
ifconfig eth0 mtu XXXX
```

```
ifconfig eth0 mtu 1000
```

```
ifconfig eth0 promisc
```

```
ifconfig eth0 -promisc
```

```
ifconfig eth0:0 172.16.25.127
```

```
ifconfig eth0:0
```

```
ping 4.2.2.2
```

```
ping www.tecmint.com
```

```
traceroute 4.2.2.2
```

```
netstat -r
```

```
dig www.tecmint.com
```

```
nslookup www.tecmint.com
```

```
route
```

```
route -n
```

```
route add -net 10.10.10.0/24 gw 192.168.0.1
```

```
route del -net 10.10.10.0/24 gw 192.168.0.1
```

```
route add default gw 192.168.0.1
```

```
host www.google.com
```

```
host -t CNAME www.redhat.com
```

```
arp -e
```

```
ethtool eno1
```

Wireless

```
iwconfig [interface]
```

```
system-config-network
```

```
/etc/network/interfaces
```

```
auto lo
```

```
iface lo inet loopback
```

```
auto eth0
iface eth0 inet static
    address 45.63.104.148
    netmask 255.255.254.0
    gateway 45.63.104.1
    dns-nameservers 108.61.10.10
    post-up ip route add 169.254.0.0/16 dev eth0
```

DHCP

```
auto eth0
iface eth0 inet dhcp
```

```
FreeBSD
/etc/rc.conf
```

```
static_routes="linklocal"
route_linklocal="-net 169.254.0.0/16 -interface vtnet0"
ifconfig_vtnet0="inet 45.63.104.148 netmask 255.255.254.0"
defaultrouter="45.63.104.1"
```

```
OpenBSD
/etc/mygate
```

```
45.63.104.1
```

```
/etc/hostname.vio0
```

```
inet 45.63.104.148 255.255.254.0 NONE
```

```
/etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=45.63.104.148
NETMASK=255.255.254.0
GATEWAY=45.63.104.1
DNS1=108.61.10.10
```

```
/etc/sysconfig/network-scripts/route-eth0
```

```
169.254.0.0/16 dev eth0
```

```
sudo route add default gw 192.168.1.1
```

```
route -n
```

Adicionar ao `/etc/network/interfaces`

```
up route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.1 vboxnet0
```

Como adicionar rotas estáticas persistentes no ubuntu

I found a solution. Its easier to make a script that adds those routes at system bootup than to try and add them to the `rc.local` file to make them get executed automatically. the procedure is as follows:

1. create a script file in the `/etc/init.d/` folder.
2. add your route definitions to this file and change it to an executable file(`chmod +x /path/to/file`).
3. run the `update-rc.d <filename> defaults` command to make the script executable at boot time.
4. reboot the system and check whether the system adds the routes at startup(`netstat -rn`).

and thats all there is to it.

PS. it goes without saying that you must first add the routes using the `route add` command before doing the above procedure.

Detalhe:

A rede do desktop deve funcionar apenas o perfil teste. O outro deve estar parado (graficamente)

Como somente pingava em IP e não em nomes, precisei adicionar o DNS ao `resolv.conf`.

```
sudo nano /etc/resolv.conf
nameserver 10.0.0.12
nameserver 10.0.0.13
```

Tanto a rota acima quanto o `resolv.conf` devem ser executados a cada boot. Precisam ficar no iniciar, talvez no `/etc/rc.local`

```
nano /etc/rc.local
```

Adicionar

```
route add default gw 192.168.0.1
```

Executar pelo terminal:

```
sudo su
echo "nameserver 10.0.0.12" >> /etc/rc.local
echo "nameserver 10.0.0.13" >> /etc/rc.local
```

Não funciona no rc.local. Preciso colocar em outro arquivo, mas como esta solução é provisória, não requer muito esforço para isso.

Sequência:

- Levantar a VM com o Zentyal
- levantar a rota
- Adicionar o DNS ao resolv.conf

Para então ter internet no desktop

1.15 – Usando o RSync

```
rsync -av -e 'ssh -p 65522' --progress --delete-after /backup/transp/rsync/  
ribafs@178.62.122.149:/home/ribafs/rsync/
```

Com porta diferente da 22

```
rsync -arvz -e 'ssh -p <port-number>' --progress --delete user@remote-  
server:/path/to/remote/folder /path/to/local/folder
```

Do desktop para o server

```
rsync -avz -e 'ssh -p 65522' /backup/transp/rsync/  
ribafs@178.62.122.149:/home/ribafs/rsync/
```

Passar a senha pelo cron

```
RSYNC_PASSWORD=zmxn1029P@  
0 12 * * * rsync -aq -e 'ssh -p 65522' --delete /backup/transp/rsync/  
ribafs@178.62.122.149:/home/ribafs/rsync/
```

No

/etc/cron.hourly

```
RSYNC_PASSWORD=zmxn1029P@  
30 9 * * * root rsync -aq -e 'ssh -p 65522' --delete  
ribafs@178.62.122.149:/home/ribafs/rsync/ /backup/transp/rsync/
```

2 – Desktop

Um bom computador desktop para o administrador de redes ou programador é muito importante.

Tanto o hardware precisa ser adequado quanto o sistema operacional, arquitetura, distribuição, versão e aplicativos.

Se for comprar um novo hardware é importante consultar a lista de compatibilidade com a distribuição que pretende usar e consultar um bom grupo sobre a experiência dos colegas com o hardware.

Melhorar a segurança no Desktop

Melhorar a segurança no desktop é importante para maior segurança do servidor.

Hábitos saudáveis como usar um sistema operacional seguro e atualizado, como usando o firewall ativo e fechando tudo que pode.

Assim como também instalando boas ferramentas de monitoramento do servidor.

Instalar no micro desktop o W3AF

```
apt-get install w3af
```

Traz uma interface para a console e uma gráfica/web

Testando vulnerabilidades web com Nikto

O Nikto é web server scanner escrito em perl usado para detectar vulnerabilidades em servidores web. Ele é muito simples de ser usado e atualizado gerando relatórios em txt, html e csv.

Requer repositório multiverse no /etc/apt/sources.list

```
apt-get install nikto
```

Atualizando os plugins:

```
nikto -update
```

Usando o Nikto

```
nikto -h HOST -p PORT
```

```
nikto -h HOST -p PORT -ssl
```

```
nikto -h ribafs.org
```

```
nikto -C all -host 200.128.X.X -o vitima.txt (mude X.X pelos números desejados)
```

- C all - Força a checagem de todos os diretórios em busca de cgi

- host - Ip da vitima

-o - Gera um arquivo de relatório

Varrendo uma porta de um host:
nikto -h google.com -p 443

Help
nikto -H | less

Esta ferramenta tanto ajuda a defender o seu site quanto ajuda para quem quer perceber vulnerabilidades em outros sites ou atacar.

Documentação oficial:
<http://cirt.net/nikto2-docs/>

Exemplos de uso:
<http://cirt.net/nikto2-docs/usage.html>

Qual a melhor distribuição desktop?

É sempre relativa ao usuário que fará uso, mas existem pontos importantes

- Aquela que suporta perfeitamente seu hardware
- Que seja customizável, caso você pretenda customizar
- Que ofereça todos os principais recursos que você espera dela para uso com facilidade:
 - Multimídia: codecs de áudio, vídeo e suporte a diversos formatos: mp3, mp4, webm, mkv, etc
 - Documentos: pdf, odt, doc, docx, etc
 - Navegação pela internet
 - Planilhas e apresentações
 - Teclas de atalho customizadas
 - Gerenciador de arquivos com suporte (peça chave numa boa distribuição):
 - Suporte a painel duplo (dois painéis numa mesma tela, dividindo-a em duas)
 - Clique único para abrir pastas e arquivos
 - Conexão a servidores ftp, ssh, etc
 - Criação de atalhos para pastas na lateral esquerda
- Precisa estar em pleno desenvolvimento, ter frequentes atualizações e uma grande comunidade
- Ser robusta e leve são quesitos importantes, mas o mais importante é o suporte ao hardware e a usabilidade aliados aos recursos que a tornam de uso simples

2.1 – Batches ou Arquivos de Lote

Batch ou arquivo de lote (também conhecidos por .bat) é um arquivo de computador utilizado para automatizar tarefas.

Podemos compará-lo, a grosso modo, aos scripts do Unix.

Lista de comandos

- 1 ATTRIB
- 2 CALL
- 3 CHDIR
- 4 CLS
- 5 COMP
- 6 COPY
- 7 DATE
- 8 DELTREE
- 9 DIR
- 10 DISKCOMP
- 11 DISKCOPY
- 12 ECHO
- 13 FIND
- 14 FOR
- 15 FORMAT
- 16 IF
- 17 LABEL
- 18 MKDIR
- 19 MODE
- 20 MORE
- 21 MOVE
- 22 PATH
- 23 PAUSE
- 24 PROMPT
- 25 RENAME
- 26 RMDIR
- 27 TREE
- 28 TIME
- 29 TITLE
- 30 TYPE
- 31 VER
- 32 EDIT
- 33 EXIT
- 34 WIN
- 35 FDISK

Exemplos= 1

Se x

```
@ECHO OFF
CLS
SET X=1
IF "%X%" == "1" GOTO ok
ECHO X não é igual a 1, X é igual a %X%
GOTO saida
:ok
```

```
ECHO X é igual a 1
:saida
```

Mensagem de acordo com a idade:

```
@ECHO OFF
SET idade=15
IF %idade% LSS 10 (
    ECHO Bom dia menino!
    ECHO.
    ECHO Você não vai para escola?
) ELSE (
    IF %idade% LSS 18 (
        ECHO Bom dia garoto!
        ECHO.
        ECHO Você não vai pro colégio?
    ) ELSE (
        IF %idade% LEQ 64 (
            ECHO Bom dia!
            ECHO.
            ECHO Você não vai trabalhar hoje?
        ) ELSE (
            ECHO Bom dia!
            ECHO.
            ECHO Tudo bem?
        )
    )
)
)
```

Remover um serviço do Windows

```
sc delete nomeserviço
```

```
sc delete apache2
```

```
sc delete mysql
```

Programação para o prompt do Windows

Exemplo

```
echo off
cls
echo "SCRIPT .BAT para realizar backup"
pause
cd\docume~1\%username%\documentos
copy| * d:\Arquivos_Backup
pause
echo "Abrir calculadora"
start calc.exe
pause
```

2.2 - Recuperação do Grub 2

- Efetuar o boot com o disco/pendrive com Super Grub Disk 2
- Detect any OS (teclar enter)
- Aparecem os sistemas instalados. Selecione o sistema para recuperar o grub e tecla Enter
- Após entrar no sistema:
 - Abra o terminal
 - sudo grub-install /dev/sda
 - sudo update-grub
- reboot

2.3 – Ajustar Relógio em Dualboot

Quando usamos Linux com Windows em dualboot após reiniciar e acessar e voltar para o Linux o relógio atraza 3 horas

Execute esse comando no terminal:
timedatectl set-local-rtc 1 --adjust-system-clock

Depois quando entrar no Windows, é só ajustar o horário correto uma única vez

2.4 – Proteção de Roteador WiFi

Proteção do Roteador no Desktop

Precisamos mudar a senha default do roteador e usar uma senha forte.

Acesse a administração web do roteador com o IP fornecido juntamente com login e senha.

Também precisamos evitar o uuso de roteadores conhecidos como de baixa qualidade.

Usar uma segurança mais forte como a WPA2.

Desligar o WPS do roteador.

O antivírus Avast tem uma ferramenta que verifica o roteador e mostra algumas dicas para melhorar a segurança:

- Abrir o Avast
- Proteção do lado esquerdo
- Verificador de Wi-Fi
- Clicar no botão Escanear Rede

Para melhorar a segurança visite:

https://help.avast.com/pt/av_free/17/securitynetwork.html

2.5 – SSH em Banda Larga ADSL

Quem usa em seu desktop uma conexão tipo banda larga ADSL não pode acessar o servidor se o mesmo estiver usando a porta 22. Precisa encontrar uma forma de acessar:

- A console VPN do servidor
- Um outro servidor na nuvem e de lá acessar o novo servidor
- Um serviço tipo cloud IDE, que tem um terminal linux
- De uma conexão com IP fixo no trabalho ou noutra lugar
- Ou então ...

Então mudar a porta para uma diferente de 22 (preferencialmente maior que a 50000) e então poderá acessar pelo desktop

```
ssh -p porta user@IP
```

2.6 - Upgrade do Debian

```
sudo apt-get update -y && sudo apt-get dist-upgrade -y
```

```
sudo -i sed 's/jessie/stretch/g' /etc/apt/sources.list
```

```
sudo apt-get update -y && sudo apt-get dist-upgrade -y
```

```
lsb_release -a
```

2.7 – Upgrade Ubuntu

Para atualizar ubuntu para versão mais recente

```
apt-get install update-manager-core
```

Executar a ferramenta de atualização com o comando:
do-release-upgrade -d

2.8 - Configurar Hora em Servidor Debian e derivados

Servidor NTP

```
sudo apt-get install ntp
```

GMT

```
sudo dpkg-reconfigure tzdata
```

```
date
```

CentOS 7

```
timedatectl list-timezones
```

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

Mostrar a atual

```
timedatectl
```

```
date
```

2.9 - Ajustar o hostname

```
nano /etc/hosts
```

```
127.0.0.1 localhost.localdomain localhost
```

```
67.205.138.188 ribafs.org www.ribafs.org ribafs
```

```
/etc/hostname
```

```
nano /etc/hostname
```

```
ribafs
```

```
reboot
```

2.10 - Para limpar o cache da RAM

```
sudo sysctl -w vm.drop_caches=3
```

Criar um script

```
sudo nano /usr/local/bin/m
```

```
sudo sysctl -w vm.drop_caches=3
sudo chmod +x /usr/local/bin/m
```

Rodar:
sudo m

2.11 - MySQL

```
#FreeBSD
```

```
mysql -u root -p --connect-expired-password -e "ALTER USER 'root'@'localhost'
IDENTIFIED BY 'zmxn1029';"
```

```
mysql -u root -p
```

```
CREATE DATABASE portal CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'portal'@'localhost' IDENTIFIED BY 'senhaforte';
GRANT ALL PRIVILEGES ON portal.* TO 'portal'@'localhost';
FLUSH PRIVILEGES;
\q
```

```
mysql -uroot -p
```

```
create database portal;
```

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'
WITH GRANT OPTION;
\q
```

```
GRANT ALL PRIVILEGES ON portalakeeba.* TO portal@localhost IDENTIFIED BY
'zmxn1029P@' WITH GRANT OPTION;
```

```
mysql -uroot -p
```

```
create database portal;
GRANT ALL PRIVILEGES ON portal.* TO 'portal@localhost' IDENTIFIED BY
'zmxn1029P@';
```

```
CREATE USER 'portal'@'localhost' IDENTIFIED BY 'senhaforte';
GRANT ALL PRIVILEGES ON portal.localhost TO 'portal'@'localhost' WITH GRANT
OPTION;
```

```
UPDATE portal SET Select_priv = 'Y' WHERE User = 'UserName' AND Db = 'DBname'
AND Host='localhost';
FLUSH PRIVILEGES;
```

Resetar senha do root

```
sudo /etc/init.d/mysql stop
```

```
sudo mysqld_safe --skip-grant-tables &
```

```
mysql -uroot
```

```
use mysql;
```

```
update user set password=PASSWORD("novasenha") where User='root';
```

```
flush privileges;
```

```
quit
```

```
sudo /etc/init.d/mysql stop
```

```
...
```

```
sudo /etc/init.d/mysql start
```

```
mysql -u root -p
```

<https://support.rackspace.com/how-to/mysql-resetting-a-lost-mysql-root-password/>

ou

```
mysqld_safe --skip-grant-tables
```

```
mysql --user=root mysql
```

```
update user set Password=PASSWORD('new-password') where user='root';
```

```
flush privileges;
```

```
exit;
```

Desinstalando totalmente o mysql em caso de problema

```
sudo apt remove --purge mariadb-server
```

```
rm -rf /var/lib/mysql
```

```
rm -rf /etc/mysql
```

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

<https://linuxide.com/linux-how-to/completely-remove-mysql-properly-install-mariadb-10/>

Executando

Uma boa opção de administração do MySQL é o phpmyadmin, que também acompanha o Xampp.

Para administração pela linha de comando use:

```
mysql -h host -u user -p (o super usuário default é root)
mysql -u root (quando estiver sem senha)
```

TROCANDO SENHA DO USUÁRIO ROOT

```
mysql -u root teste (Usuário root acessar banco teste)
use mysql;
```

```
UPDATE user SET Password=PASSWORD("novasenha") WHERE user="root";
FLUSH PRIVILEGES;
```

Ou

```
mysql -u root clientes
SET PASSWORD FOR root=PASSWORD('senhadoroot');
```

CRIANDO USUÁRIOS

```
mysql --user=root mysql
GRANT ALL PRIVILEGES ON *.* TO super@localhost
IDENTIFIED BY 'senha' WITH GRANT OPTION;
```

```
GRANT ALL PRIVILEGES ON *.* TO super@"%"
IDENTIFIED BY 'some_pass' WITH GRANT OPTION;
```

super - é um total super usuário que pode se conectar no localhost e de qualquer lugar ("%"), mas precisa usar senha

```
GRANT RELOAD,PROCESS ON *.* TO admin@localhost;
```

admin - usuário que pode se conectar no localhost sem senha.

Pode executar os comandos mysqladmin reload, mysqladmin refresh, and mysqladmin flush-*

e mysqladmin processlist . Não tem nenhum privilégio relacionado aos bancos.

```
GRANT USAGE ON *.* TO fraco@localhost;
```

fraco - pode conectar somente via localhost sem senha mas sem privilégios, somente para uso.

Exemplo:

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'
WITH GRANT OPTION;
mysql -u ribafs // Dá erro de senha
```

```
mysql -u ribafs -p //Funciona após entrar a senha ribafs
```

REMOVENDO USUÁRIOSxn

```
DROP USER nomeusuario;
```

PRIVILÉGIOS

```
REVOKE GRANT ALL ON nomebancooutabelaou*ou*.* FROM nomeusuario
```

* - todas as tabelas

. todos os bancos e todas as tabelas

banco.* - todas as tabelas do banco

```
GRANT SELECT,INSERT,UPDATE ON nomebanco.* TO nomeuser;
```

```
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP ON nomebanco.* TO
usuario@localhost
IDENTIFIED BY 'senha';
```

```
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP ON nomebanco.* TO
usuario@dominio.com.br
IDENTIFIED BY 'senha';
```

```
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP ON nomebanco.* TO
usuario@'% '
IDENTIFIED BY 'senha';
```

INSTALAR COMO SERVIÇO

Instalar MySQL como serviço no Windows para trabalhar com Java (J2EE):

```
mysqld-nt --install --ansi --sql-mode=ANSI_QUOTES
```

Instalar como serviço:

```
bin\mysqld-nt --install mysql
```

Remover o serviço:

```
bin\mysqld --remove mysql
```

Remover serviço ansi:

```
bin\mysqld --remove --ansi
```

CRIAR TABELAS COM RELACIONAMENTOS

```
create table produto(
    codigo int not null primary key,
    nome varchar(50) not null unique,
    descricao varchar(200),
    valor real(6, 2)
) ENGINE=INNODB;
```

```
create table cliente(
    codigo int not null primary key,
    nome varchar(50) not null,
    email varchar(100) not null unique,
    cpf varchar(11) not null
) ENGINE=INNODB;
```

```
create table pedido(
  numero int not null primary key auto_increment,
  codigocliente int not null references cliente(codigo),
  valortotal real(7,2) DEFAULT '0.00' NOT NULL
) ENGINE=INNODB;
```

```
create table item(
  numeropedido int not null references pedido(numero),
  codigoproduto int not null references produto(codigo),
  quantidade int not null,
  primary key(numeropedido, codigoproduto)
) ENGINE=INNODB;
```

```
CREATE TABLE product (
  category INT NOT NULL,
  id INT NOT NULL,
  price DECIMAL,
  PRIMARY KEY(category, id)
) ENGINE=INNODB;
```

```
CREATE TABLE product_order (
  no INT NOT NULL AUTO_INCREMENT,
  product_category INT NOT NULL,
  product_id INT NOT NULL,
  customer_id INT NOT NULL,
  PRIMARY KEY(no),
  INDEX (product_category, product_id),
  FOREIGN KEY (product_category, product_id)
  REFERENCES product(category, id) ON UPDATE CASCADE ON DELETE
  RESTRICT,
  INDEX (customer_id),
  FOREIGN KEY (customer_id)
  REFERENCES customer(id)
) ENGINE=INNODB;
```

O tipo InnoDB dá suporte à constraint Foreign Key (references).

REMOVER SERVIÇO NO WINDOWS NT/XP

```
mysql\bin\mysqld -- remove(remove o serviço mysql)
-- remove --ansi (remover o serviço ansi)
```

RESUMO DE USO

1) mysql -u root -p ou mysql -u root

mysql -h host -u user -p banco

Obs: Caso receba a mensagem: Can't connect to MySQL server on 'localhost'
Falta startar o MySQL

- 2) create database nomebanco;
- 3) use nomebanco;
- 4) create table nometabela(campos tipos...);
- 5) select * from nometabela;
- 6) show databases;
- 7) show tables;
- 8) describe nometabela;

IMPORTAR E EXPORTAR

Exportando:

```
bin\mysqldump -u user -p passwd banco > banco.sql
```

Importando:

```
bin\mysql -u user -p password banco < banco.sql
```

Mudar Conjunto de Characters para LATIN1

```
mysql -u root  
\C latin1
```

POPULANDO TABELAS APÓS A CRIAÇÃO

O comando LOAD DATA pode ser utilizado para popular tabelas, trazendo de arquivos:

```
LOAD DATA LOCAL INFILE '/path/arquivo.txt' INTO TABLE nometabela;
```

```
SELECT DATABASE();
```

```
SHOW CHARACTER SET;
```

```
CREATE DATABASE db_name  
[[DEFAULT] CHARACTER SET charset_name]  
[[DEFAULT] COLLATE collation_name]  
ALTER DATABASE db_name  
[[DEFAULT] CHARACTER SET charset_name]  
[[DEFAULT] COLLATE collation_name]
```

```
CREATE TABLE tbl_name (column_list)  
[[DEFAULT] CHARACTER SET charset_name] [COLLATE collation_name]  
ALTER TABLE tbl_name
```

```
[[DEFAULT] CHARACTER SET charset_name] [COLLATE collation_name]
```

Example:

```
CREATE TABLE t1 ( ... ) CHARACTER SET latin1 COLLATE latin1_danish_ci;
```

```
col_name {CHAR | VARCHAR | TEXT} (col_length)
[CHARACTER SET charset_name] [COLLATE collation_name]
```

Example:

```
CREATE TABLE Table1
(
column1 VARCHAR(5) CHARACTER SET latin1 COLLATE latin1_german1_ci
);
```

FUNÇÕES COM DATAS

DATE_SUB

```
SELECT something FROM tbl_name WHERE DATE_SUB(CURDATE(),INTERVAL 30
DAY) <= date_col;
SELECT DATEDIFF('1997-12-31 23:59:59','1997-12-30');
```

DATE_ADD

```
SELECT DATE_ADD('2006-05-00',INTERVAL 1 DAY);
```

```
SELECT CURDATE();
```

```
SELECT CURTIME();
```

DATE_FORMAT

```
SELECT date_format( '2006-04-30', '%d/%m/%Y' ); -- 30/04/2006
SELECT DATE_FORMAT('2003-10-03',GET_FORMAT(DATE,'EUR')); -- 03.10.2003
SELECT DATE_FORMAT('2006-06-00', '%d/%m/%Y');
```

```
SELECT NOW();
```

```
SELECT TO_DAYS('1997-10-07'); -- RETORNA DIAS
```

```
SELECT YEAR('2000-01-01');
```

Backup e restore de todos os bancos

```
mysqldump -u root -psenha --add-drop-database --all-databases > todos.dump
```

Em uma instalação limpa do MySQL ou sobrescrevendo os bancos existentes

```
mysql -u root -psenha < todos.dump
```

2.12 – Adicionar partição de Swap ao Linux

Adicionar partição de swap com 2GB

```
dd if=/dev/zero of=/swapfile bs=1M count=2048
mkswap /swapfile
chmod 600 /swapfile
swapon /swapfile
```

```
nano /etc/fstab
/swapfile  swap  swap  defaults  0  0
```

Testar
free -m

2.13 – Clamav

```
sudo su
apt-get update
apt-get install clamav clamav-daemon
freshclam
```

Checando
clamscan -r /home/ribafs
clamscan -r /

Todo o computador
clamscan -r --bell -i /

Criar lista de arquivos infectados
clamscan -r /home/ribafs/ | grep FOUND >> report.txt

Versão
clamdscan -V

Adicionando ao cron

```
crontab -e
```

```
00 00 * * * clamscan -r /home
```

Instalar gui
apt-get install ClamTK

<https://www.unixmen.com/installing-scanning-clamav-ubuntu-14-04-linux/>

3 – Hospedagem tipo VPS

3.1 - Hospedagem na Digital Ocean

O principal deste conteúdo se aplica a qualquer hospedagem tipo VPS e também para servidores dedicados e para servidores particulares que usem Linux.

Para contratar a DigitalOcean precisa de um cartão de crédito internacional ou uma conta no paypal.

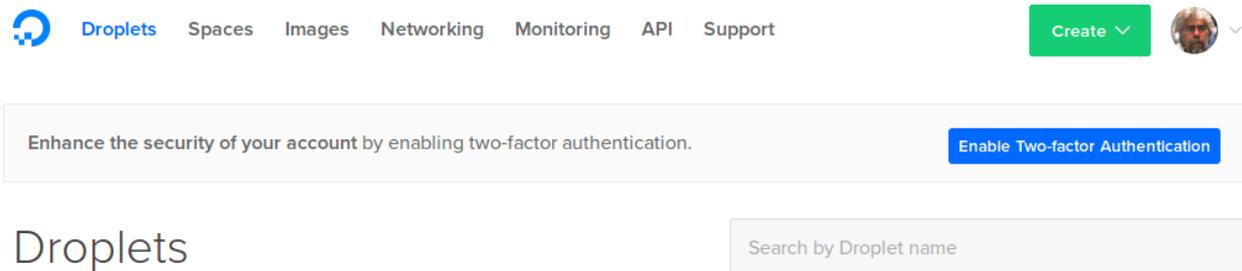
Uma boa ideia para testar é conseguir um cupom/coupo de uns 5 a 15 dólares e usar para criar sua conta. Basta para isso efetuar uma busca no DuckDuckGo ou no Google por "digitalocean coupon".

Com isso contrate o plano desejado – <http://digitalocean.com>

Após contratar e ter recebido o e-mail de boas vindas acesse o site acima e efetue login.

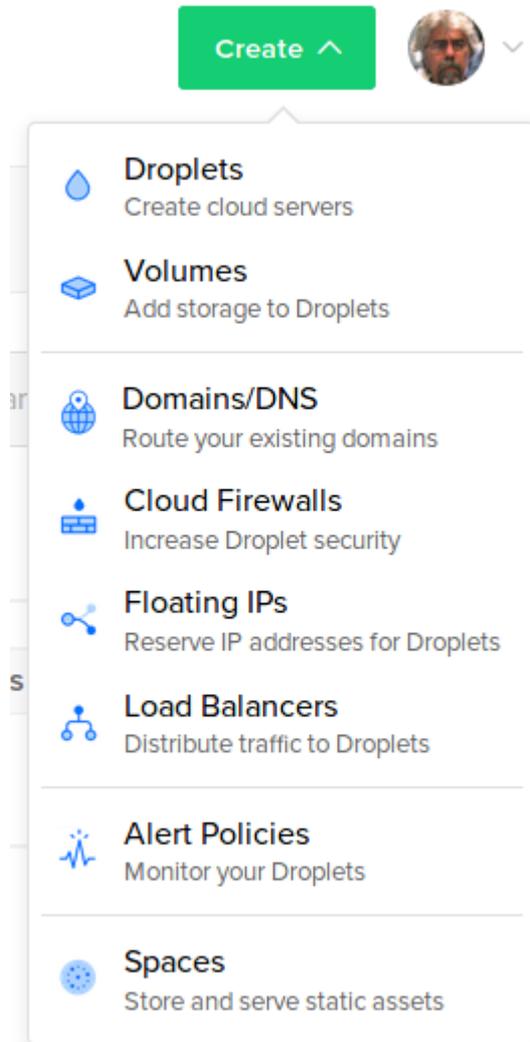
Veja que atualmente a DigitalOcean te obriga a digitar um código de 6 dígitos que ele te envia por e-mail, confirmando se você é você.

Após efetuar o login no site da DigitalOcean a tela de entrada é esta:



Criando um Servidor

A primeira providência é criar um servidor, que a DigitalOcean chama de droplet. Para criar uma droplet, clique no botão verde acima e à direita. Então ele abre um popup:



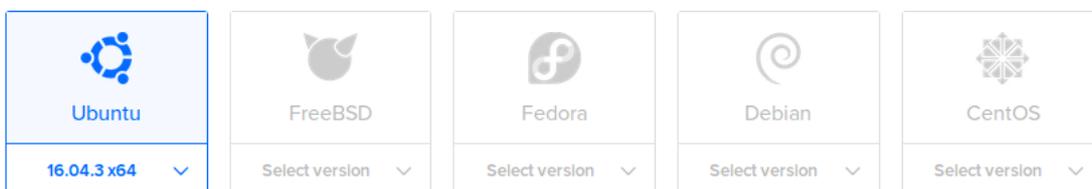
Clique no primeiro item, Droplets

Escolha o tipo de distribuição que usará em seu servidor

Create Droplets

Choose an image ?

[Distributions](#) [Container distributions](#) [One-click apps](#) [Snapshots](#)



Irei usar o Ubuntu 16.04, que é a primeira opção, que já está selecionada.

Escolher o perfil do Servidor

Choose a size

Standard Droplets

Balanced virtual machines with a healthy amount of memory tuned to host and scale applications like blogs, web applications, testing / staging environments, in-memory caching and databases.

| MEMORY | vCPUs | SSD DISK | TRANSFER | PRICE |
|--------|---------|----------|----------|-----------------------|
| 1 GB | 1 vCPU | 25 GB | 1 TB | \$5/mo \$0.007/hr |
| 2 GB | 1 vCPU | 50 GB | 2 TB | \$10/mo \$0.015/hr |
| 4 GB | 2 vCPUs | 80 GB | 4 TB | \$20/mo \$0.030/hr |

Cliquei no perfil com Memória de 1GB e 1 vCPU, que é o primeiro.

Escolher a Região do Datacenter

Choose a datacenter region

| | | | | | |
|--|---|---|---|--|---|
|  New York 1 2 3 |  San Francisco 1 2 |  Amsterdam 2 3 |  Singapore 1 |  London 1 |  Frankfurt 1 |
|  Toronto 1 |  Bangalore 1 | | | | |

Deixei o primeiro selecionado.

Existem outras opções que não são obrigatórias e não as selecionarei.

Finalizar e Criar

Finalize and create

How many Droplets?

Deploy multiple Droplets with the same configuration .

— 1 Droplet +

Choose a hostname

Give your Droplets an identifying name you will remember them by. Your Droplet name can only contain alphanumeric characters, dashes, and periods.

ribafs.org

Add Tags

Create

Gosto de usar meu domínio como hostname. Inclusive isso é importante pois a DO usa para criar nosso domínio reverso.

Veja que existe opção de criar mais de uma droplet de uma vez.

Então clicar no botão Create e aguardar.

Droplets

Search by Droplet name

Droplets Volumes

| Name | IP Address | Created ▲ | Tags |
|--|------------|-----------|------|
|  ribafs.org 1 GB / 25 GB Disk / NYC3 - Ubuntu 16.04.3 x64 | | | |

Senha via E-mail

Após criar sua droplet a DigitalOcean automaticamente te envia um e-mail com a senha provisória de acesso ao servidor como root, tipo este:

Your new Droplet is all set to go! You can access it using the following credentials:

Droplet Name: [ribafs.org](https://cloud.digitalocean.com/droplets/ribafs.org)

IP Address: 159.65.37.179

Username: root

Password: 1c54c1244ceb8bb00ee4ac68d1

For security reasons, you will be required to change this Droplet's root password when you login. You should choose a strong password that will be easy for you to remember, but hard for a computer to guess. You might try creating an alpha-numerical phrase from a memorable sentence (e.g. "I won my first spelling bee at age 7," might become "lwm#1sbaa7"). Random strings of common words, such as "Mousetrap Sandwich Hospital Anecdote," tend to work well, too.

As an added security measure, we also strongly recommend adding an SSH key to your account. You can do that here: <https://cloud.digitalocean.com/account/ssh-keys>.

Once added, you can select your SSH key and use it when creating future Droplets. This eliminates the need for root passwords altogether, and makes your Droplets much less vulnerable to attack.

Para isso deve acessar a Console existente no site da DigitalOcean, como explicado mais adiante.

Após criada clicando em seu nome aparecem os recursos disponíveis e operações que podem ser realizadas com o servidor/droplet.

Veja abaixo

The screenshot displays the DigitalOcean console interface for a specific Droplet. At the top, there is a navigation bar with links for Droplets, Spaces, Images, Networking, Monitoring, API, and Support. A green 'Create' button and a user profile icon are also visible. Below the navigation bar, a security notification prompts the user to 'Enable Two-factor Authentication'. The main section shows the Droplet details for 'ribafs.org', including its specifications: 1 GB Memory / 25 GB Disk / AMS3 - Ubuntu 16.04.3 x64. A toggle switch for 'ON' is present. Below the details, network information is shown: ipv4: 128.199.63.251, ipv6: Enable now, Private IP: Enable now, and Floating IP: Enable now. A 'Console' link is also available. The bottom section features monitoring graphs for CPU and Memory usage over a 6-hour period. The CPU graph shows a sharp spike to 100% usage around 08:30 AM, while the Memory graph shows a steady usage level around 33%.

Enhance the security of your account by enabling two-factor authentication. [Enable Two-factor Authentication](#)

ribafs.org 1 GB Memory / 25 GB Disk / AMS3 - Ubuntu 16.04.3 x64

ipv4: 128.199.63.251 ipv6: [Enable now](#) Private IP: [Enable now](#) Floating IP: [Enable now](#) [Console](#)

Graphs Last updated just now. [Create alert policy](#) 6 hours

CPU ?

| Time | CPU Usage (%) |
|----------|---------------|
| 04 AM | ~10 |
| 05 AM | ~10 |
| 06 AM | ~10 |
| 07 AM | ~10 |
| 08 AM | ~10 |
| 08:30 AM | 100 |
| 09 AM | ~10 |

Memory ?

| Time | Memory Usage (%) |
|-------|------------------|
| 04 AM | ~33 |
| 05 AM | ~33 |
| 06 AM | ~33 |
| 07 AM | ~33 |
| 08 AM | ~33 |
| 09 AM | ~33 |

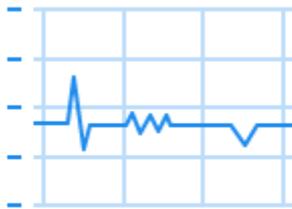
Monitoramento

Este é um serviço gratuito da DigitalOcean

Após criar uma droplet executar:

```
curl -sSL https://agent.digitalocean.com/install.sh | sh
```

Acesse a interface administrativa da DigitalOcean e clique acima em Monitoring



Looks like you don't have any alert policies

Alert policies watch your Droplets and alert you if there are any issues.

Create alert policy

This service requires an agent on each Droplet you wish to monitor. If you did not enable monitoring when creating your Droplet, run this command to manually install the agent:

```
curl -sSL https://agent.digitalocean.com/install.sh | sh
```

Após executar o comando no terminal então clique em Create alert policy

Então podemos configurar as condições para receber o alerta:

Create alert policy

Select metric & set threshold

CPU is above 70% 5 min

Select Droplets or Tags

ribafs.org x Please type a Droplet or Tag Name

Send alerts via

Email ribafs@gmail.com



Name and create alert policy

CPU is running high Create alert policy

Configure e clique em Create alert policy

Então recebemos (decidi mudar e monitorar a memória):

Monitoring

Alert Policies

[Setup instructions](#)

[Create alert policy](#)

| Name | Last Alert | Applied to |
|--|------------|---|
|  Memory is running high Memory Utilization is above 70% for 5 min | Never |  ribafs.org More |

Neste caso, caso a memória fique acima de 70% de uso por 5 minutos receberei o alerta.

Testando o disparo do alarme

Para gerar o uso da CPU necessário para disparar o alerta instale stress:

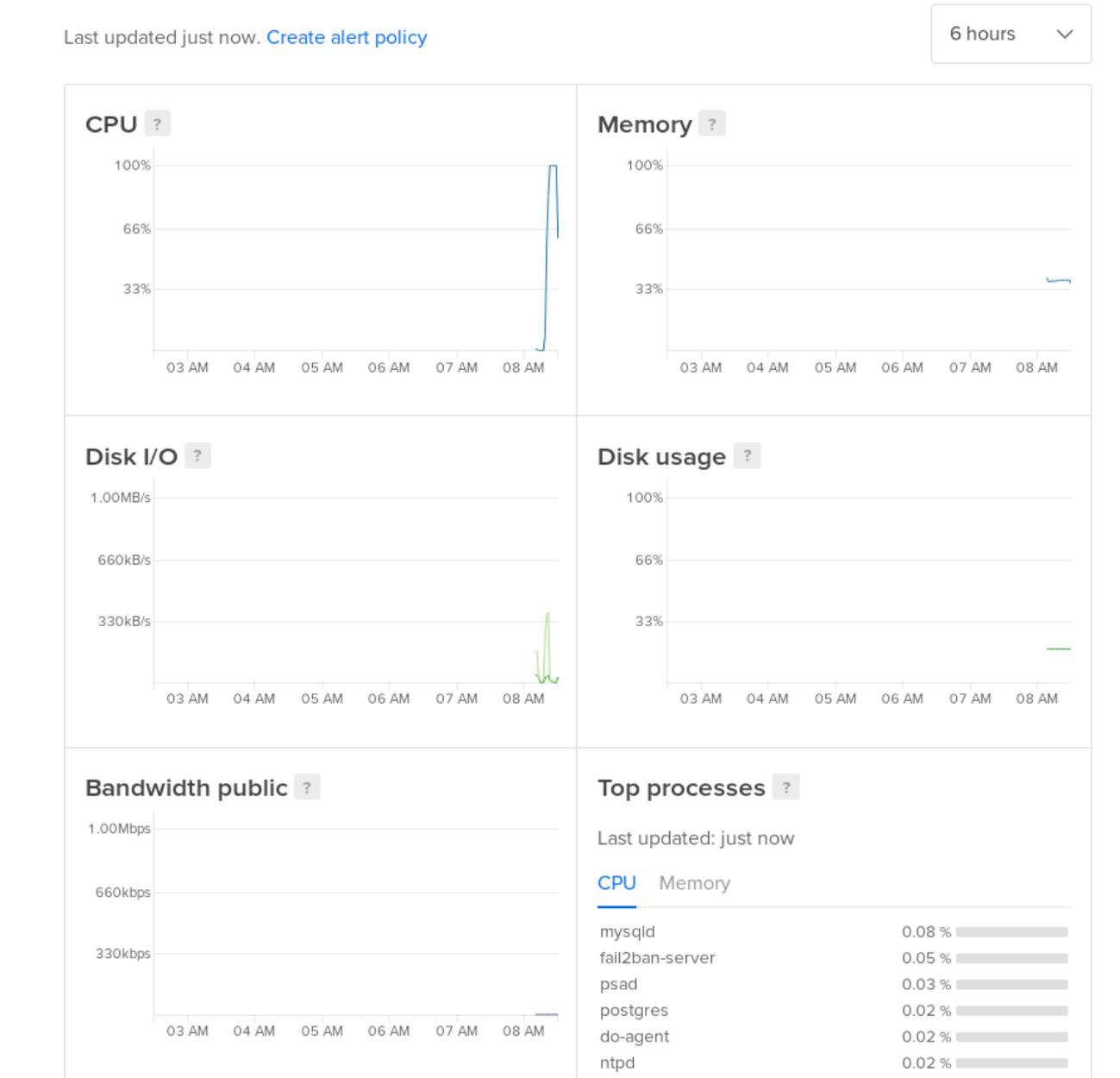
```
sudo apt-get update
sudo apt-get install stress
```

E execute:

```
stress -c `nproc` --all`
```

Gráficos

Também temos um monitoramento gráfico através da administração
 Clique no nome da droplet e Graphs



E podemos monitorar os principais recursos do nosso servidor.

Neste caso está mostrando para as últimas 6 horas, mas podemos selecionar, clicando na combo com 6 hours, as últimas 24 horas, 7 dias e 30 dias.

Console de Acesso Online

Um recurso importante que existe no site de administração da DigitalOcean é a console.

Através dele podemos acessar nosso servidor e efetuar algumas operações. Como também podemos trocar nossa senha de root ou receber a senha para uma nova droplet.

Ao criar uma nova droplet você automaticamente recebe um e-mail com a senha de root que deve ser usada na console.

Ou então a qualquer momento pode trocar a senha do root:

- Clique sobre o nome da droplet
- Access
- Reset Root Password

Assim ele enviará uma senha provisória para seu e-mail

Com esta senha em mãos acesse a console usando o usuário root e esta senha.

Alerta: tente digitar rápido pois a sessão espira e terá que repetir o processo.

Para melhorar eu copio a senha para o gedit, separo os dígitos em grupos de 4 ou de 6 e começo digitando grupo a grupo e teclando Alt+Tab.

Após entrar a senha correta será solicitado a mudar a senha,

Para isso digite novamente a senha recebida,

depois digita a nova senha

então repita a nova senha.

Assim

```
Ubuntu 16.04.3 LTS example tty1
example login: root
Password:
You are required to change your password immediately (root enforced)
Changing password for root.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password: _
```

Acesso via SSH

Veja o capítulo sobre Segurança – Reforçar a Segurança do SSH

Histórico de Acesso

<https://cloud.digitalocean.com/settings/security?i=651c46>

Adicionar Certificado SSL

Quem não implementar pelo sistema operacional pode implementar por aqui

<https://cloud.digitalocean.com/settings/security?i=651c46>

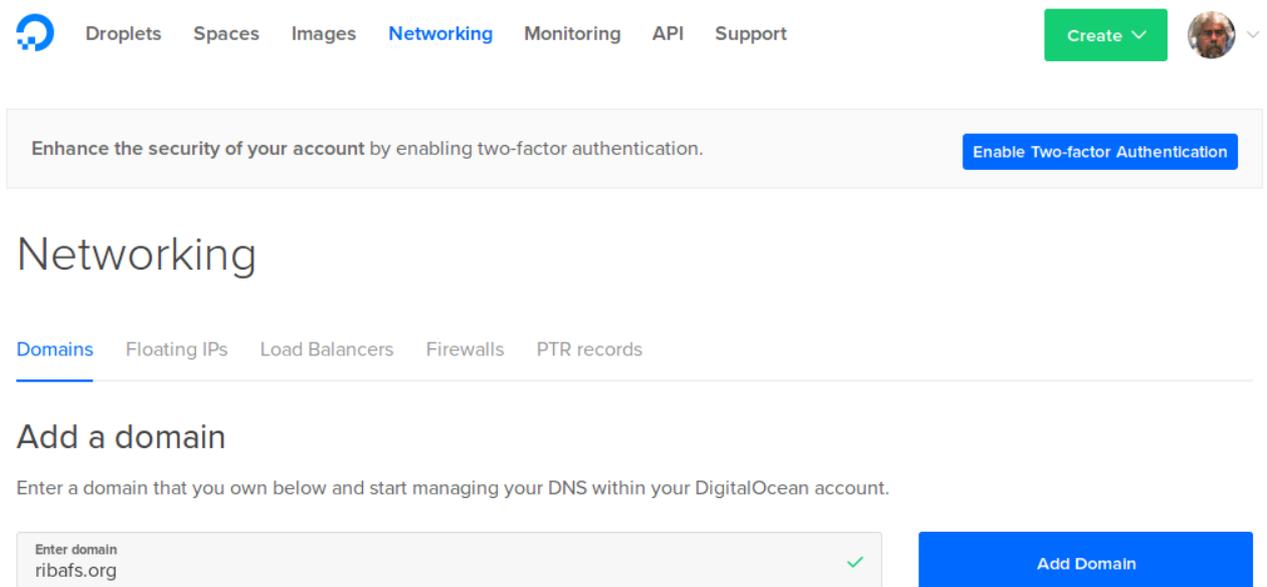
Configurando o DNS

A DigitalOcean oferece uma interface web para administrar o DNS, adicionando cada um dos registros.

Adicionar um Domínio

Faça login e acesse a página de administração.

Clique acima em Networking, adicione um domínio. Ao clicar no domínio adicionado poderá configurar o DNS.



The screenshot shows the DigitalOcean dashboard with the 'Networking' tab selected. A notification banner at the top suggests enabling two-factor authentication. Below the 'Networking' header, the 'Domains' sub-tab is active. The 'Add a domain' section contains a text input field with 'ribafs.org' and a green checkmark, and a blue 'Add Domain' button.

Digite o domínio e clique em Add Domain

Agora poderá configurá-lo como desejar.

Para um servidor web basicamente precisamos adicionar os registros:

A
CNAME

Adicionando Registros ao DNS

Adicionando Registro tipo A

A Digital Ocean nos oferece o formulário abaixo para a configuração dos registros:

ribafs.org

Create new record

[A](#) AAAA CNAME MX TXT NS SRV CAA

Use @ to create the record at the root of the domain or enter a hostname to create it elsewhere. A records are for IPv4 addresses only and tell a request where your domain should direct to.

| HOSTNAME | WILL DIRECT TO | TTL (SECONDS) | |
|-----------------------|------------------------------------|------------------|---------------|
| Enter @ or hostname * | Select resource or enter custom IP | Enter TTL 3600 ✓ | Create Record |

Se quero criar um registro do tipo A, que é para IPV4, então

- Clico acima em A
- Digito @ na caixa HOSTNAME
- Escolho o nome da droplet começando a digitar seu nome na caixa WILL DIRECT TO

Ficará assim:

| HOSTNAME | WILL DIRECT TO | TTL (SECONDS) | |
|----------------------------|-------------------------------------|------------------|---------------|
| Enter @ or hostname ✓ @ | ribafs.org AMS3 / 128.199.63.251 | Enter TTL 3600 ✓ | Create Record |

ribafs.org

Então clico em Create Record

Adicionando Registro tipo CNAME

- Clicar acima em CNAME
- Em HOSTNAME digitar www
- Em IS A ALIAS OF digite ribafs.org (seu domínio)

Ficará assim:

| HOSTNAME | IS AN ALIAS OF | TTL (SECONDS) | |
|-------------------------|-------------------------------------|-------------------|---------------|
| Enter hostname ✓ www | Enter @ or hostname ✓ ribafs.org | Enter TTL 43200 ✓ | Create Record |

www.ribafs.org

Agora clique em Create Record

Veja como configurei meu domínio

Enhance the security of your account by enabling two-factor authentication.

[Enable Two-factor Authentication](#)

← Domains

ribafs.org

Create new record

[A](#) [AAAA](#) [CNAME](#) [MX](#) [TXT](#) [NS](#) [SRV](#) [CAA](#)

Use @ to create the record at the root of the domain or enter a hostname to create it elsewhere. A records are for IPv4 addresses only and tell a request where your domain should direct to.

| HOSTNAME | WILL DIRECT TO | TTL (SECONDS) | |
|--|---|---|--|
| <input type="text" value="Enter @ or hostname"/> | <input type="text" value="Select resource or enter custom IP"/> | <input type="text" value="Enter TTL 3600"/> | <input type="button" value="Create Record"/> |

Tutorial da DigitalOcean

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-host-name-with-digitalocean>

Apenas adicionei um registro tipo A e dois CNAME:

DNS records

| Type | Hostname | Value | TTL (seconds) | |
|-------|-------------------|----------------------------------|---------------|------------------------|
| CNAME | cursos.ribafs.org | is an alias of ribafs.org. | 43200 | More ▾ |
| CNAME | www.ribafs.org | is an alias of ribafs.org. | 43200 | More ▾ |
| A | ribafs.org | directs to 128.199.63.251 | 3600 | More ▾ |
| NS | ribafs.org | directs to ns1.digitalocean.com. | 1800 | More ▾ |
| NS | ribafs.org | directs to ns2.digitalocean.com. | 1800 | More ▾ |
| NS | ribafs.org | directs to ns3.digitalocean.com. | 1800 | More ▾ |

Agora precisamos providenciar à configuração do nosso domínio para que aponte para a DigitalOcean.

Acesse a administração do seu domínio, remova os nameservers existentes e os NameServers da DigitalOcean:

ns1.digitalocean.com
 ns2.digitalocean.com
 ns3.digitalocean.com

Backup do Servidor

Existem duas formas de efetuar backup da droplet pela interface de administração da DigitalOcean: backup e snapshot. Ambas são pagas.

Backup – gera um backup automático da droplet e custa 20% do valor da droplet. Se a droplet for de US\$ 5,00/mês, então o backup custará US\$ 1,00 dólar mensal.

Snapshot – guarda um backup pontual estático de como a droplet se encontra no momento da criação do snapshot. Custa US\$ 0,05/GB/mês. Se guardamos um snapshot de 5GB por um mês, então custará US\$ 0,25, um quarto de dólar no mês, vinte e cinco centavos de dólar.

É importante guardar um backup/snapshot da droplet logo que ela esteja finalmente configurada e com tudo que precisa instalar. E cada vez que fizer alterações, remova o snapshot e crie novamente. Para maior segurança mantenha o(s) anteriores.

Detalhes:

<https://www.digitalocean.com/community/tutorials/digitalocean-backups-and-snapshots-explained>

Recuperando um Backup

Caso tenha algum problema em seu servidor e perca o controle poderá restaurar o backup guardado (backup ou snapshot). Uma forma é acessar o snapshot clicar em More e depois em Restore Droplet. Assim ele restaurará o snapshot para a droplet atual, apagando tudo que tem na droplet e restaurando o snapshot.

A droplet ficará da mesma forma em que estava quando criamos o snapshot. Isso mostra que precisamos guardar sempre uma cópia toda vez que fizermos alterações no servidor.

Tanto backup quanto snapshot podem ser replicados para várias regiões onde a DigitalOcean tem datacenter. Caso seu servidor seja importante é algo a ser considerado além de outros serviços da DigitalOcean como balanceamento de carga, ips flutuantes e outros. Veja aqui em Tools & Services: <https://www.digitalocean.com/pricing/>

Alguns outros recursos importantes e gratuitos como Monitoramento e Firewall.

Caso seu site vá aumentando a demanda por recursos basta ir melhorando seu servidor pois a DigitalOcean oferece flexibilidade e para isso.

Consultando seus Créditos

Clique acima e à direita em seu avatar

Settings

Billing - Your Credit

Para ver detalhes dos gastos clique em

View Usage Details

Inscrição para a newsletter da DigitalOcean

<https://cloud.digitalocean.com/settings/notifications?i=651c46>

Habilitar Autenticação de Dois Fatores

<https://cloud.digitalocean.com/settings/security?i=651c46>

Referências

<http://digitalocean.org>

<https://www.youtube.com/watch?v=kGABOBxFHy0>

<https://www.youtube.com/watch?v=Vfc9n8kzRVI>



DO Agent unresponsive

The DO Agent on this Droplet has been unresponsive for over 1 hour. Please try re-installing the DO agent by following the instructions below.

1. Log into your Droplet

```
$ ssh root@128.199.63.251
```

2. Run this command to install the DO Agent

```
$ curl -sSL https://agent.digitalocean.com/install.sh | sh
```

This update takes a few minutes, we'll let you know when it's complete.

[Learn more about installing the DO Agent.](#)

Update alert policy

Select metric & set threshold

| | | | | |
|--------------------|----------|----|---|-------|
| Memory Utilization | is above | 70 | % | 5 min |
|--------------------|----------|----|---|-------|

Select Droplets or Tags

 ribafs × Please type a Droplet or Tag Name

Send alerts via

Email ribafs@gmail.com

 Connect Slack

Name and create alert policy

| | |
|------------------------------|-------------------|
| Memory Lotada ✓ | Save alert policy |
|------------------------------|-------------------|

Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All

| Type | Protocol | Port Range | Sources |
|--------|----------|------------|-------------------------------|
| HTTP | TCP | 80 | All IPv4 All IPv6 |
| HTTPS | TCP | 443 | All IPv4 All IPv6 |
| Custom | TCP | 65522 | 177.130.208.59 177.14.224.188 |

New rule ▾

Outbound Rules

Set the Firewall rules for outbound traffic. Outbound traffic will only be allowed to the specified ports.

| Type | Protocol | Port Range | Destinations |
|---------|----------|------------|-------------------|
| All TCP | TCP | All ports | All IPv4 All IPv6 |
| All UDP | UDP | All ports | All IPv4 All IPv6 |

Digital Ocean - <http://digitalocean.com>

Ao contratar a DigitalOcean e receber o e-mail de boas vindas eles apontam alguns tutoriais úteis para a criação e configurações de um servidor (droplet) com eles.

É útil guardar estes links:

- <http://pages.news.digitalocean.com/ibDE0XI5y5600V020Rx3D0q>
- <http://pages.news.digitalocean.com/G5I0DD30Rcq6E0V60200yXx>
- <http://pages.news.digitalocean.com/MX0D2x0REDq5V00d60yI073>
- <http://pages.news.digitalocean.com/I0529ER06qyfXV3x0D0ID00>
- <http://pages.news.digitalocean.com/HE0030x0XygRDDq265I00aV>
- <http://pages.news.digitalocean.com/ihDE0XI5yb600V020Rx3D0q>
- <http://pages.news.digitalocean.com/dV06y5cXDx2DR00Iqi030E0>
- <http://pages.news.digitalocean.com/G5I0DD30RjqdE0V60200yXx>
- <http://pages.news.digitalocean.com/F5Rl600ek0E2y3Dx000DVXq>

Na comunidade do DO sobre ubuntu:

<https://www.digitalocean.com/community/tags/ubuntu>

Nome da droplet - ribafs.org

IP - 128.199.63.251

Mudar senha do meu user para que tenha caracteres especiais, letras maiúsculas, minúsculas e algarismos

O projeto é de instalar:

- apache2
- php7
- mysql 5.7
- postgresql 9.5
- slite 3
- Após tudo configurado criar um snapshot desta droplet para ser usado na criação de novas droplets ou no rebuild desta.

Não instalarei servidor de e-mail, para isso usarei o gmail

Apenasn indicarei o iRedMail e o Zimbra

Instalerei apenas servidores web e de bancos de dados

Configuração do DNS

A - ribafs.org

CNAME - www

CNAMW - cursos

NS defaults

Desinstalei o módulo Mod_maxmenu

- tive que desinstalar
- Remover seu diretório
- Remover no banco o módulo e em extensões

Com isso tive que reinstalar o site várias vezes. Sempre após desinstalar o maxmenu o site caia.

Então resolvi deixar ele lá e até atualizá-lo.

Inicialmente, após contratar a DigitalOcean e receber acesso ao painel administrativo Crie uma droplet escolhendo a distribuição e versão desejada

Depois disso abra a droplet criada e clique em Access e então em Reset Root Password

Ele te enviará um e-mail com uma senha provisória.

Acesse a console e use a senha recebida para acessar como root

Quando conseguir digitar a senha ele pedirá para criar uma nova senha, leia com cuidado. Entre com a senha provisória e depois crie uma nova.

Caso não consiga trocar a senha solicite ao suporte liberação para trocar a senha da droplet

- Ele libera e você acessa a console do DO e troca a senha seguindo as recomendações do suporte
- Depois de nova resposta do suporte, que finalmente libera teu acesso para a droplet via console com o usuário root
- Agora é hora de você liberar o acesso via ssh que ainda tá bloqueado para o usuário root

Portanto quando quiser destruir uma droplet para criar outra não vou simplesmente apagar e criar outra pois perco o IP e tudo que fiz.

Devo usar uma opção mais ágil:

Criar um snapshot quando a droplet estiver bem configurada

E quando quiser criar uma nova ou efetuar um rebuild usar o snapshot criado.

O uso de snapshot custa US\$ 0,05 por GB/mês

O uso de backup, que tem mais recurso e fica como uma cópia redundante da droplet, custa 20% do valor da droplet.

- Efetuar o login
- Clicar no nome da droplet
- Clicar em Destroy
- Abaixo em Rebuild clicar na caixa de texto onde tem Select an image e selecionar a distribuição e versão
 - Comece a digitar o nome do snapshot e o selecione para o rebuild
 - Clicar em Rebuild

O rebuild usando o snapshot apagará a droplet atual e voltará ao estado em que se encontrava ao criar o snapshot.

Droplet snapshots
Selecionar o snapshot
More - Restore droplet

Assim este rebuild terá o conteúdo do snapshot e estado igual a quando criaste o snapshot

Para criar uma nova não tem jeito, precisará esperar pelo suporte.

Instalei o servidor de e-mail com o iRedMail e estou pensando e recriar a droplet sem ele. Acontece que o rebuild preserva apenas o IP, apagando tudo, formata e instala a distribuição escolhida do zero.

3.1.1 – Snapshot

Na DigitalOcean custa US\$ 0,05/GB/mês

Na Vultr até o momento é grátis

Um snapshot salva uma cópia fiel do servidor no específico momento da criação.

Bom para compartilhar uma cópia do servidor com uma equipe.

== Bom para efetuar o rebuild de um servidor danificado:

- Abrir o servidor na administração web da DO
- Destroy
- Rebuild
- Select image (digitar o nome da droplet)

Com isso o servidor volta ao estado em que se encontrava no momento da criação do snapshot

Dica: remover o snapshot sempre que fizer alterações substanciais no servidor e criar um novo.

Se for importante não remova mas crie um novo

== Criação de um snapshot

Alguns gerenciadores de bancos de dados devem ser parados para que seja criado o snapshot. Melhor parar o servidor.

Desligar o servidor antes de criar o snapshot

Para criar um novo servidor partindo de um snapshot:

Create
Droplet
Snapshot
Selecionar o snapshot, tamanho/porte, região, etc.

Restaurando um snapshot

Images
 Snapshot
 Selecionar o snapshot
 More
 Restore Droplet

Excluindo um snapshot

Selecionar a droplet
 Snapshot
 More
 Delete

Referências

<https://www.youtube.com/watch?v=fM3G7yLNAjQ> - Redes linux

<https://www.youtube.com/watch?v=20GPIp4xCjg> - Redes com Debian

3.1.2 – DNS na Digital Ocean

DNS records

| Type | Hostname | Value | TTL (seconds) | |
|-------|-------------------|----------------------------------|-----------------------|--|
| TXT | ribafs.org | returns "v=spf1 a mx -all" | 3600 | More  |
| MX | mx.ribafs.org | mail handled by mx.ribafs.org | 10 14400 | More  |
| A | mail.ribafs.org | directs to 128.199.63.251 | 3600 | More  |
| CNAME | cursos.ribafs.org | is an alias of ribafs.org. | 43200 | More  |
| CNAME | www.ribafs.org | is an alias of ribafs.org. | 43200 | More  |
| A | ribafs.org | directs to 128.199.63.251 | 3600 | More  |
| NS | ribafs.org | directs to ns1.digitalocean.com. | 1800 | More  |
| NS | ribafs.org | directs to ns2.digitalocean.com. | 1800 | More  |
| NS | ribafs.org | directs to ns3.digitalocean.com. | 1800 | More  |

DNS records

| Type | Hostname | Value | TTL (seconds) | |
|-------|-----------------|--|---------------|--|
| TXT | mail.ribafs.org | returns v=spf1 ip4:159.65.163.142 -all | 3600 | More  |
| TXT | mail.ribafs.org | returns google-site-verification=JBXL56VIGw... | 3600 | More  |
| MX | ribafs.org | mail handled by mail.ribafs.org | 14400 | More  |
| A | mail.ribafs.org | directs to 159.65.163.142 | 3600 | More  |
| CNAME | php.ribafs.org | is an alias of ribafs.org. | 43200 | More  |
| CNAME | www.ribafs.org | is an alias of ribafs.org. | 43200 | More  |
| A | ribafs.org | directs to 128.199.63.251 | 3600 | More  |
| NS | ribafs.org | directs to ns1.digitalocean.com. | 1800 | More  |
| NS | ribafs.org | directs to ns2.digitalocean.com. | 1800 | More  |
| NS | ribafs.org | directs to ns3.digitalocean.com. | 1800 | More  |

3.2 – Servidores VPS na Vultr

Criação de um servidor na Vultr

Para a contratação da Vultr (<https://vultr.com/>) precisamos de um cartão de crédito tipo débito internacional, uma conta no Paypal, Bitcoin, Alipay e até Gift Code/Coupom.

Crie uma conta na Vultr, cadastre seu cartão com algum crédito e já pode começar a criar seu servidor.

Documentação

Uma boa ideia é ler alguns dos tutoriais da Vultr

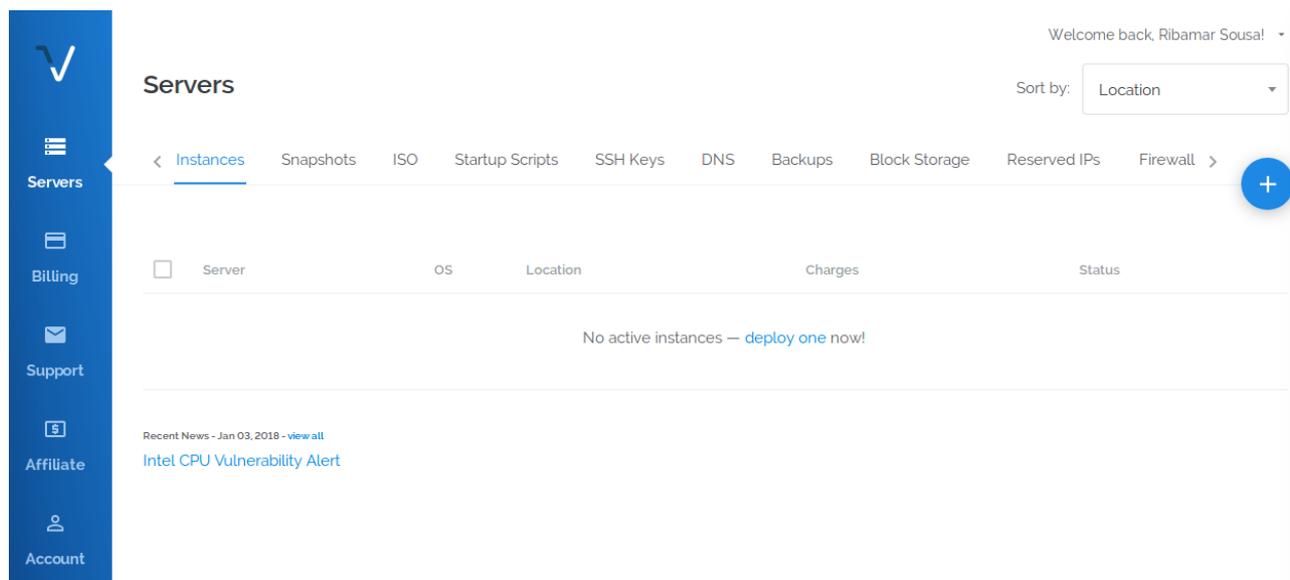
<https://www.vultr.com/docs/>

Suporte

Se aparecerem dúvidas ative o suporte

<https://my.vultr.com/support/>

Após efetuar o login aparece a área de administração de servidores



The screenshot displays the Vultr dashboard interface. On the left is a blue sidebar with navigation icons for Servers, Billing, Support, Affiliate, and Account. The main content area is titled 'Servers' and includes a 'Welcome back, Ribamar Sousa!' message. Below the title is a 'Sort by:' dropdown menu set to 'Location'. A horizontal navigation bar contains links for Instances, Snapshots, ISO, Startup Scripts, SSH Keys, DNS, Backups, Block Storage, Reserved IPs, and Firewall. A blue circular button with a white plus sign is located on the right side of this bar. Below the navigation bar is a table with columns for Server, OS, Location, Charges, and Status. The table is currently empty, displaying the message 'No active instances — [deploy one now!](#)'. At the bottom of the page, there is a 'Recent News' section with a link to 'Intel CPU Vulnerability Alert'.

Criar um Servidor

Para criar um novo servidor clique no botão azul com um símbolo de + e circular à direita

Localização do Data Center

Após clicar no sinal de +, aparece a tela para seleção da região do datacenter

Deploy New Instance

Vultr Cloud Compute (VC2)
Bare Metal Instance
Storage Instance
Dedicated Instance

60% OFF PROMO

Server Location

All Locations
America
Europe
Australia
Asia

| | | | |
|---|--|---|---|
|  <p>Tokyo Japan</p> |  <p>Singapore Singapore</p> |  <p>Amsterdam Netherlands</p> |  <p>Paris France</p> |
|  <p>Frankfurt Germany</p> |  <p>London United Kingdom</p> |  <p>New York (NJ) United States</p> |  <p>Chicago United States</p> |
|  <p>Dallas United States</p> |  <p>Atlanta United States</p> |  <p>Los Angeles United States</p> |  <p>Miami United States</p> |
|  <p>Seattle United States</p> |  <p>Silicon Valley United States</p> |  <p>Sydney Australia</p> | |

No caso escolhi Miami por indicação de um colega do grupo de Joomla, por ser um dos mais rápidos.

Tipo de Servidor

Ao rolar mais a tela precisamos selecionar o tipo de servidor, que sistema operacional, em sendo linux qual a distribuição Linux e versão. No caso eu selecionei CentOS 7 x64

2 Server Type

64 bit OS 32 bit OS Application Upload ISO ISO Library Backup Snapshot

| | | | |
|--|---|---|--|
|  CentOS 7 x64 |  CoreOS Stable x64 |  Debian Select Version |  Fedora Select Version |
|  FreeBSD Select Version |  OpenBSD 6 x64 |  Ubuntu Select Version |  Windows Select Version |

Tamanho do Servidor

Agora é a hora de selecionar o porte do servidor. Eu escolhi com 1024 M de RAM e 1 CPU, que custa US\$ 5/mês

3 Server Size

| | | | |
|---|--|---|--|
| 20 GB SSD \$2.50/mo \$0.004/h | 25 GB SSD \$5/mo \$0.007/h | 40 GB SSD \$10/mo \$0.015/h | 60 GB SSD \$20/mo \$0.03/h |
| 1 CPU 512MB Memory 500GB Bandwidth | 1 CPU 1024MB Memory 1000GB Bandwidth | 1 CPU 2048MB Memory 2000GB Bandwidth | 2 CPU 4096MB Memory 3000GB Bandwidth |

Então aparecem algumas opções opcionais que não selecionei:

- Additional Features
- Startup Script
- SSH Keys

Hostname do Servidor

Então finalmente vamos escolher um hostname para o servidor. No caso usei o meu domínio para isso:

7 Server Hostname & Label

Enter server hostname
ribafs.org

Enter server label
ribafs.org

Servers Qty: Summary: **\$5.00/mo** (\$0.007/hr)

[Deploy Now](#)

Para finalizar clico no botão Deploy Now.

E aguardo a criação do servidor.

Observe a mensagem de que o servidor foi adicionado e que está sendo criado:

Servers Sort by: Location

[Instances](#) [Snapshots](#) [ISO](#) [Startup Scripts](#) [SSH Keys](#) [DNS](#) [Backups](#) [Block Storage](#) [Reserved IPs](#) [Firewall](#)

Server added successfully!

| <input type="checkbox"/> | Server | OS | Location | Charges | Status |
|--------------------------|-------------------------------------|---|---|---------|--|
| <input type="checkbox"/> | ribafs.org 1024 MB Server |  |  Miami | --- |  Installing |

Agora vemos que foi criado e que está pronto para ser administrado

Server added successfully!

| <input type="checkbox"/> | Server | OS | Location | Charges | Status |
|--------------------------|---|---|---|---------|--|
| <input type="checkbox"/> | ribafs.org 1024 MB Server - 45.63.104.148 |  |  Miami | --- |  Running Manage |

Ao clicar no link Manage recebemos a informação que ainda não está pronto. Veja em amarelo abaixo

Please note: Your server may still be finishing installing and booting up during the first few minutes of activation.
If the server does not ping, you can [view the console](#) to monitor progress.

| | | |
|---|----------------------------|--|
| Bandwidth Usage 0GB/1000GB | CPU Usage -- | Current Charges \$0.01 |
| Location:  Miami | CPU: 1 vCore | Label: ribafs.org |
| IP Address: 45.63.104.148  | RAM: 1024 MB | Tag: [Click here to set] |
| Username: root | Storage: 25 GB SSD | OS: CentOS 7 x64 |
| Password:   | Bandwidth: 0 GB of 1000 GB | |

Veja também que nada aparece em CPU usage e também que o fato de criar um servidor já gasta 1 centavo de dólar do nosso crédito.

Aguardar até que apareça 0% em CPU usage.

Podemos efetuar um ping do nosso desktop para o IP do servidor criado para saber se ele já está ativo.

```
ping 45.63.104.148
```

Se aparecer algo como

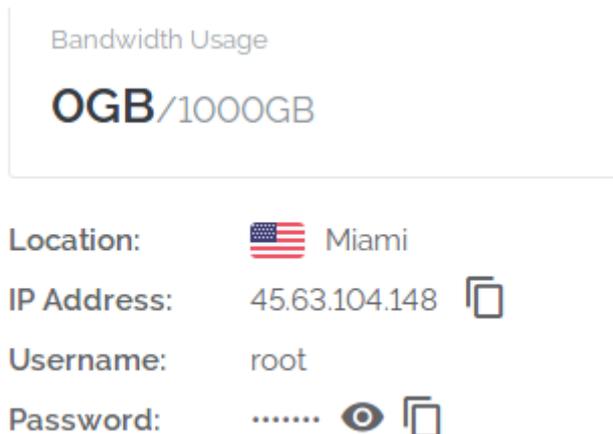
```
ribafs@ribamint ~ $ ping 45.63.104.148
PING 45.63.104.148 (45.63.104.148) 56(84) bytes of data.
64 bytes from 45.63.104.148: icmp_seq=1 ttl=49 time=155 ms
64 bytes from 45.63.104.148: icmp_seq=2 ttl=49 time=154 ms
64 bytes from 45.63.104.148: icmp_seq=3 ttl=49 time=154 ms
64 bytes from 45.63.104.148: icmp_seq=4 ttl=49 time=154 ms
64 bytes from 45.63.104.148: icmp_seq=5 ttl=49 time=154 ms
```

Então já podemos acessar via ssh assim:

```
ssh root@45.63.104.148
```

Como saber a senha deste servidor?

Na página de administração do servidor na Vultr, quando abrimos o servidor, aparece o seguinte:



Veja que em Password não aparece nada, exceto alguns pontinhos.

Mas existe um olho que quando passamos o ponteiro do mouse sobre ele ele mostra a frase "Show password" e duas folhinhas à direita que quando passamos o mouse sobre elas aparece "Copy Password" (esta opção não funcionou comigo), precisei clicar no olho para que mostre a senha. Então selecionei a senha, tecliei Ctrl+C para copiar e no terminal apenas Shift+Insert quando a senha foi solicitada.

```
ssh root@45.63.104.148
```

E teclar enter

Digitar yes e Enter e digitar a senha abaixo

Caso tenha dificuldade copie e cole a senha em um processador de textos e amplie para garantir que digitará corretamente.

Trocar a senha do Root

Vamos logo trocar a senha por uma que lembraremos, mas é importante que usemos uma senha forte.

```
passwd root
```

Entre com a nova senha e repita.

Agora vamos cuidar de configurar o servidor, otimizá-lo para nosso uso e implementar a segurança.

Vejam na administração o item Settings – networking configuration:

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=45.63.104.148
NETMASK=255.255.254.0
GATEWAY=45.63.104.1
DNS1=108.61.10.10
```

/etc/sysconfig/network-scripts/route-eth0

```
169.254.0.0/16 dev eth0
```

Dados da rede

| Address | Netmask | Gateway | Reverse DNS |
|---------------|---------------|-------------|---|
| 45.63.104.148 | 255.255.254.0 | 45.63.104.1 | 45.63.104.148.vultr.com |

Informações adicionais sobre o IPV4

IPv4 Addresses cost \$2/month or \$0.003/hour.

- Addresses must remain active for 60 minutes before they can be removed.
- You will need to manually configure additional IPs on your VPS.
- You are limited to a maximum of 2 additional IPv4 IPs per VPS.

3.2.1 - Restauração de Snapshot na Vultr

Um snapshot é um backup pontual de um servidor. Que em sendo restaurado deixará o servidor no estado do momento em que o snapshot foi criado.

Atualmente, na fase beta, snapshot é gratuito.

Criação de um Snapshot de um servidor

Acessar o servidor no site de administração da Vultr

Clicar em Snapshots acima

Digitar um label e clicar em Take Snapshot

Restauração de um Snapshot

Para restaurar devemos criar um novo servidor tendo como base o snapshot criado.

- Clicar no sinal de + para criar um novo servidor

- Escolha a localização do servidor (Server Location)
- No momento de escolher a distribuição (Server Tyle) selecione Snapshot
 - Caso não apareça clique em Add New e siga as instruções
 - Então volte e comece novamente a criar o servidor. Repetindo o primeiro passo, depois escolhendo Snapshot e selecione o snapshot desejado clicando nele
 - Então selecione o tamanho do servidor
 - Ao final digite o Server Hostname e clique em Deploy Now

Obs.: snapshots podem ser restaurados somente para discos do mesmo tamanho o maior.

Veja que também existe a opção de baixar um snapshot por upload

3.2.2 – DNS na Vultr

DNS

[← Instances](#) [Snapshots](#) [ISO](#) [Startup Scripts](#) [SSH Keys](#) [DNS](#) [Backups](#)

[Add Domain](#)

| Domain | Date Created |
|------------|---------------------|
| ribafs.org | 2018-02-20 14:25:34 |

Vultr DNS Introduction

You can learn more about Vultr DNS and its features on the [Introduction to Vultr DNS](#) guide.

Vultr Name Servers

- ns1.vultr.com
- ns2.vultr.com

| | | | | | |
|--------------------------|-------|------|---------------|------|----|
| <input type="checkbox"/> | A | mail | 45.63.104.148 | 3600 | |
| <input type="checkbox"/> | A | | 45.63.104.148 | 300 | |
| <input type="checkbox"/> | CNAME | * | ribafs.org | 300 | |
| <input type="checkbox"/> | CNAME | php | ribafs.org | 3600 | |
| <input type="checkbox"/> | CNAME | www | ribafs.org | 3600 | |
| <input type="checkbox"/> | MX | | ribafs.org | 300 | 10 |
| <input type="checkbox"/> | NS | | ns1.vultr.com | 300 | |
| <input type="checkbox"/> | NS | | ns2.vultr.com | 300 | |

4 – Melhorando a Segurança de um VPS com CentOS 7

Requisitos:

Instalar o CentOS 7

Atualizar,

Fazer upgrade

reboot

Instalar o LAMP

adduser ribafs

passwd ribafs

usermod -a -G wheel ribafs

mkdir /home/ribafs/backup

Implementemos a segurança, para estar usando o servidor de forma mais segura.

4.0. Cuidados Iniciais

Selecionar uma distribuição desejada e adequada para a finalidade.

Faça a instalação

Efetue login e atualize a distribuição em seguida. Ao final efetue um reboot.

Evite instalar pacotes para desenvolvimento como gcc, make, etc.

Evite instalar repositórios instáveis.

Para forçar a memória, logo após a configuração final do servidor, já crie um backup ou snapshot do mesmo e fique atento para criar outro backup logo que o servidor esteja concluído e bem configurado.

Agora (logo após a instalação do nginx, mysql e php) é uma boa hora para efetuar uma cópia dos scripts de configuração originais que estão funcionando. Para em caso de problema restaurar este script que funciona para que volte a funcionar. Guarde uma cópia no diretório /home/seuuser/backup do usuário que irá administrar o servidor:

- nginx.conf e default.conf

- php.ini e php-fpm.ini

...

Backup local do Servidor

Uma boa ideia é ter uma box no Vagrant do CentOS 7 x64 em seu desktop, sendo cópia fiel e original do servidor localmente, com todos os pacotes do servidor para ter uma cópia fiel do servidor em seu desktop. Em caso de problema no servidor poderá resolver com uma cópia do script do desktop.

Primeira Atualização

```
yum update  
reboot
```

Gerenciador de Arquivos Modo Texto

Uma boa pedida é instalar o gerenciador de arquivos modo texto mc:

```
yum install mc
```

No centos instale o unzip:

```
yum install unzip  
yum install net-tools
```

Backup Regular

Efetuar backup com frequência de tudo que tem no servidor, especialmente após alterações:

- sites
- aplicativos
- arquivos

Ajustar Fuso Horário

Mudar fuso horário para America/Fortaleza (no meu caso)

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

Verificar timezona

```
timedatectl
```

ou

```
timedatectl list-timezones
```

Monitorar arquivos modificados

```
find /var/www/html -type f -ctime -1 -exec ls -ls {} \;
```

Podemos colocar no cron para que seja executado a cada madrugada e nos envie um e-mail.

Procurar arquivos com 666

```
find /var/www/html -xdev -perm +o=w ! \( -type d -perm +o=t \) ! -type l -print
```

Procurar diretórios com 777

```
find /var/www/html -type d -perm -o+w -exec ls -ld {} \;
```

Procurar contas sem senha

```
awk -F: '($2 == "") {print}' /etc/shadow
```

Limpar cache de RAM

Criar um script para rodar com mais praticidade

Executar antes `free -m` e após executar o script para comparar os valores.

```
sudo nano /usr/local/bin/m
```

```
sudo sysctl -w vm.drop_caches=3
```

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

Rodar:

```
sudo m
```

Adicionar partição de Swap

Adicionar partição de swap com 2GB

```
dd if=/dev/zero of=/swapfile bs=1M count=2048
```

```
mkswap /swapfile
```

```
swapon /swapfile
```

Adicionar ao fstab

```
nano /etc/fstab
```

```
/swapfile swap swap defaults 0 0
```

Testar

```
free -m
```

4.1. Habilitação e Configurar firewall com ufw

iptables -L

Ver arquivo texto com...

4.2. Secure shared memory no fstab

Edite o fstab e adicione a linha ao final. Somente após o reboot terá efeito:

```
nano /etc/fstab
tmpfs      /run/shm      tmpfs      defaults,noexec,nosuid    0      0
```

4.3. Reforçar a segurança do SSH

Vamos otimizar a configuração do SSH:

Adicionar usuário administrador

Adicionar um usuário que gerenciará o computador com sudo e que será o único a acessar via ssh:

```
sudo su
adduser nomeuser      # Troque nomeuser pelo login desejado
adduser nomeuser admin # No Debian o grupo admin precisa ser criado
```

```
usermod -aG wheel nomeuser
```

```
nano /etc/sudoers
```

Adicione a linha a seguir abaixo da linha do root

```
nomeuser ALL=(ALL) NOPASSWD:ALL
```

```
su - nomeuser
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_nomeuser -t dsa (Enter 2 vezes)
cat ../.ssh/id_nomeuser*.pub > ../.ssh/authorized_keys
```

```
exit
```

Escolha uma porta alta, como a 10522 ou mais alta

Agora já podemos sanear o SSH:

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

```
#Faça as alterações abaixo:
Port 65522
```

```
LoginGraceTime 30 # reduzir tempo do timeout  
PasswordAuthentication yes  
AllowUsers nomeuser root
```

```
service sshd restart  
exit
```

Veja que manteve o acesso ao root. Mas após o primeiro acesso com o nomeuser e sentir segurança então remove o root da linha AllowUsers, além disso mudar no sshd_config a linha:

```
PermitRootLogin no
```

E reiniciar o ssh

Experimente agora conectar com o root.

Gere as chaves do SSH em seu micro desktop com:

```
ssh-keygen -t rsa -b 4096
```

Apenas tecle Enter duas vezes

Então copie sua chave para o servidor, para que possa conectar sem digitar a senha. Na primeira vez te pedirá a senha mas sua senha do desktop, mas memorizará e não mais pedirá. Assim ficará mais seguro.

```
ssh-copy-id ribafs@ip_servidor -p 10522
```

Mesmo com scp não pedirá senha.

Sugestão - Criar um script para conectar:

```
sudo nano /usr/local/bin/docean
```

```
ssh -p 65522 ribafs@128.199.63.251
```

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

Conecte com
docean

Monitorar login do root

```
sudo yum install mailx
```

Adicione ao início do script .bashrc do root:

```
nano /root/.bashrc
```

```
echo -e "Acesso ao shell do Root em `tty` \n `w`" | mail -s "Alerta: Acesso do root"  
ribafs@gmail.com
```

OBS.: para envio de e-mail precisa de solicitar do suporte a liberação. Problema de spam.

Notificação de acesso via ssh pelo ribafs

```
cd /home/ribafs
nano .bashrc
echo 'ALERT - Root Shell Access (ServerName) on:' `date` `who` | mail -s "Alert: Root
Access from `who | cut -d'(' -f2 | cut -d')' -f1`" ribafs@gmail.com
```

4.4. Reforçar a segurança da rede configurando o sysctl

Para prevenir fontes de roteamento de pacotes de entrada e logs de IPs malformados

```
sudo nano /etc/sysctl.conf
```

Descomente

```
# IP Spoofing protection
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Disable source packet routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0

# Block SYN attacks
net.ipv4.tcp_syncookies = 1

# Log Martians
net.ipv4.conf.all.log_martians = 1
```

Adicione ao final:

```
# Ignore send redirects
net.ipv4.conf.all.send_redirects = 0

# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Disable source packet routing
net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0

# Ignore send redirects
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5
```

```
# Log Martians
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1
```

Reiniciar

```
sudo systemctl -p
```

4.5. Prevenir IP Spoofing

Edite o

```
nano /etc/host.conf
```

E deixe seu conteúdo assim:

```
order bind,hosts
multi on
nospoof on
```

4.6. Reforçar a segurança do PHP

Uma boa forma de melhorar a segurança do php é instalando o phpsecinfo:

<https://github.com/funkatron/phpsecinfo>

<http://phpsec.org/projects/phpsecinfo/>

E corrigir os erros apontados com as respectivas recomendações.

Algumas sugestões para reforçar a segurança do PHP:

edite o php.ini e faça as alterações:

```
nano /etc/php.ini
```

ALERTA – ao efetuar as alterações abaixo faça uma a uma, sempre reiniciando o apache e abrindo o site e efetuando um refresh para testar. Caso tenha problema desfaça ou ajuste o parâmetro com problema.

```
disable_functions = exec,system,shell_exec,passthru,
html_errors = Off
mail.add_x_header = Off
session.name = NEWSSESSID
```

Na linha com `disable_functions` já existem várias funções por padrão que são desabilitadas. Não as remova, apenas adicione as recomendações acima ao início, separadas por vírgula.

Com a ajuda do `PHPsecinfo` também ajustei estes abaixo:

```
allow_url_fopen = Off
upload_tmp_dir = /usr/share/nginx/html/phpup
```

Criei o diretório `/usr/share/nginx/html/phpup`

Estes dois últimos parâmetros devem ser adotados com cuidado, de acordo com a sua necessidade. Abaixo são os valores default na versão 7 do php:

```
post_max_size = 8M
upload_max_filesize = 2M
```

```
service nginx restart
```

Depois dos ajustes acima alguma coisa pode não funcionar. Então efetue os ajustes devidos, sem exagerar.

Proteger arquivos de configuração do apache, php e mysql contra escrita:

```
/etc/php/php.ini
/etc/nginx/conf.d/default.conf e demais
/etc/mysql/my.cnf
```

4.8. Instalar e Configurar ModSecurity e ModEvasive

4.9. Scannear logs e banir hosts suspeitos

Usando DenyHosts e Fail2Ban

Denyhosts – bloqueia ataques de SSH adicionando entradas ao `/etc/hosts.dny`. Também avisa ao administrador sobre hosts suspeitos, ataques de usuários e logins suspeitos.

```
sudo apt install denyhosts
```

Após instalar edite o

```
sudo nano /etc/denyhosts.conf
```

E atualize seu e-mail e outras configurações que desejar.

```
ADMIN_EMAIL = ribafs@gmail.com
SMTP_HOST = localhost
SMTP_PORT = 25
#SMTP_USERNAME=foo
#SMTP_PASSWORD=bar
SMTP_FROM = DenyHosts nobody@localhost
#SYSLOG_REPORT=YES
```

```
service denyhosts restart
```

Fail2Ban

O fail2ban é mais eficiente que o denyhosts, pois ele estende a monitoração de logs para outros serviços além do ssh, como o apache, courier, ftp e mais.

O fail2ban escaneia arquivos de log e bane IPs que parecem suspeitos (muitas tentativas erradas de senha, procurando por exploits, etc)

Geralmente bloqueia através do firewall por um certo tempo que é configurável

Instalação

```
sudo apt install fail2ban
```

Após instalar edite

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

E crie o filtro de regras requerido

Ative todos os serviços que deseja que o fail2ban monitore

Para que monitore o ssh, altere enable para true:

OBS: atente para mudar de ssh para o número que escolheu, caso não use a 22.

[sshd]

```
enabled = true
port    = ssh
filter  = sshd
logpath = /var/log/auth.log
maxretry = 3
```

Caso o seu ssh esteja usando outra porta, mude port = sua porta

Checar status:

```
fail2ban-client status
```

Restartar

```
/etc/init.d/fail2ban restart
```

Desbloquear um certo IP bloqueado por engano

```
iptables -L -n
```

Checar porta 443

```
iptables -L -n | grep 443
```

Caso o comando acima mostre o IP 201.14.45.23 rodamos o seguinte comando para liberar:

```
iptables -D fail2ban-SSH -s 201.14.45.23 -j DROP
```

Comando mais específico:

```
fail2ban-client set ssh-iptables unbanip IpaRemove
```

Whitelisting

Whitelisting é configurada no jail.conf usando uma lista separada por espaço

```
[DEFAULT]
```

```
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not  
# ban a host which matches an address in this list. Several addresses can be  
# defined using space separator.
```

```
Ignoreip = 127.0.0.1 192.168.1.0/24 8.8.8.8
```

4.10. Detectar Intrusões – PSAD

PSAD é uma coleção de 3 pequenos daemons do sistema, que rodam para analisar mensagens de log do iptables para detectar scanneamento de portas e outros tráficos suspeitos.

Instalação

```
sudo apt install psad
```

Configuração básica

```
sudo nano /etc/psad/psad.conf
```

- **EMAIL_ADDRESSES** – mude para seu e-mail
- **ENABLE_AUTO_IDS** - se Y o psad agirá automaticamente
- **ENABLE_AUTO_IDS_EMAILS** - se Y psad mandará um e-mail em cada suspeita

```
sudo service psad restart
```

4.11. Checar por RootKits – RKHunter e CHKRootKit

Rootkits e RKHunter basicamente fazem a mesma coisa, procuram rootkits no sistema. Nenhuma ofensiva aqui, apenas mostram o que veem.

Instalação

```
sudo apt install rkhunter chkrootkit
```

Executando chkrootkit

```
sudo chkrootkit
```

Atualizando e rodando rkhunter

```
sudo rkhunter --update  
sudo rkhunter --propupd  
sudo rkhunter --check
```

4.12 Varrendo portas abertas com Nmap

O nmap é um software para descobrir a rede e para auditar segurança.

Instalação

```
sudo apt install nmap
```

Varrer seu sistema por portas abertas

```
nmap -v -sT localhost
```

Saída

```
Not shown: 995 closed ports  
PORT      STATE SERVICE  
25/tcp    open  smtp  
80/tcp    open  http  
443/tcp   open  https  
3306/tcp  open  mysql  
5432/tcp  open  postgresql
```

Lembrando que varre apenas até a porta 1000, portando não mostrou a do ssh
Outro detalhe é que para acesso externo somente as portas 80 e 443, as demais oferecem acesso somente interno.

O acesso externo se dá ao mysql somente através do Apache. O visitante do site acessa o site pela porta 80 ou 443 e chega até aqui ao servidor, aqui o apache vai ao mysql e solicita o que deseja. O mysql somente é acessado via localhost.

```
sudo nmap -v -sS localhost.
```

4.13. Instalar e configurar o Apparmor

É um software que melhora o kernel para isolamento de aplicativos. Este confinamento é provido por perfis de aplicativos do kernel.

Mais detalhes:

<https://wiki.ubuntu.com/AppArmor>

<https://help.ubuntu.com/lts/serverguide/apparmor.html>

<https://help.ubuntu.com/community/AppArmor>

Instalação

```
sudo apt-get install apparmor apparmor-profiles
```

Checar funcionamento

```
sudo apparmor_status  
ou  
sudo aa-status
```

4.14. Auditar segurança do sistema com Tiger e Tripwire

Tiger é uma ferramenta de segurança que pode ser usada para auditoria e detecção de intrusão do sistema.

Tripwire é um sistema de detecção de intrusão (HIDS) que checa a integridade de arquivos e pastas.

Detalhes

<https://www.digitalocean.com/community/tutorials/how-to-use-tripwire-to-detect-server-intrusions-on-an-ubuntu-vps>

Instalação

```
sudo apt install tiger tripwire
```

Responda sim para fornecer senha para arquivos e guarde bem as senhas

Criar banco de dados

```
sudo tripwire --init  
Entre com a senha fornecida acima.
```

Criar arquivo de polícia

```
sudo twadmin --create-polfile /etc/tripwire/twpol.txt  
Entre com a senha fornecida acima.
```

Executando tiger

```
sudo tiger
```

Toda a saída do tiger pode ser vista em:
`/var/log/tiger`

Para visualizar o relatório de segurança do tiger:
`sudo less /var/log/tiger/security.report*`

Aqui ele gerou este:
/var/log/tiger/security.report.ribafs.org.180214-20:50

4.15. Atualizar a distribuição

Atualizar automaticamente somente as atualizações de segurança:

```
aptitude install unattended-upgrades
```

```
nano /etc/apt/apt.conf.d/10periodic
```

Excluir tudo e adicionar:

```
APT::Periodic::Update-Package-Lists "1";  
APT::Periodic::Download-Upgradeable-Packages "1";  
APT::Periodic::AutocleanInterval "7";  
APT::Periodic::Unattended-Upgrade "1";
```

Isso somente atualiza pacotes de segurança

Atualização completa, de todos os pacotes:

```
apt-get update  
apt-get upgrade
```

Atualiza o servidor manualmente pelo menos uma vez por dia.

4.16. Usar Senhas Fortes

De que vai adiantar ter todo este trabalho de escolher uma boa hospedagem, de instalar um sistema operacional seguro, atualizar o sistema e efetuar diversas medidas para melhorar a segurança, nada vai adiantar se usarmos senhas fracas.

É como cagar e não limpar o c*.

Senhas fortes são grandes (8 dígitos ou mais) e usam uma mistura de algarismos, letras minúsculas, letras maiúsculas e símbolos.

4.17. Melhorando a segurança de sites com Joomla

O site está em
/var/www/html/portal

- Copiar configuration.php para o /var/www com o nome cfg.php
- Remover todo o conteúdo do /portal/configuration.php e deixar apenas estas duas linhas:

```
<?php
require_once( dirname( __FILE__ ) . '/../..'/cfg.php' );
```

Obs.: lembre de fazer o backup do arquivo cfg.php, que agora está fora do html.

4.18. Melhorar a segurança no Desktop

Melhorar a segurança no desktop é importante para maior segurança do servidor. Hábitos saudáveis como usar um sistema operacional seguro e atualizado, como usando o firewall ativo e fechando tudo que pode.

Assim como também instalando boas ferramentas de monitoramento do servidor.

Instalar no micro desktop o W3AF

```
apt-get install w3af
```

Traz uma interface para a console e uma gráfica/web

Testando vulnerabilidades web com Nikto

O Nikto é web server scanner escrito em perl usado para detectar vulnerabilidades em servidores web. Ele é muito simples de ser usado e atualizado gerando relatórios em txt, html e csv.

Requer repositório multiverse no /etc/apt/sources.list

```
apt-get install nikto
```

Atualizando os plugins:

```
nikto -update
```

Usando o Nikto

```
nikto -h HOST -p PORT
```

```
nikto -h HOST -p PORT -ssl
```

```
nikto -h ribafs.org
```

```
nikto -C all -host 200.128.X.X -o vitima.txt (mude X.X pelos números desejados)
```

- C all - Força a checagem de todos os diretórios em busca de cgi

- host - Ip da vitima

-o - Gera um arquivo de relatório

Varrendo uma porta de um host:

```
nikto -h google.com -p 443
```

Help
nikto -H | less

Esta ferramenta tanto ajuda a defender o seu site quanto ajuda para quem quer perceber vulnerabilidades em outros sites ou atacar.

Documentação oficial:
<http://cirt.net/nikto2-docs/>

Exemplos de uso:
<http://cirt.net/nikto2-docs/usage.html>

4.19. Melhorando a Segurança do MySQL

Uma forma de melhorar a segurança do mysql é criar usuários restritos, que somente tenham poder de agir num banco específico.

O exemplo abaixo é usado para criar um usuário a ser usado em site com Joomla:

```
mysql -u root -p  
create database portal;
```

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senha' WITH GRANT OPTION;  
\q
```

Importar Script:
mysql -u root -p portal < portal.sql

Exportar banco para script:
mysqldump -u root -p portal > portal.sql

Também importante é executar

```
mysql_secure_installation
```

4.20. Melhorando a segurança com Lynis

Executa diversos testes a procura de vulnerabilidade no sistema.

Instalação (abaixo é uma só linha)

```
wget -O - http://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add - > /dev/null
```

```
echo "deb [arch=amd64] https://packages.cisofy.com/community/lynis/deb/ trusty
main" | sudo tee -a /etc/apt/sources.list.d/cisofy-lynis.list
```

```
sudo apt-get update
```

```
sudo apt install lynis
```

Atualização

```
sudo lynis --help
```

```
sudo lynis update info
```

Executando

```
sudo lynis audit system
```

Guarda os relatórios em

```
- Test and debug information : /var/log/lynis.log
- Report data                : /var/log/lynis-report.dat
```

Dica: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

Audit remoto

```
sudo lynis audit system remote ribafs.org
```

How to perform a remote scan:

```
=====
```

```
Target : ribafs.org
```

```
Command : ./lynis audit system --quick ribafs.org
```

* Step 1: Create tarball

```
mkdir -p ./files && cd .. && tar czf ./lynis/files/lynis-remote.tar.gz --exclude=files/lynis-remote.tar.gz ./lynis && cd lynis
```

* Step 2: Copy tarball to target ribafs.org

```
scp -q ./files/lynis-remote.tar.gz ribafs.org:~/tmp-lynis-remote.tgz
```

* Step 3: Execute audit command

```
ssh ribafs.org "mkdir -p ~/tmp-lynis && cd ~/tmp-lynis && tar xzf ../tmp-lynis-remote.tgz && rm ../tmp-lynis-remote.tgz && cd lynis && ./lynis audit system --quick ribafs.org"
```

* Step 4: Clean up directory

```
ssh ribafs.org "rm -rf ~/tmp-lynis"
```

* Step 5: Retrieve log and report

```
scp -q ribafs.org:~/tmp/lynis.log ./files/ribafs.org-lynis.log
```

```
scp -q ribafs.org:~/tmp/lynis-report.dat ./files/ribafs.org-lynis-report.dat
```

* Step 6: Clean up tmp files (when using non-privileged account)

```
ssh ribafs.org "rm /tmp/lynis.log /tmp/lynis-report.dat"
```

Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

4.21. Cuidados Extras

Busca por backdoors

```
grep -iR 'c99' /var/www/html/  
grep -iR 'r57' /var/www/html/  
find /var/www/html/ -name \*.php -type f -print0 | xargs -0 grep c99  
grep -RPn "(passthru|shell_exec|system|base64_decode|fopen|fclose|eval)"  
/var/www/html/
```

Referência

<https://geek.linuxman.pro.br/geek/ubuntu-pronto-para-guerra>

<https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1604-lts-server-part-1-basics>

<https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/>

<https://hostpresto.com/community/tutorials/how-to-install-and-use-lynis-on-ubuntu-14-04/>

5 - Monitorando um servidor Linux Ubuntu 16.04

Espaço em disco

```
df -h
```

Memória RAM e Swap

```
free -m
```

Monitorar serviços na memória com sysv-rc-conf

Instalar

```
sudo apt install sysv-rc-conf
```

Testando se portas estão abertas

```
telnet smtp.gmail.com 587
```

```
telnet smtp.gmail.com 25
```

Monitorar arquivos modificados

```
find /var/www/html -type f -ctime -1 -exec ls -ls {} \;
```

Podemos colocar no cron para que seja executado a cada madrugada e nos envie um e-mail.

Procurar arquivos com 666

```
find /var/www/html -xdev -perm +o=w ! \( -type d -perm +o=t \) ! -type l -print
```

Procurar diretórios com 777

```
find /var/www/html -type d -perm -o+w -exec ls -ld {} \;
```

Procurar contas sem senha

```
awk -F: '($2 == "") {print}' /etc/shadow
```

Monitorar login do root

```
sudo apt install mailutils
```

Adicione ao início do script .bashrc do root:

```
nano /root/.bashrc
```

```
echo -e "Acesso ao shell do Root em `tty` \n `w`" | mail -s "Alerta: Acesso do root" ribafs@gmail.com
```

Notificação de acesso via ssh pelo ribafs

```
cd /home/ribafs
```

```
nano .bashrc
```

```
echo 'ALERT - Root Shell Access (ServerName) on:' `date` `who` | mail -s "Alert: Root Access from `who` | cut -d'(' -f2 | cut -d')' -f1`" ribafs@gmail.com
```

5.1 - Varrendo portas abertas com Nmap

O nmap é um software para descobrir a rede e para auditar segurança. Melhor é instalar no desktop para varrer do mesmo.

Instalação

```
apt install nmap
```

Varrer seu sistema por portas abertas

```
nmap -v -sT localhost
```

Saída

```
Not shown: 995 closed ports
```

```
PORT      STATE SERVICE
```

```
25/tcp    open  smtp
```

```
80/tcp    open  http
```

```
443/tcp   open  https
```

```
3306/tcp  open  mysql
```

```
5432/tcp  open  postgresql
```

Lembrando que varre apenas até a porta 1000, portanto não mostrou a do ssh
Outro detalhe é que para acesso externo somente as portas 80 e 443, as demais oferecem acesso somente interno.

O acesso externo se dá ao mysql somente através do Apache. O visitante do site acessa o site pela porta 80 ou 443 e chega até aqui ao servidor, aqui o apache vai ao mysql e solicita o que deseja. O mysql somente é acessado via localhost.

```
sudo nmap -v -sS localhost.
```

É importante executar manualmente alguns softwares como:

- rkhunter

```
rkhunter --update
```

```
rkhunter --propupd
```

```
rkhunter --check
```

```
tail /var/log/rkhunter.log
```

- nikto

```
nikto -h ribafs.org
```

```
nikto -C all -host 200.128.12.34 -o vitima.txt
```

- psad

```
psad -S
```

```
tail /var/log/psad
```

- denyhosts

```
/etc/hosts.allow - permitidos
```

/etc/hosts.deny - negados

- ngrep
ngrep -d any port 25

- nmap
nmap -v -sT localhost
nmap -v -A dominio.com

Scannear SYN:
nmap -v -sS localhost

netstat -tulp
nmap -sTU 10.40.100.123

ls -li -n | egrep 'COMMAND|LISTEN|UDP'

- arquivos modificados
find /var/www -type f -ctime -1 -exec ls -ls {} \;

Procurar arquivos com 666
find /var/www -xdev -perm +o=w ! \(-type d -perm +o=t \) ! -type l -print

Procurar diretórios com 777
find /var/www -type d -perm -o+w -exec ls -ld {} \;

Procurar contas sem senha
awk -F: '(\$2 == "") {print}' /etc/shadow

- atualizar permissões do /var/www/html

chown -R www-data:www-data /var/www/html
find /var/www/html -type d -exec chmod 2755 {} \;
find /var/www/html -type f -exec chmod 0644 {} \;

Ou executar o script
- logs

Apache /var/log/apache2
access.log
error.log

Mail /var/log/
mail.log
mail.err
mail.info
mail.warn
tail -f /var/log/mail.log /var/log/iredapd.log /var/log/cbpolicyd.log

Mysql /var/log/mysql

error.log

Outros /var/log

auth.log

fail2ban.log

mysql.err

mysql.log

syslog

user.log

Adicionar Serviços ao Boot num Debian

cd /etc/init.d (exemplo)

update-rc.d firewall defaults

Remover serviços do boot

cd /etc/init.d

update-rc.d -f bluetooth remove

Ferramentas para gerenciar serviços no boot

sysv-rc-conf - mostra todos os runlevel

rcconf - pode alterar, mas mostra poucos

chkconfig - só mostra, não altera

apt-get install sysv-rc-conf rcconf chkconfig

Desativar os serviços não usados

Usuários logados:

who

Usuário atual

whoami

Dividindo a tela em duas

Como dois terminais um acima e outro abaixo com o Splitvt

sudo apt install splitvt

Divide tela ao meio abrindo dois terminais

Para mudar para cima ou abaixo, clicar com o mouse

A tela ficará dividida em duas. Digite "tty" e aperte [Enter] para ser mostrado o dispositivo correspondente. Você verá que este é um terminal virtual. Alterne de terminal apertando [Ctrl]+[W] e repita o procedimento. O resultado será o mesmo, mudando apenas de número.

Para sair aperte

[Ctrl]+[O] e então [Q].

Podemos chegar a conclusão de que sobre um terminal real rodavam dois terminais virtuais.

Usando htop

```
apt-get install htop
```

```
htop
```

Monitorando a rede

```
iptraf - monitorar a rede
```

```
apt-get install iptraf
```

Usando

```
iptraf
```

```
netstat -a
```

```
netstat -at
```

```
netstat -s
```

du - mostra todos todos os subdiretórios e seus tamanhos

du -sh (silente e mostrando total do diretório atual em GB)

du -a (tamanhos de cada diretório e cada arquivo)

Verificando BlackLists

Quando um certo IP foi para uma lista negra por engano ou de qualquer forma queremos remover, que procedimentos devemos executar?

Ver a lista do mod_evasive:

```
nano /etc/apache2/mods-available/mod-evasive.conf
```

Ver a lista do Denyhosts:

```
nano /etc/hosts.deny
```

Adicionar assim:

```
ALL: 65.61.204.40
```

Ver os Ips barrados pelo fail2ban:

```
iptables -L | grep IP
```

Como saber que portas estão abertas

```
apt-get install nmap
```

```
nmap -v localhost
```

```
nmap -v 192.168.0.1
```

Instalar no desktop

```
sudo apt-get install wireshark
```

Monitorando logs

```
tail -f 50 /var/log/mail.log
less +F /var/mail.log
```

Monitorando a rede com ngrep

```
apt-get install ngrep
ngrep -h (help)
```

Usando:

```
Ficar escutando na porta 25
ngrep -d any port 25
```

Monitorar todas as atividades cruzando origem e destino da porta 25 (SMTP)
Observe que o terminal fica parado a espera de ações na porta 25. Envie um e-mail do seu servidor para qualquer e-mail e veja o que acontece.

```
ngrep -d any 'error' port syslog
```

Monitorar qualquer tráfego na rede baseado no syslog procurando a ocorrência da palavra ``error".

```
ngrep -wi -d any 'user|pass' port 21
```

Monitorar qualquer tráfego cruzando origem e destino na porta 21

Origem: <http://ngrep.sourceforge.net/usage.html>

Cuidados Extras

Busca por backdoors

```
grep -iR 'c99' /var/www/html/
grep -iR 'r57' /var/www/html/
find /var/www/html/ -name \*.php -type f -print0 | xargs -0 grep c99
grep -RPn "(passthru|shell_exec|system|base64_decode|fopen|fclose|eval)"
/var/www/html/
```

5.2 - Auditar segurança do sistema com Tiger e Tripwire

Tiger é uma ferramenta de segurança que pode ser usada para auditoria e detecção de intrusão do sistema.

Tripwire é um sistema de detecção de intrusão (HIDS) que checa a integridade de arquivos e pastas.

Detalhes

<https://www.digitalocean.com/community/tutorials/how-to-use-tripwire-to-detect-server-intrusions-on-an-ubuntu-vps>

Instalação

```
apt install tiger tripwire
```

Responda sim para fornecer senha para arquivos e guarde bem as senhas

Criar banco de dados

```
tripwire --init
```

Entre com a senha fornecida acima.

Criar arquivo de política

```
twadmin --create-polfile /etc/tripwire/twpol.txt
```

Entre com a senha fornecida acima.

Executando tiger

```
tiger
```

Toda a saída do tiger pode ser vista em:

```
/var/log/tiger
```

Para visualizar o relatório de segurança do tiger:

```
less /var/log/tiger/security.report*
```

Aqui ele gerou este:

```
/var/log/tiger/security.report.ribafs.org.180214-20:50
```

6 – Segurança em Servidores Linux

Os cuidados com a segurança colaboram para que os sites e aplicativos instalados no servidor sejam executados de forma esperada, rápida e sem interrupção.

Princípios básicos de segurança:

- Hospede seu site em servidor seguro
- Efetue backup regularmente, especialmente a cada alteração no site
 - A melhor opção atualmente para backup é o Akeeba Backup - <https://www.akeebabackup.com/download.html>
 - Caso tenha dificuldade de usar o formato JPA, altere em Configuration - Archiver engine para ZIP format
 - Ele gera o backup com um instalador. Para restaurar apenas instale como se fosse instalar o Joomla
 - Faça também backup dos scripts de configuração do servidor para o caso de uma reinstalação
 - Lembre de fazer o backup do servidor com os recursos da hospedagem ou crie um snapshot
- Também faça teste de restore de vez em quando para garantir que o backup está íntegro
- A quantidade de cópias de backup a ser guardada depende da importância do site. Se mais importante mais cópias
- As cópias devem ser armazenadas em mídia confiável: HD e DVD
- Efetue atualização com frequência. Mantenha o aviso de atualização ativo para que receba um aviso por e-mail e atualize imediatamente
- Após a primeira atualização reinicie o servidor
- Acessar de forma segura usando SSH (enxuto e configurado para salvar a senha) e nunca via FTP
- Manter seu desktop seguro, usando um sistema operacional seguro no mesmo, com firewall e outros cuidados
- Use e abuse da comunidade com seus conhecimentos e generosidade para manter-se atualizado em termos de segurança e proteger seu site
- Use senhas fortes
- Use o SSL para proteger pelo menos o administrador
- Use boas extensões para reforçar a segurança
- Remova todas as extensões que não estiver usando e não somente desabilite
- Evite instalar pacotes para desenvolvimento como gcc, make, etc e evite também instalar repositórios instáveis.
- Monitorar frequentemente os logs à procura de algo suspeito em todos os serviços ativos
 - Use softwares tipo IDS que detectam intrusões
 - Instalar um bom firewall de aplicativos como o mod_security
 - Ficar bem atento, estudando, se informando sempre sobre o assunto de que cuida
 - Logo após a configuração final do servidor já crie um backup ou snapshot da droplet e fique atento para criar outro logo que o servidor esteja concluído e bem configurado.
 - Uma boa ideia é ter uma box no Vagrant do Ubuntu 16.04 em seu desktop, sendo cópia fiel e original do servidor localmente, mesma distribuição, mesma versão

6.1 - Atualizar automaticamente somente as atualizações de segurança

```
aptitude install unattended-upgrades
```

```
nano /etc/apt/apt.conf.d/10periodic
```

Excluir tudo e adicionar:

```
APT::Periodic::Update-Package-Lists "1";  
APT::Periodic::Download-Upgradeable-Packages "1";  
APT::Periodic::AutocleanInterval "7";  
APT::Periodic::Unattended-Upgrade "1";
```

Isso somente atualiza pacotes de segurança

Atualização completa, de todos os pacotes:

```
apt-get update  
apt-get upgrade
```

Atualiza o servidor manualmente pelo menos uma vez por dia.

6.2 – Remover serviços que não estão em uso

Parar e depois remover

```
sudo service cups stop  
sudo systemctl disable cups
```

6.3 – Senhas Fortes

De que vai adiantar ter todo este trabalho de escolher uma boa hospedagem, de instalar um sistema operacional seguro, atualizar o sistema e efetuar diversas medidas para melhorar a segurança, nada vai adiantar se usarmos senhas fracas.

É como cagar e não limpar o c*.

Senhas fortes são grandes (8 dígitos ou mais) e usam uma mistura de algarismos, letras minúsculas, letras maiúsculas e símbolos.

6.4 – Ferramentas

Testes de vulnerabilidade online

<https://geekflare.com/online-scan-website-security-vulnerabilities/>

Bons clientes de sftp

FileZilla - <http://filezilla.sourceforge.net/>

WinSCP - <http://winscp.net/>

<https://www.digitalocean.com/community/tutorials/an-introduction-to-securing-your-linux-vps>

<https://www.serverwatch.com/server-trends/10-secure-linux-distributions-you-need-know-about.html>

<https://www.linux.com/learn/how-make-your-linux-server-more-secure>

<https://documentation.cpanel.net/display/68Docs/Configure+PHP+and+suEXEC>

<http://www.alain.knaff.lu/howto/PhpSuexec/>

<http://blog.stuartherbert.com/php/2008/01/18/using-suphp-to-secure-a-shared-server/>

<https://linsider.wordpress.com/2009/11/21/how-to-suphp-an-alternative-to-phpsuexec/>

<https://suphpexecute.wordpress.com/>

<https://geekflare.com/nginx-webserver-security-hardening-guide/>

<https://geekflare.com/install-modsecurity-on-nginx/>

<https://geekflare.com/nginx-webserver-security-hardening-guide/>

<https://geekflare.com/modsecurity-owasp-core-rule-set-nginx/>

<https://www.vultr.com/docs/how-to-install-modsecurity-for-nginx-on-centos-7-debian-8-and-ubuntu-16-04>

https://www.howtoforge.com/tutorial/install-nginx-with-mod_security-on-ubuntu-15-04/

<https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-16-04>

<https://rikynity.wordpress.com/2012/05/30/installing-nginx-with-php5-and-php-fpm-and-mysql-support-on-ubuntu-11-04/>

<https://www.binarytides.com/install-nginx-php-fpm-mariadb-debian/>

Tutorial: Nginx com PHP 7 e MySQL no Ubuntu 16.04 LTS

<https://pplware.sapo.pt/tutoriais/tutorial-nginx-php-7-mysql-no-ubuntu-16-04-lts/?format=pdf>

6.5 – Desempenho do Servidor

Gostaria da opinião de colegas que têm experiências parecidas.

Até hoje tenho usado sites em hospedagem compartilhada ou em VPS usando Ubuntu e Apache.

Agora estou testando VPS na DigitalOcean e me parece que 1GB da RAM oferecido agora não dá o desempenho de 512 há algum tempo.

Então comecei a repensar minhas escolhas. Primeiro mudei para Debian. Não tive a facilidade de usar o ufw na versão 9.3 do Debian e desisti. Depois fui testar o nginx, que dizem ter melhor desempenho que o Apache. Também tive dificuldades em configurar com php e desisti.

Acontece que estou gostando do DO e como está com Ubuntu e Apache não tá dando para usar o plano menor.

Então decidi usar o Debian 9.3 com iptables e pesquisar bem o uso do nginx. Desta vez, com mais interesse, deu certo. Fui tendo um problema e fui resolvendo. Esta sensação de poder/controle me agrada.

Logo percebi as leves diferenças de desempenho. Agora com Debian 9.3, nginx e iptables me parece que o site fica melhor.

Então usar a ferramenta online:

<https://tools.pingdom.com/> (Website speed teste). Ela me fala várias coisas, entre elas que meu novo site, com Debian e cia tem um Load time de 1.11 segundos enquanto a outra com Debian fica com 3.70 segundos. O antigo era melhor que os 43% de sites testados enquanto que usando Debian e cia é melhor que 87% dos testados.

Gostaria de "ouvir" o que tem a dizer outros colegas que passaram por algo assim.

O servidor com Ubuntu já está usando swap, enquanto que o com Debian não está.

Edson Correia no Joomla Brasil - Ribamar FS é praticamente impossível listar todos os fatores que podem deixar um servidor mais rápido ou mais lento. É uma mistura de hardware com software, configurações finas, largura de banda, quantidade de acessos, localização do servidor, etc. Se formos analisar os aspectos isolados, sim: Nginx é extremamente mais rápido que o Apache, pelo fato de não ter diversas funcionalidades extras que o Apache tem, mas que não fazem falta para a grande maioria dos sites. Outra coisa que faz o site acelerar bastante, principalmente o nosso amado Joomla, é o PHP 7. Há um ganho de velocidade perceptível entre o 7 e o 5.6. Eu também uso Digital Ocean e vi que eles atualizaram os planos, mas não sei quanto ao desempenho como mencionou... Não duvido que tenham piorado em certa medida, pois não existe almoço

grátis... Mas, pode ser também que você esteja experimentando performances diferentes diante das diversas opções de sistema operacional / servidor web que tem testado. Eu sigo os tutoriais do site Fator Binário que são muito bons e ensinam como montar um Debian com ISPConfig que usa Nginx e fica bastante rápido. Depois dá uma olhada lá.

Rafael Oliveira de Santana no Joomla Brasil

Edson já respondeu tudo. Só adicionando uma informação.... Digital Ocean, Vultr e Linode são as melhores opções custo benefício em Vps. Escolha uma opção que tenha uma latência baixa. As do Sul do EUA por exemplo. Na Vultr tem a opção de Miami... Média de 400 ms. Em termo de hardware, latência eu acho melhor, bem acompanhado da Linode e depois a Digital Ocean. No fator binário o foco é utilizar o ispconfig, um painel free e ótima alternativa ao pago Cpanel. Utilizando nginx no debandada. Assim, como tutoriais relacionado de segurança, email. Tudo pra vc gerenciar seus sites de forma fácil, sem ser na mão.

<https://developers.google.com/speed/pagespeed/insights/>

Sugestões de otimização

- Ativar compactação
- Eliminar JavaScript e CSS de bloqueio de renderização no conteúdo acima da borda
- Aproveitar cache do navegador
- Otimizações já implementadas
- Compactar CSS
- Sua CSS está reduzida. Saiba mais sobre como reduzir a CSS.
- Compactar HTML
- Seu HTML está reduzido. Saiba mais sobre como reduzir o HTMLI.
- Compactar JavaScript
- Seu conteúdo JavaScript está reduzido. Saiba mais sobre como reduzir o JavaScript.
- Evitar redirecionamentos da página de destino
- Sua página não tem redirecionamentos. Saiba mais sobre como evitar os redirecionamentos da página de destino.
- Otimizar imagens
- Suas imagens estão otimizadas. Saiba mais sobre como otimizar as imagens.
- Priorizar o conteúdo visível
- Você tem conteúdo acima da dobra com a prioridade correta. Saiba mais sobre como priorizar o conteúdo visível.
- Reduzir o tempo de resposta do servidor
- Seu servidor respondeu rapidamente. Saiba mais sobre a otimização do tempo de resposta do servidor.

Outras ferramentas

<https://www.webpagetest.org/>

<https://gtmetrix.com/analyze.html>

<https://developers.google.com/speed/pagespeed/insights/>

<https://tools.pingdom.com/>

Edson Correia no Joomla Brasil Essas compactações automáticas raramente funcionam a contento. Todas as vezes que eu ativei tais otimizações o site quebrou todo. E do que funcionava não ficava tão rápido a ponto de ser perceptível. Então pela minha experiência

o que posso dizer é que não esquite tanto com essas pseudo otimizações. É mais efetivo usar um servidor não compartilhado como um vps e usar os métodos nativos do Joomla como cache e compressão gzip. Se o servidor tiver caches como APC ou Memcache são melhores que o cache nativo do Joomla. E se puder usar uma CDN como a Cloudflare isso também ajuda muito.

6.6 – Criptografia

OpenSSL

Criptografar um arquivo texto ou tar. O arquivo é criptografado com uma senha e quem a conhecer poderá descriptografar

Criptografar o arquivo.txt para arquivo.aes

```
openssl aes-128-cbc -salt -in arquivo.txt -out arquivo.aes
```

Descriptografar o arquivo.aes para arquivo.txt

```
openssl aes-128-cbc -d -salt -in arquivo.aes -out arquivo.txt
```

Empacotar com tar e criptografar todo um diretório

```
tar -cf - pasta | openssl aes-128-cbc -salt -out pasta.tar.aes
```

Desempacotar e descriptografar

```
openssl aes-128-cbc -d -salt -in pasta.tar.aes | tar -x -f -
```

Empacotar e zipar todo um diretório criptografar

```
tar -zcf - pasta | openssl aes-128-cbc -salt -out pasta.tar.gz.aes
```

Deszipar e descriptografar

```
openssl aes-128-cbc -d -salt -in pasta.tar.gz.aes | tar -xz -f -
```

Use -k senha após aes-128-cbc para evitar a requisição interativa da senha

Use aes-256-cbc ao invés de aes-128-cbc para ter uma criptografia mais forte, mas exigirá mais CPU

GPG

O arquivo é criptografado com uma senha e quem a conhecer poderá descriptografar

GPG adiciona uma extensão .gpg ao arquivo criptografado

Criptografar o arquivo file

```
gpg -c file
```

Descriptografar

```
gpg file.gpg
```

Usando chaves

```
gpg --gen-key
```

Isso pode demorar

```
~/.gnupg/pubring.gpg      # Contains your public keys and all others imported
~/.gnupg/secring.gpg     # Can contain more than one private key
```

Opções mais usadas

-e encrypt data

-d decrypt data

-r NAME encrypt for recipient NAME (or 'Full Name' or 'email@domain')

-a create ascii armored output of a key

-o use as output file

Criptografia apenas para uso pessoal

```
gpg -e -r 'Your Name' file      # Encrypt with your public key
gpg -o file -d file.gpg        # Decrypt. Use -o or it goes to stdout
```

Criptografar e Descriptografar com chave

```
gpg -a -o alicekey.asc --export 'Alice' # Alice exported her key in ascii file.
gpg --send-keys --keyserver subkeys.pgp.net KEYID # Alice put her key on a server.
gpg --import alicekey.asc # You import her key into your pubring.
gpg --search-keys --keyserver subkeys.pgp.net 'Alice' # or get her key from a server.
```

Logo que a chave é importada fica fácil de criptografar e descriptografar

```
gpg -e -r 'Alice' file # Encrypt the file for Alice.
gpg -d file.gpg -o file # Decrypt a file encrypted by Alice for you.
```

Administração de chaves

Key administration

```
# gpg --list-keys # list public keys and see the KEYIDS
```

The KEYID follows the '/' e.g. for: pub 1024D/D12B77CE the KEYID is D12B77CE

```
# gpg --gen-revoke 'Your Name'      # generate revocation certificate
# gpg --list-secret-keys            # list private keys
# gpg --delete-keys NAME           # delete a public key from local key ring
# gpg --delete-secret-key NAME     # delete a secret key from local key ring
# gpg --fingerprint KEYID         # Show the fingerprint of the key
# gpg --edit-key KEYID             # Edit key (e.g sign or add/del email)
```

6.6 - Melhorar a segurança da memória compartilhada

Edite o fstab e adicione a linha ao final.
Somente após o reboot terá efeito:

```
nano /etc/fstab
tmpfs /run/shm tmpfs defaults,noexec,nosuid 0 0
```

6.7 – Firewall

6.7.1 – IPTables

<https://www.vivaolinux.com.br/artigo/IPTABLES-Conceitos-e-aplicacao>
<https://www.hostinger.com.br/tutoriais/tutorial-iptables/>

O Kernel do Linux traz uma inovação no que diz respeito a ferramenta de firewall padrão do sistema.

iptables - Sistema de controle de filtros para protocolos ipv4. É com ele que montamos as regras do firewall;

iptables-save - Salva as regras em um arquivo especificado como argumento do comando. Normalmente não utilizamos este aplicativo e sim um shell script (por exemplo rc.firewall), inicializado pelo sistema;

iptables-restore - Restaura regras salvas pelo utilitário iptables-save.

Regras

As regras são como filtros aplicados ao iptables para que o mesmo implemente o que chamamos de filtro de pacote de acordo com o endereço IP/porta de origem/destino, interface de origem/destino, etc. As regras são armazenadas dentro dos chamados chains e processadas na ordem que são inseridas. Estas mesmas regras são armazenadas no kernel, o que significa que quando o sistema é reinicializado as mesmas são perdidas.

A sintaxe de uma regra é a seguinte:

iptables comando parâmetros extensões

Algo similar a isto na prática:

```
# iptables -A INPUT p- tcp -s 10.0.0.1 -j DROP
```

Uma regra é uma linha do arquivo de configuração

Comandos principais

Basicamente o IPTABLES tem as seguintes regras:

ACCEPT: significa que o pacote seguirá adiante.

DROP: significa que o pacote não seguirá adiante.

RETURN: significa que voltaremos as regras do pacote anterior.

INPUT: esse canal envia ao servidor, pacotes de entrada que podem ser bloqueados ou liberados via portas, protocolos ou endereços de IP.

Forward: esse canal é usado para filtrar pacotes que chegam ao servidor mas que precisam ser mandados adiante.

Output: esse canal é usado para filtrar pacotes que irão a outro servidor.

Comandos básicos do iptables:

-A - Este comando acrescenta uma regra às existentes no sistema, ou seja, permite colocar/atualizar regras já existentes na estrutura do firewall.

-I - Este comando insere uma nova regra dentro das existentes no firewall.

-D - Este comando exclui uma regra específica no firewall.

-P - Este comando define a regra padrão do firewall.

-L - Este comando lista todas as regras existentes no firewall.

-F - Este comando zera todas as regras do firewall (o chamado flush). Se este comando for executado todas as regras do firewall são excluídas.

-h - Invoca o help, ajuda do comando.

-R - Este comando substitui uma regra no firewall.

-C - Checa as regras básicas do firewall.

-Z - Zera uma regra específica.

-N - Cria uma nova regra com um nome específico.

-X - Exclui uma regra específica por seu nome.

Para listar as regras atuais:

```
iptables -L
```

Listar com números de linhas

```
iptables -L --line-numbers
```

Para apagar todas as regras

```
iptables -F
```

```
/sbin/iptables-save
```

CentOS 7 está usando FirewallD agora!

Desabilitar firewalld e remover:
systemctl disable firewalld

Então instalar iptables-service:
yum install iptables-services

Habilitar como serviço
systemctl enable iptables
ou
systemctl enable iptables.service

service iptables restart
ou
systemctl restart iptables

Mostrar regras atuais

```
iptables -L
```

ou

```
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP  
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP  
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
```

```
iptables -L --line-numbers
```

```
iptables -A INPUT -i lo -j ACCEPT  
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT  
iptables -A INPUT -p tcp --dport 65522 -j ACCEPT  
iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate  
NEW,ESTABLISHED -j ACCEPT  
iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate  
ESTABLISHED -j ACCEPT  
iptables -P OUTPUT ACCEPT  
iptables -P INPUT DROP
```

```
iptables -L -n
```

```
service iptables save
```

Salvar cópia das regras

```
iptables-save > /home/ribafs/iptables_rules.v4
```

Salvar as regras do iptables:

```
systemctl restart iptables
```

Referências

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-basic-iptables-firewall-on-centos-6>

Exemplo de Firewall

```
#!/bin/bash
IPT="/sbin/iptables"

##### IPS #####
# Get server public ip
SERVER_IP=$(ifconfig eth0 | grep 'inet addr:' | awk -F'inet addr:' '{ print $2}' | awk '{ print $1}')
LB1_IP="204.54.1.1"
LB2_IP="204.54.1.2"

# Do some smart logic so that we can use damm script on LB2 too
OTHER_LB=""
SERVER_IP=""
[[ "$SERVER_IP" == "$LB1_IP" ]] && OTHER_LB="$LB2_IP" || OTHER_LB="$LB1_IP"
[[ "$OTHER_LB" == "$LB2_IP" ]] && OPP_LB="$LB1_IP" || OPP_LB="$LB2_IP"

### IPs ###
PUB_SSH_ONLY="122.xx.yy.zz/29"

##### FILES #####
BLOCKED_IP_TDB=/root/.fw/blocked.ip.txt
SPOOFIP="127.0.0.0/8 192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 169.254.0.0/16 0.0.0.0/8
240.0.0.0/4 255.255.255.255/32 168.254.0.0/16 224.0.0.0/4 240.0.0.0/5 248.0.0.0/5
192.0.2.0/24"
BADIPS=$( [[ -f ${BLOCKED_IP_TDB} ]] && egrep -v "^#|^$" ${BLOCKED_IP_TDB})

### Interfaces ###
PUB_IF="eth0" # public interface
LO_IF="lo" # loopback
VPN_IF="eth1" # vpn / private net

### start firewall ###
echo "Setting LB1 $(hostname) Firewall..."

# DROP and close everything
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

# Unlimited lo access
$IPT -A INPUT -i ${LO_IF} -j ACCEPT
$IPT -A OUTPUT -o ${LO_IF} -j ACCEPT
```

```

# Unlimited vpn / pnet access
$IPT -A INPUT -i ${VPN_IF} -j ACCEPT
$IPT -A OUTPUT -o ${VPN_IF} -j ACCEPT

# Drop sync
$IPT -A INPUT -i ${PUB_IF} -p tcp ! --syn -m state --state NEW -j DROP

# Drop Fragments
$IPT -A INPUT -i ${PUB_IF} -f -j DROP

$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL ALL -j DROP

# Drop NULL packets
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL NONE -m limit --limit 5/m --limit-burst 7
-j LOG --log-prefix " NULL Packets "
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL NONE -j DROP

$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

# Drop XMAS
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags SYN,FIN SYN,FIN -m limit --limit 5/m --limit-
burst 7 -j LOG --log-prefix " XMAS Packets "
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP

# Drop FIN packet scans
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags FIN,ACK FIN -m limit --limit 5/m --limit-burst
7 -j LOG --log-prefix " Fin Packets Scan "
$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags FIN,ACK FIN -j DROP

$IPT -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP

# Log and get rid of broadcast / multicast and invalid
$IPT -A INPUT -i ${PUB_IF} -m pkttype --pkt-type broadcast -j LOG --log-prefix "
Broadcast "
$IPT -A INPUT -i ${PUB_IF} -m pkttype --pkt-type broadcast -j DROP

$IPT -A INPUT -i ${PUB_IF} -m pkttype --pkt-type multicast -j LOG --log-prefix " Multicast "
$IPT -A INPUT -i ${PUB_IF} -m pkttype --pkt-type multicast -j DROP

$IPT -A INPUT -i ${PUB_IF} -m state --state INVALID -j LOG --log-prefix " Invalid "
$IPT -A INPUT -i ${PUB_IF} -m state --state INVALID -j DROP

# Log and block spoofed ips
$IPT -N spooflist
for ipblock in $SPOOFIP
do
    $IPT -A spooflist -i ${PUB_IF} -s $ipblock -j LOG --log-prefix " SPOOF List Block "
    $IPT -A spooflist -i ${PUB_IF} -s $ipblock -j DROP

```

```

done
$IPT -I INPUT -j spooflist
$IPT -I OUTPUT -j spooflist
$IPT -I FORWARD -j spooflist

# Allow ssh only from selected public ips
for ip in ${PUB_SSH_ONLY}
do
  $IPT -A INPUT -i ${PUB_IF} -s ${ip} -p tcp -d ${SERVER_IP} --destination-port 22 -j
ACCEPT
  $IPT -A OUTPUT -o ${PUB_IF} -d ${ip} -p tcp -s ${SERVER_IP} --sport 22 -j ACCEPT
done

# allow incoming ICMP ping pong stuff
$IPT -A INPUT -i ${PUB_IF} -p icmp --icmp-type 8 -s 0/0 -m state --state
NEW,ESTABLISHED,RELATED -m limit --limit 30/sec -j ACCEPT
$IPT -A OUTPUT -o ${PUB_IF} -p icmp --icmp-type 0 -d 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT

# allow incoming HTTP port 80
$IPT -A INPUT -i ${PUB_IF} -p tcp -s 0/0 --sport 1024:65535 --dport 80 -m state --state
NEW,ESTABLISHED -j ACCEPT
$IPT -A OUTPUT -o ${PUB_IF} -p tcp --sport 80 -d 0/0 --dport 1024:65535 -m state --state
ESTABLISHED -j ACCEPT

# allow outgoing ntp
$IPT -A OUTPUT -o ${PUB_IF} -p udp --dport 123 -m state --state NEW,ESTABLISHED -j
ACCEPT
$IPT -A INPUT -i ${PUB_IF} -p udp --sport 123 -m state --state ESTABLISHED -j ACCEPT

# allow outgoing smtp
$IPT -A OUTPUT -o ${PUB_IF} -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j
ACCEPT
$IPT -A INPUT -i ${PUB_IF} -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT

#### add your other rules here ####

#####
# drop and log everything else
$IPT -A INPUT -m limit --limit 5/m --limit-burst 7 -j LOG --log-prefix " DEFAULT DROP "
$IPT -A INPUT -j DROP

```

Limpar IPTables

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

6.7.2 – ufw

UFW

Resumo

```
ufw status verbose
ufw enable
```

```
ufw allow 65522
ufw logging on
ufw allow http
ufw allow https
```

```
ufw status verbose
```

O ufw é um firewall nativo do Ubuntu, que é bem simples de implementar que é uma interface para o IPTables.

Tutorial - <https://help.ubuntu.com/community/UFW>

Verificando seu status:

```
sudo ufw status    # Estado: inativo
```

Não requer instalação, pois ele já vem instalado por padrão no Ubuntu. Apenas precisamos habilitá-lo.

```
sudo ufw enable
```

Ao habilitar ele fecha todas as entradas e abre todas as saídas e habilita na inicialização do sistema:

```
sudo ufw status verbose
```

```
ufw allow from 177.14.224.188 to any port 65522
```

Veja o que diz:

Estado: ativo
 Logando: on (low)
 Predefinido: deny (entrada), allow (saída), disabled (roteado)
 Novos perfis: skip

Assim ninguém tem acesso a este servidor através da rede, nem pela web (porta 80), nem via ssh, nem ao banco de dados. Somente eu poderia acessar se fosse diretamente/fisicamente frente a ele ou então através do console, no caso do DigitalOcean.

Então precisamos abrir inicialmente a porta 22 para garantir o acesso. Depois trocaremos esta porta para que fique mais trabalhoso o acesso.

Como liberar uma portas ou serviços?

```
sudo ufw allow ssh
ou
sudo ufw allow 22
```

Vejamos:

```
sudo ufw status verbose:
nomeuser@ribaln ~ $ sudo ufw status verbose
Para          Ação      De
----          -
22            ALLOW IN  Anywhere
22 (v6)       ALLOW IN  Anywhere (v6)
Ele liberou a porta 22.
```

E se quisermos bloquear a porta 22?

```
sudo ufw deny 22
```

E se quiser remover esta regra deny que sempre aparece no status:

```
sudo ufw delete deny 22
```

Habilitando logs

```
ufw logging on
```

Agora eu quero que somente certo IP possa se conectar ao meu servidor

```
sudo ufw allow from 207.46.232.182
```

Agora que somente uma certa rede possa se conectar:

```
sudo ufw allow from 192.168.1.0/24
```

Agora que seja aberta a todos mas que via ssh somente para certo IP:

```
ufw allow from 192.168.0.4 to any port 22
```

Esta regra é indicada para maior segurança. Mesmo que use um desktop com internet ADSL, que muda o IP, mesmo assim. Quando seu IP mudar e você perder o acesso vá

até o console da hospedagem e atualiza seu IP. Melhor ter um pouco mais de trabalho e manter seu servidor no ar.

Não devo ter uma regra permitindo que todos acessem a porta 22
E em seguida uma dizendo que somente um IP pode acessar a porta 22
Não vai funcionar pois a primeira regra está liberando todos.
Negar acesso a certo IP
sudo ufw deny from <ip address>

Exemplificando um servidor LAMP na sua DMZ:
ufw allow proto tcp from 192.168.5.0/24 to 192.168.100.2 port 22
ufw allow proto tcp from any to any port 80
ufw enable

Onde:

192.168.5.0/24 é sua rede interna.

192.168.100.2 é o IP interno do seu LAMP server

Ou um servidor de DNS apenas com ip válido:

```
# ufw allow proto tcp from 200.200.200.201 to 200.200.200.10 port 22
# ufw allow proto udp from any to 200.200.200.10 port 53
# ufw allow proto tcp from 200.1.1.200 to 200.200.200.10 port 53
# ufw enable
```

Onde:

200.200.200.201 é o IP nateado da sua rede
200.200.200.10 é o IP do seu servidor de DNS
200.1.1.200 é o seu DNS Slave

6.8 – Logs

```
tail -f /var/log/secure
```

```
tail -f /var/log/messages
```

Monitorar quem está tentando acessar o servidor em tempo real
tcpdump -n -e -ttt -i pflog0

```
grep CRON /var/log/syslog
```

```
service rsyslog restart
```

```
grep -i cron /var/log/syslog|tail -2
```

Ver em tempo real

```
tail -fn 50 /var/log/apache2/error.log
```

6.9 – Apache

Restringir informações mostradas do Apache

Lembrar de ativar o módulo headers e depois reiniciar o apache
a2enmod headers

```
nano /etc/apache2/conf-available/security.conf
```

Mude desta forma alguns parâmetros:

```
ServerTokens Prod  
ServerSignature Off  
Header unset ETag  
Header always unset X-Powered-By  
FileETag None
```

Reiniciar o apache
sudo service apache2 restart

<https://www.tecmint.com/apache-security-tips/>

13 dicas de segurança e reforço do servidor web Apache

Ocultar a a versão do Apache e do sistema operacional nos erros

```
nano /etc/httpd/conf/httpd.conf (RHEL/CentOS/Fedora)  
nano /etc/apache2/apache2.conf (Debian/Ubuntu)
```

Segurança no Apache/Nginx

```
Header unset Server  
ServerSignature Off  
ServerTokens Prod  
TraceEnable Off  
Options all -Indexes  
Header always unset X-Powered-By
```

```
service httpd restart (RHEL/CentOS/Fedora)  
service apache2 restart (Debian/Ubuntu)
```

Desabilitar listagem de diretórios

```
nano httpd.conf ou apache2.conf
```

```
<Directory /var/www/html>  
Options -Indexes  
</Directory>
```

Mantenha o Apache atualizado

```
yum update httpd  
apt-get install apache2
```

Desabilitar módulos desnecessários

```
# grep LoadModule /etc/httpd/conf/httpd.conf  
# have to place corresponding `LoadModule' lines at this location so the  
# LoadModule foo_module modules/mod_foo.so  
LoadModule auth_basic_module modules/mod_auth_basic.so  
LoadModule auth_digest_module modules/mod_auth_digest.so  
LoadModule authn_file_module modules/mod_authn_file.so  
LoadModule authn_alias_module modules/mod_authn_alias.so  
LoadModule authn_anon_module modules/mod_authn_anon.so  
LoadModule authn_dbm_module modules/mod_authn_dbm.so  
LoadModule authn_default_module modules/mod_authn_default.so  
LoadModule authz_host_module modules/mod_authz_host.so  
LoadModule authz_user_module modules/mod_authz_user.so  
LoadModule authz_owner_module modules/mod_authz_owner.so  
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so  
LoadModule authz_dbm_module modules/mod_authz_dbm.so  
LoadModule authz_default_module modules/mod_authz_default.so  
LoadModule ldap_module modules/mod_ldap.so  
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so  
LoadModule include_module modules/mod_include.so  
LoadModule log_config_module modules/mod_log_config.so  
LoadModule logio_module modules/mod_logio.so  
LoadModule env_module modules/mod_env.so  
LoadModule ext_filter_module modules/mod_ext_filter.so
```

```
ls /etc/apache2/mods-available/
```

Rodar o Apache com um usuário e grupo diferentes

```
groupadd http-web  
useradd -d /var/www/ -g http-web -s /bin/nologin http-web
```

Usar allow e deny para controlar o acesso do document_root

```
<Directory />  
Options None  
Order deny,allow  
Deny from all  
</Directory>
```

1. Options None – Esta opção impede que usuários habilitem qualquer característica
2. Order deny, allow – Esta é a ordem em que as diretivas "Negar" e "Permitir" serão processadas. Aqui, "negará" primeiro e "permitirá" depois.
3. Deny from all – Isto deve negar pedidos de qualquer usuário para acessar o diretório raiz, ninguém poderá acessar este diretório.

Usar os módulos security e evasive para reforçar a segurança do apache

Desabilitar para que Apache não siga links simbólicos

Options -FollowSymLinks

Caso algum user ou aplicativo precise de link simbólico adicione para ele um .htaccess:

```
# Enable symbolic links  
Options +FollowSymLinks
```

Desligue includes server side e Execução de CGI

```
Options -Includes  
Options -ExecCGI
```

Para fazer isso apenas para certp diretório

```
<Directory "/var/www/html/web1">  
Options -Includes -ExecCGI  
</Directory>
```

Limite o tamanho do request

LimitRequestBody

De 0 a 2147483647 (2GB)

Para mudar em um diretório uploads

```
<Directory "/var/www/html/uploads">
LimitRequestBody 512000
</Directory>
```

Habilitar os logs do Apache

```
<VirtualHost *:80>
DocumentRoot /var/www/html/example.com/
ServerName www.example.com
DirectoryIndex index.htm index.html index.php
ServerAlias example.com
ErrorDocument 404 /story.php
ErrorLog /var/log/httpd/example.com_error_log
CustomLog /var/log/httpd/example.com_access_log combined
</VirtualHost>
```

Melhorar a segurança do Apache com SSL

Configurando o .htaccess

Referências

<https://httpd.apache.org/docs/current/pt-br/howto/htaccess.html>
<https://my.justhost.com/cgi/help/htaccess>
<http://www.devin.com.br/htaccess/>

No geral, você nunca deve usar arquivos .htaccess a não ser que você não tenha acesso ao arquivo de configuração principal do Apache.

Arquivos .htaccess devem ser usados em casos onde os provedores de conteúdo do site precisem fazer mudanças na configuração do servidor por-diretório, mas não tem acesso root ao sistema do servidor. Caso o administrador do servidor não esteja disposto a fazer mudanças freqüentes nas configurações do servidor, é desejável permitir que os usuários possam fazer essas mudanças através de arquivos .htaccess eles mesmos. Isso é particularmente verdade, por exemplo, em casos onde provedores estão fornecendo múltiplos sites para usuários em apenas uma máquina, e querem que seus usuários possam alterar suas configurações.

É o caso dos servidores de hospedagem compartilhada.

No entanto, de modo geral, o uso de arquivos .htaccess deve ser evitado quando possível. Quaisquer configurações que você considerar acrescentar em um arquivo .htaccess, podem ser efetivamente colocadas em uma seção <Directory> no arquivo principal de configuração de seu servidor.

Existem duas razões principais para evitar o uso de arquivos .htaccess.

A primeira delas é a performance. Quando AllowOverride é configurado para permitir o uso de arquivos .htaccess, o Apache procura em todos diretórios por arquivos .htaccess.

A segunda consideração é relativa à segurança. Você está permitindo que os usuários modifiquem as configurações do servidor, o que pode resultar em mudanças que podem fugir ao seu controle. Considere com cuidado se você quer ou não dar aos seus usuários esses privilégios. Note também que dar aos usuários menos privilégios que eles precisam, acarreta em pedidos de suporte técnico adicionais.

O uso de arquivos .htaccess pode ser totalmente desabilitado, ajustando a diretriz AllowOverride na seção <Directory> para none:
AllowOverride None

Para habilitar:
AllowOverride All

Definir os arquivos de índice

```
.htaccess
```

```
DirectoryIndex index.php index.html
```

Criando páginas de erro customizadas:

```
ErrorDocument 404 /404.html
```

Páginas de erro:

```
401 - Authorization Required
```

```
400 - Bad request
```

```
403 - Forbidden
```

```
500 - Internal Server Error
```

```
404 - Wrong page
```

Permitir que arquivos de diretório sejam listados:

```
Options All +Indexes
```

Impedir a listagem de diretório:

```
Options ExecCGI Includes IncludesNOEXEC SymLinksIfOwnerMatch -Indexes
```

ou

```
## No directory listings
```

```
<IfModule autoindex>
```

```
IndexIgnore *
```

```
</IfModule>
```

Bloquear certos IPs:

```
order allow,deny
```

```
deny from 123.123.123.123 #specify a specific address
```

```
deny from 123.123.123.123/30 #specify a subnet range
```

```
deny from 123.123.* #specify an IP address wildcard
```

allow from all

Permitir certos IPs:

```
order deny,allow
allow from 123.123.123.123 #specify a specific address
allow from 123.123.123.123/30 #specify a subnet range
allow from 123.123.* #specify an IP address wildcard
deny from all
```

Redirecionar de um arquivo para outro:

```
Redirect /redirect_from.html http://www.newsite.com/folder/redirect_to.html
```

Redirecionar de uma pasta para outra:

```
Redirect /redirect_from http://www.newsite.com/redirect_to
```

Deixa a Intranet acessar

```
Order allow,deny
allow from 192.168.0.
deny from all
```

Deixa todo mundo acessar, menos o IP 192.168.0.25

```
Order deny,allow
deny from 192.168.0.25
allow from all
```

```
ErrorDocument 401 /erros/falhaautorizacao.html
ErrorDocument 404 /erros/naoencontrado.html
ErrorDocument 403 /erros/acessonegado.html
ErrorDocument 500 /erros/errointerno.html
```

Redirecionar páginas de erro 404 para a index do site:

Supondo que o site está na pasta /joomla

1) Criar no raiz a pasta

erros

2) Dentro da pasta criar o arquivo 404.php contendo:

```
<?php
header('location: /joomla/index.php');
```

3) Criar o arquivo .htaccess na pasta do site contendo:

```
ErrorDocument 404 /erros/404.php
```

6.10 – PHP

Reforçando a Segurança do PHP

Filtrando dados com PHP

<https://phpro.org/tutorials/Filtering-Data-with-PHP.html>

Segurança no PHP

<https://www.phpro.org/tutorials/PHP-Security.html>

Top 7 PHP Security Blunders

<https://www.sitepoint.com/php-security-blunders/>

<http://www.phpfreaks.com/tutorial/php-security>

<http://phpsecurity.org/>

https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet

<http://phpsec.org/projects/phpsecinfo/index.html>

php.ini

```
display_errors = Off
expose_php = Off
date.timezone = America/Fortaleza
disable_functions = proc_open, popen, disk_free_space, set_time_limit, leak, tempfile,
exec,system, shell_exec, passthru, curl_exec, curl_multi_exec, parse_ini_file,
show_source, apache_get_modules,apache_get_version,apache_getenv,apache_note,
apache_setenv, disk_free_space, diskfreespace, dl, highlight_file, ini_alter, ini_restore,
openlog, proc_nice, symlink, phpinfo
```

Uma boa forma de melhorar a segurança do php é instalando o phpsecinfo:

<https://github.com/funkatron/phpsecinfo>

<http://phpsec.org/projects/phpsecinfo/>

E corrigir os erros apontados com as respectivas recomendações.

Algumas sugestões para reforçar a segurança do PHP:

edite o php.ini e faça as alterações:

```
nano /etc/php/7.0/apache2/php.ini
```

ALERTA – ao efetuar as alterações abaixo faça uma a uma, sempre reiniciando o apache e abrindo o site e efetuando um refresh para testar. Caso tenha problema desfaça ou ajuste o parâmetro com problema.

```

disable_functions = exec,system,shell_exec,passthru,
html_errors = Off
mail.add_x_header = Off
session.name = NEWSID

```

Na linha com `disable_functions` já existem várias funções por padrão que são desabilitadas. Não as remova, apenas adicione as recomendações acima ao início, separadas por vírgula.

Com a ajuda do PHPsecinfo também ajustei estes abaixo:

```

allow_url_fopen = Off
upload_tmp_dir = /var/www/html/phpup

```

Criei o diretório `/var/www/html/phpup`

Estes dois últimos parâmetros devem ser adotados com cuidado, de acordo com a sua necessidade. Abaixo são os valores default na versão 7 do php:

```

post_max_size = 8M
upload_max_filesize = 2M

```

```
sudo service apache2 restart
```

Depois dos ajustes acima alguma coisa pode não funcionar. Então efetue os ajustes devidos, sem exagerar.

Segurança e phpini

Adicionar diretamente ao `php.ini`, para o caso de se ter acesso ao `php.ini` no servidor.

```

session.save_path = "/var/www/html/tmp"
cgi.force_redirect = 1
allow_url_fopen= 0
display_errors = 0
expose_php = 0
magic_quotes_gpc = 0
memory_limit = 8388608
#open_basedir = 1
post_max_size = 262144
upload_max_filesize = 262144
upload_tmp_dir = "/var/www/html/tmp"
disable_functions = proc_open, popen, disk_free_space, set_time_limit, leak, tempfile,
exec, system, shell_exec, passthru, curl_exec, curl_multi_exec, parse_ini_file,
show_source, apache_get_modules, apache_get_version, apache_getenv, apache_note,
apache_setenv, disk_free_space, diskfreespace, dl, highlight_file, ini_alter, ini_restore,
openlog, proc_nice, symlink, phpinfo

```

Adicionar ao configuration.php, para o caso de não ter acesso direto ao php.ini

```
ini_set('session.save_path', '/var/www/html/tmp');
ini_set('cgi.force_redirect', 1);
ini_set('allow_url_fopen', 0);
ini_set('display_errors', 0);
ini_set('allow_url_include', 0);
ini_set('expose_php', 0);
ini_set('magic_quotes_gpc', 0);
ini_set('post_max_size', '262144'); // Ajustar a gosto
ini_set('upload_max_filesize', '262144'); // Ajustar a gosto
ini_set('upload_tmp_dir', '/var/www/html/tmp');
// Funções a serem desabilitadas
$disfunctions = 'proc_open, popen, disk_free_space, set_time_limit, leak, tempfile, exec,
system, shell_exec, passthru, curl_exec, curl_multi_exec, parse_ini_file, show_source,
apache_get_modules, apache_get_version, apache_getenv, apache_note,
apache_setenv, disk_free_space, diskfreespace, dl, highlight_file, ini_alter, ini_restore,
openlog, proc_nice, symlink, phpinfo';
ini_set('disable_functions', $disfunctions);
```

Verificar existência e as versões no seu servidor:

```
zend_extension=/usr/local/php52/lib/php/extensions/ioncube.so
zend_extension_manager.optimizer=/usr/local/Zend/lib/Optimizer-3.3.3
zend_extension_manager.optimizer_ts=/usr/local/Zend/lib/Optimizer_TS-3.3.3
zend_optimizer.version=3.3.3
zend_extension=/usr/local/Zend/lib/ZendExtensionManager.so
zend_extension_ts=/usr/local/Zend/lib/ZendExtensionManager_TS.so
```

Vários dos recursos acima você precisará confirmar com o suporte do seu servidor para ver se estão disponíveis.

6.11 - Melhorando a Segurança do MySQL/MariaDB

Uma forma de melhorar a segurança do mysql é criar usuários restritos, que somente tenham poder de agir num banco específico.

O exemplo abaixo é usado para criar um usuário a ser usado em site com Joomla:

```
mysql -u root -p
create database portal;
```

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senha' WITH
GRANT OPTION;
```

```
\q
```

Importar Script:

```
mysql -u root -p portal < portal.sql
```

Exportar banco para script:

```
mysqldump -u root -p portal > portal.sql
```

Também importante é executar

```
mysql_secure_installation
```

6.12 – Reforçando a Segurança do Joomla

Melhorando a segurança de sites com Joomla

Se o site está em

```
/var/www/html/portal
```

- Copiar configuration.php para o /var/www com o nome cfg.php
- Remover todo o conteúdo do /portal/configuration.php e deixar apenas estas duas linhas:

```
<?php  
require_once( dirname( __FILE__ ) . '/../..'/cfg.php' );
```

Obs.: lembre de fazer o backup do arquivo cfg.php, que agora está fora do html.

<https://geekflare.com/joomla-security/>

Não existe segurança perfeita mas quem administra um site sempre deve fazer o melhor que puder, se informando e procurando proteger da melhor forma. Sem esquecer do backup atualizado e testado.

Scannear site em busca de vulnerabilidade

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

1) Usar uma senha forte no administrator e mudar usuário de admin para outro

Acesse o site e o use para ajudar

<https://www.serveu.net/secure-password-generator.html>

2) Faça backup completo (arquivos e banco) regularmente, especialmente após qualquer alteração.

Teste também regularmente o backup feito. Guarde bem guardado.

3) Mantenha o Joomla e todas as extensões sempre atualizados

Antes de instalar qualquer extensão consulte a lista de extensões vulneráveis

https://docs.joomla.org/Archived:Vulnerable_Extensions_List

4) Monitore seu site

Veja

<https://geekflare.com/monitor-website-uptime/>

5) Habilite SEF no site

URLs amigáveis e outros

6) Evite extensões não conhecidas e remova as não usadas

7) Use extensões para melhorar a segurança

<https://geekflare.com/security-extensions-to-protect-joomla-website/>

8) Mantenha arquivos e pastas com permissões adequadas

PHP files – 644

Config Files – 644

Other folders – 755

9) Use um firewall de aplicações como o mod_security

Recomendações sobre segurança

- Usar senhas de no mínimo 6 caracteres. Quanto mais melhor, mas de 8 a 10 tá bom.
- Misturar caracteres alfabéticos maiúsculas, minúsculas, números e caracteres especiais como:
-, _, *, \$, !, %
- Não use senhas fáceis como data de nascimento, número de identidade, nomes de filhos e cônjuges.
- Procure não usar palavras do mundo real
- Pense num episódio que apenas você conhece ou lembra e forme uma frase com suas iniciais
- Crie senhas posicionais, por exemplo: primeira letra da última fila, primeira letra da primeira fila, última letra da última fila, última letra da primeira fila e assim por diante.
- Mesmo que ilógicas as senhas devem ser, para você, de fácil memorização, pois você deve evitar anotar as senhas
- Evite usar a mesma senha para todos os seus acessos
- Atualize com uma certa frequência suas senhas

Evitar o uso do ftp para transferir/baixar arquivos para/do servidor, pois ele envia seus dados (login e senha) em texto claro.

Se precisar usar o ftp use o FileZilla, que usa o sftp.

<https://filezilla-project.org/>

Instalação:

Debian e derivados

```
sudo apt-get install filezilla
```

Windows 64

<https://filezilla-project.org/download.php?platform=win64>

Ferramentas para melhorar a segurança

Usar a ferramenta joomscan

Um bom tutorial

<http://www.100security.com.br/joomscan/>

Download

<https://github.com/rezasp/joomscan>

No Linux Mint 18.1 instalar antes

```
sudo apt-get install libswitch-perl
```

- Descompactar e acessar a pasta

- Atualizar

```
./joomscan.pl update
```

Checar a atualização

```
svn co https://joomscan.svn.sourceforge.net/svnroot/joomscan joomscan
```

Varrer site procurando vulnerabilidades

```
./joomscan.pl -u http://www.joomla.org
```

Relação de extensões e ferramentas que reforçam a segurança

- joomlascan - <https://github.com/rezasp/joomscan>
- AdminTools - <https://www.akeebabackup.com/products/admin-tools.html>
- Plugin osolcapcha - <http://www.outsource-online.net/osol-captcha-for-joomla.html>
- com_encrypt - <http://www.ratmilwebsolutions.com/category/10-encryption-configuration.html>
- jHackGuard - <https://www.siteground.com/joomla-hosting/joomla-extensions/ver1.5/jhack.htm>
- jadmin_bruteforceprotection - <https://www.siteguarding.com/en/website-extensions>
- jAdminProtection - <https://www.siteguarding.com/en/website-extensions>
- jGraphicalCaptchaProtection - <https://www.siteguarding.com/en/website-extensions>
- Plugin osolcapcha - <http://www.outsource-online.net/osol-captcha-for-joomla.html>
- OSOLCaptcha - <https://github.com/osolgithub/OSOLCaptcha4Joomla3>
- SimpleBackup - https://github.com/ribafs/com_simplebackup
- AdminExile - <https://www.richeyweb.com/software/joomla/plugins/1-adminexile>

- SecurityCheck - <https://securitycheck.protegetuordenador.com/downloads/securitycheck-j3x/securitycheck-j3x-2-8-21>
- Brute Force Stop - <https://extensions.joomla.org/extensions/extension/access-a-security/site-security/brute-force-stop/>
- AskMyAdmin - <https://extensions.joomla.org/extensions/extension/access-a-security/site-security/askmyadmin/>
- <https://geekflare.com/security-extensions-to-protect-joomla-website/>
- <https://extensions.joomla.org/extensions/extension/access-a-security/site-security/centrora-security/>
- <https://www.incapsula.com/joomla-extension/joomla-plugin.html>
- <https://www.siteguarding.com/en/antivirus-website-protection-for-joomla>

Free scanner para sites online

<https://www.siteguarding.com/> - bom relatório comr ecomendações

Monitorando sites

<https://geekflare.com/monitor-website-uptime/>

Segurança na Web

Alterar permissões de arquivos:

Alterar todos os arquivos para 644 e todas as pastas para 755 com:

```
find . -type f -exec chmod 644 {} \;
find . -type d -exec chmod 755 {} \;
```

Depois criar algumas exceções...

configuration.php – 400

index.php do site – 400

index.php do template padrão – 400

Permissões de pastas:

includes e libraries – 500

Adicionar ao .htaccess:

```
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
```

```
# Block out any script trying to base64_encode crap to send via URL
```

```
RewriteCond %{QUERY_STRING} base64_encode.*\(.*\) [OR]
```

```
# Block out any script that includes a <script> tag in URL
```

```
RewriteCond %{QUERY_STRING} (\<|\%3C).*script.*(\>|\%3E) [NC,OR]
```

```
# Block out any script trying to set a PHP GLOBALS variable via URL
```

```
RewriteCond %{QUERY_STRING} GLOBALS(=|\\[|\\%[0-9A-Z]{0,2}) [OR]
```

```
# Block out any script trying to modify a _REQUEST variable via URL
```

```
RewriteCond %{QUERY_STRING} _REQUEST(=|\\[|\\%[0-9A-Z]{0,2})
```

```
# Send all blocked request to homepage with 403 Forbidden error!
```

```
RewriteRule ^(.*)$ index.php [F,L]
```

Lembre que:

O Joomla possui uma equipe que em 4 horas consegue lançar uma versão estável do produto após uma invasão.

A maioria dos ataques ocorre pelo fato dos arquivos estarem com 777 ou usuário instalou componentes "não confiáveis".

Existe o Security Strike no Joomla! que cuida somente deste assunto

https://docs.joomla.org/Security_Strike_Team

<https://developer.joomla.org/security-centre.html>

<https://volunteers.joomla.org/teams/security-strike-team>

Para verificar sites que foram hackeados/defaced:

<http://www.zone-h.org/archive?zh=1>

Componente para criptografar senhas

Dá para notar seu trabalho.

Logo após digitar a senha e teclar Enter ou clicar em Acessar observe que ele enche a caixa da senha com bolinhas, mostrando que ele está enviando algo diferente do que digitamos.

O componente com_encrypt requer o módulo bcmath do php.

Sempre que o usuário fizer login a senha será criptografada antes de ser enviada para o servidor.

Ao chegar ao servidor será descriptografada.

O mesmo autor do componente criou vários plugins para outros módulos e extensões de terceiros:

<http://www.ratmilwebsolutions.com/category/4-encryption-configuration-plugins.html>

Opcionalmente podemos gerar uma nova chave de criptografia, mas talvez não seja necessário pois uma é gerada automaticamente a cada 180 dias.

Também podemos alterar a frequência de geração de chaves e seu tamanho.

O componente criptografa a senha de login do form de login do administrador por padrão e já vem com vários outros recursos marcados por padrão:

Back-end login, Back-end edit profile, Back-end edit profile repeat password, Update RSA private KEY, Joomla off-line login, Front-end login module, Front-end login, Create account, Create account repeat password, Edit profile, Edit profile repeat password, Reset password e Reset password confirm

Download

<http://www.ratmilwebsolutions.com/category/10-encryption-configuration.html>

Ajuda

<http://www.ratmilwebsolutions.com/documentation/47-encryptioncomponenthelp.html>

Segurança no Joomla (parte 1)

Dicas de segurança no Joomla.

Muitas pessoas utilizam o CMS Joomla, no entanto a maior parte destas "esquece-se" do fator segurança nos seus sites. Existem pequenos pormenores extremamente fáceis de implementar que aumentarão consideravelmente a segurança do teu site Joomla.

Desligar os relatórios de erro

Um deles é desligar os relatórios de erros, os relatórios de erros além de diminuir a velocidade do site indicarão também ao "hackers" falhas na segurança deste. Isto pode ser desativado em 'Configuração Geral -> Sistema'.

Depois de desativada esta função não te será permitido visualizar os erros gerados pelo Joomla, o que é uma coisa boa uma vez que o utilizador comum não os vê (o que não era muito profissional) e os hackers não podem forçar erros de forma a descobrirem métodos de comprometer o sistema.

Utilizar um componente SEF

A maioria dos hackers utilizam o comando 'inurl:' do Google para procurarem por falhas em websites. Uma boa solução para contrariar este potencial risco é instalar um componente que re-escreva os Url, aconselho o SH404SEF ou o Artio-JoomSef.

O componente SEF irá trazer-lhe também bastantes vantagens a nível de SEO (rank mais elevado aos "olhos" do Google).

Mover o ficheiro configuration.php para fora da raiz.

Mova simplesmente o ficheiro de configuração para qualquer pasta que você queira dentro do site e atribua-lhe um novo nome. No exemplo utilizei 'joom.conf'.

Crie um novo ficheiro de configuração na raiz com o nome de configuration.php contendo o seguinte código:

```
<?php  
require( dirname( __FILE__ ) . '/../joom.conf' );  
?>
```

Realize backups regulares

Esta tarefa pode ser feita através do Cpanel de qualquer conta de alojamento, no entanto existem também alguns componente muito bons que realizam esta tarefa. O meu favorito é o JoomlaPack. Um backup semanal caso atualize o seu site regularmente é uma boa opção, ou então backups mensais.

Não mostrar que versões das extensões utiliza

Em primeiro lugar qualquer admin de um website deveria ter uma lista de todas as extensões que utiliza e fazer o update a estas quando sai-se uma nova versão. No entanto todos nos sabemos que o tempo não chega para tudo e muitas vezes fazer um update a uma extensão pode ser um bocado moroso. É então boa política remover a versão da extensão que utiliza a quando da instalação desta, isto pode ser feito editando os ficheiros da extensão com o notepad por exemplo.

Segunda parte

Um site em Joomla! é muito mais do que instalá-lo no servidor, mover alguns módulos de posição, instalar componentes, plugins e pronto! Já temos um site completo, feito em três dias e podemos ganhar mais de mil reais do nosso cliente.

Sinceramente, pessoal, o Joomla é tão complicado de usar quanto se programar um site do zero. Claro que você não terá mais a necessidade de digitar todas as linhas de código, mas eventuais alterações serão necessárias e é importante saber o que, onde e por que está sendo feita aquela mudança.

Além disso, a segurança é muito importante. Hoje existe uma gama enorme de componentes e módulos para Joomla, mas antes de usarem, perguntem-se: "este componente é seguro?". A maioria das invasões em sites Joomla! é feita através do próprio cms mal configurado ou de seus componentes desatualizados. Experiência própria: é muito mais difícil você contornar uma invasão do que prevenir que ela não aconteça.

Trabalho com o Joomla há mais de três anos, desde a versão 1.0.12, e desde lá já aprendi muito, tomei muito na cabeça e hoje me viro tranqüilo, tanto é que tenho mais de 20 clientes em minha região e todos utilizam o Joomla!, mas a cada nova atualização de componentes, preciso dar atenção a estes sites, pois é a segurança dos dados e informações dos mesmos que estão em jogo.

Por isso minha gente, tenho um sério conselho a dar a vocês: Estudem!

Estudem muito o Joomla, pesquisem sobre servidores web (apache), sobre dicas de segurança no PHP, informações sobre servidores de e-mail, segurança de arquivo, permissões de acesso a pastas e arquivos, etc...

Mostrei apenas o caminho das pedras, agora é Google na veia e tempo e disciplina para estudar. Hoje existem mil vezes mais materiais sobre esse assunto do que quando comecei. Inclusive a maioria mais detalhada e em português, no "meu tempo" os bons artigos e tutoriais eram em inglês.

Este e-mail foi escrito como um alerta aos desavisados, para não saírem por ai usando o Joomla! sem considerar o uso de medidas sobre segurança.

Isso evitará os seus sites de serem invadidos e assim o indivíduo não vai sair por aí xingando todo mundo em qualquer fórum destinado ao Joomla!, falando mal do sistema para qualquer um que aparecer, alegando que "não é seguro".

Quem faz o Joomla ser seguro é você".

Escrito por Roberto Jonikaites para o Yahoogrupos – Curso de Design para Joomla! De Bruno Ávila.

Este artigo foi encontrado no site abaixo, mas não mais o encontrei em minha última tentativa de visita:

http://www.joomlarj.com.br/site/index.php?option=com_content&view=article&id=26:seguranca-no-joomla-parte-2&catid=15:seguranca-no-joomla&Itemid=15

Ocultar o meta generator

Editar o index.php do template default e inserir no início

```
<?php $this->setGenerator(null); ?>
```

Checklist de Segurança para Joomla

- Se possível/viável escolher a melhor hospedagem do mercado, não a mais barata;
- Utilizar sempre a última versão do CMS e das extensões;
- Efetue um backup completo de todos os arquivos e do banco e restaure localmente
- Efetuar backup completo com frequência, especialmente antes de instalar novas extensões ou efetuar alterações como adição de conteúdo
- Ativar URLs amigáveis e mod_rewrite
- Mover configuration.php para fora do public_html, usando:
require_once(dirname(__FILE__) . '/../..../portal.cfg');
- Bloquear cadastro de usuários pelo site caso não tenha necessidade: Configuração Global - Sistema - Permitir Cadastro de Usuários - Não
- Alterar metatags em Configuração Global - Configurações de Meta Dados (Trocar Joomla por outra palavra)
- Adicionar para a tag <head> do template (para ocultar Joomla na origem do código HTML), no início do index.php:
<?php \$this->setGenerator('Ribafs - Desenvolvimento Web'); ?>
ou
<?php \$this->setGenerator(""); ?>

- Faça sempre o download do Joomla do site oficial - <http://joomla.org>
 - Cheque o hash MD5 do arquivo baixado:
md5sum Joomla_3.7.5-Stable-Full_Package.zip
bd67cb02627e60bfffef5e3b4ba3b2ece Joomla_3.7.5-Stable-Full_Package.zip
 - Algumas extensões úteis:
Firebug/Inspetor
 - Instalar os principais navegadores para testar o site:
Firefox, Chrome, Internet Explorer, Opera, Safari
 - Mantenha os arquivos de configuração, logs e os diretórios de upload (repositórios de documentos, imagens e cache) fora do public_html.
 - Remover desnecessários:
Arquivos
- Extensões (se não precisa remova e não simplesmente desabilite. Quando precisar instale)
- Sempre antes de instalar novas extensões:
 - faça um backup completo do site e instale localmente
 - Verifique se a extensão é confiável em:
https://docs.joomla.org/Archived:Vulnerable_Extensions_List
 - Faça o download do site do criador
 - Teste bastante localmente e somente então envie para o servidor
 - Evite instalar extensões que tenham código criptografado
 - Sempre que possível evite hospedar seu site em servidores compartilhados
 - Use um servidor de SSL, pelo menos para o administrador
 - Use o .htaccess
 - Atualize para a versão 3 e última do Joomla

Referências sobre Segurança

<https://docs.joomla.org/Security>
<https://extensions.joomla.org/category/access-a-security/site-security/>
https://docs.joomla.org/Security_Checklist
<https://developer.joomla.org/security.html>
<https://www.siteground.com/tutorials/joomla/joomla-security.htm>

<https://geekflare.com/joomla-security/>
<https://www.keycdn.com/blog/joomla-security/>
<https://extensions.joomla.org/extensions/extension/communication/live-support/onwebchat/>

6.13 – SELinux

SELinux

SELinux é uma poderosa ferramenta que controla que ferramentas podem fazer o que no sistema. Ele faz isso controlando processos, arquivos, diretórios, dispositivos, portas, etc, rotulando cada um.

Um exemplo: o apache recebe o rótulo `httpd_t`, que por default apenas ler os arquivos. Para poder ler e escrever em arquivos recebe o rótulo `httpd_sys_content_t` e `httpd_sys_content_rw_t`

SELinux oferece confinamento para uma aplicação se ela for hackeada ou se estiver rodando como root. O processo hackeado não poderá causar danos ao sistema mas somente agir como um processo comum do SELinux.

Inicialmente desenvolvido pela agência NSA dos EUA para proteger sistemas de computadores de maliciosas intrusões.

Um computador com o SELinux bem configurado reduz bastante os riscos de segurança.

Com SELinux você pode definir o que um usuário ou processo podem fazer. Ele confina qualquer processo para seu próprio domínio.

Lista de pacotes do SELinux:

- policycoreutils (provides utilities for managing SELinux)
- policycoreutils-python (provides utilities for managing SELinux)
- selinux-policy (provides SELinux reference policy)
- selinux-policy-targeted (provides SELinux targeted policy)
- libselinux-utils (provides some tools for managing SELinux)
- setroubleshoot-server (provides tools for deciphering audit log messages)
- setools (provides tools for audit log monitoring, querying policy, and file context management)
- setools-console (provides tools for audit log monitoring, querying policy, and file context management)
- mcstrans (tools to translate different levels to easy-to-understand format)

Mudando a porta padrão do apache para 88
`semanage port -a -t http_port_t -p tcp 88`

Pesquisando pacotes selinux instalados:

```
rpm -qa | grep selinux
```

Após a listagem dos que estão instalados instalar os demais:

```
yum install -y polycoreutils polycoreutils-python selinux-policy selinux-policy-targeted  
libselinux-utils setroubleshoot-server setools setools-console mcstrans
```

Estando desinstalado após instalar estes pacotes acima e reiniciar ele inicia enforcing.

```
getsebool -a | less  
getsebool -a | grep off  
getsebool -a | grep on
```

```
semanage login -l | grep ribafs
```

```
semanage user -l | grep staff_u
```

```
newrole -r sysadm_r
```

```
semanage login -a -s staff_u -r s0 ribafs
```

Por default SELinux permite o ssh somente na porta 22. Vamos mudar:

```
semanage port -a -t ssh_port_t -p tcp 65522
```

Deletar uma porta

```
semanage port --delete -t http_port_t -p tcp 8899-8902
```

ou

```
semanage port -d -t http_port_t -p tcp 22
```

Checar

```
semanage port -l | grep ssh
```

```
systemctl restart sshd.service
```

Permitir a porta nova no firewalld

```
firewall-cmd --permanent --zone=public --add-port=65522/tcp
```

```
firewall-cmd --reload
```

Checar se escuta a porta do ssh

```
ss -tnlp|grep ssh
```

```
ssh -p 65522 ribafs@ip
```

O SELinux pode ser configurado de 3 modos:

- Enforcing
- Permissive

- Disabled

Enforcing

No enforcing modo ele força sua política no sistema linux e garante que qualquer tentativa de acesso não autorizado por usuários ou processos seja negada.

Permissive

É um modo semi-habilitado. Não aplica sua política, de forma que nenhum acesso será negado mas mesmo assim tudo é registrado nos logs.

Esta é uma forma de testar o SELinux antes de mudar para enforcing.

Checar o modo atual do SELinux:

```
getenforce
```

Disabled

Estado em que o SELinux está desabilitado.

Verificar o estado do SELinux

```
sestatus
```

Para habilitar o SELinux edite o script

```
nano /etc/selinux/config
```

E mude o estado para o desejado.

```
SELINUX=enforcing
```

Basta mudar a linha

```
SELINUX=enforcing
```

Para um dos 3 estados:

```
# enforcing - SELinux security policy is enforced.
```

```
# permissive - SELinux prints warnings instead of enforcing.
```

```
# disabled - No SELinux policy is loaded.
```

Após alterar reinicie o sistema:

```
reboot
```

ou em

```
/etc/sysconfig/selinux
```

Monitorando os logs

```
cat /var/log/messages | grep "SELinux"
```

Usuários

O SELinux traz um conjunto de usuários. Toda conta de usuário do Linux é mapeada para uma conta de usuário ou mais no SELinux.

Sujeito

Em termos de SELinux um processo é chamado de sujeito.

Regras/Roles

Uma role é como um gateway que se situa entre um usuário e um processo. Uma role define que usuário pode acessar que processo. Roles não são como grupos mas como filtros. Que usuários têm acesso para qual role.

Um sujeito é um processo e pode potencialmente afetar um objeto.

Um objeto em SELinux é qualquer coisa que pode continuar. Pode ser um arquivo, um diretório, uma porta, um socket tcp, o cursor ou até o servidor X. As ações que um sujeito pode executar em um objeto são as permissões do sujeito.

Domínios são para Sujeitos

Um domínio é o contexto em que um sujeito (processo) SELinux pode rodar. Ele diz ao processo o que ele pode e o que não pode fazer. O domínio deve definir que arquivos, diretórios, links, dispositivos ou portas são acessíveis para o sujeito.

Tipos são para Objetos

Um tipo é o contexto para o contexto de um arquivo que estipula os usos do arquivo. Um contexto de um arquivo é chamado de tipo na linguagem do SELinux.

Política do SELinux

Define acesso de usuários para roles, acesso de roles para domínios e acesso de domínios para tipos.

Primeiro o usuário tem que ser autorizado para entrar numa role e então a role tem que ser autorizada para acessar o domínio. O domínio então é restringido para acessar somente certos tipos de arquivos.

A política em si é um conjunto de regras/roles que diz tal e qual usuário pode assumir tal e qual regras/role e estas roles/regras devem ser autorizadas para acessar somente tais e quais domínios.

Um processo rodando com um domínio particular pode executar somente certas operações em certos tipos de objetos é chamado Type Enforcement (TE).

Por default SELinux deve restringir somente certos processos no sistema que não são destinados a rodar em domínios não confinados.

Listar módulos carregados na memória
semodule -l | less

Diretório onde os módulos são gravados:
ls -l /etc/selinux/targeted/modules/active/modules/

Políticas

ls -l /etc/selinux/targeted/policy/

Listando módulos de forma booleana:

semanage boolean -l | less

Vendo estado de um módulo
getsebool ftpd_anon_write

Mudando o estado de off para on
setsebool ftpd_anon_write on

Para off
setsebool ftpd_anon_write off

Ver mapas de usuários
semanage login -l

Mostrar contextos
id -Z

Adicionar usuário ao SELinux
semanage login -a -s s_user_u nomeuser

Comandos para resolver problemas

chcon R t httpd_sys_content_t /var/www/html

semanage fcontext a t httpd_sys_content_t '/var/www/html(/.*)?

restorecon R /var/www/html

matchpathcon /var/www/html

tail -f /var/log/audit/audit.log

Instalar
yum install setroubleshoot setools

Usar a ferramenta sealerts
sealert -a /var/log/audit/audit.log

Configuração do SELinux para LAMP com WordPress no CentOS 7

Antes de habilitar o SELinux instalar os pacotes e o LAMP e o Wordpress devem ser configurados.

SELinux somente deve ser configurado após tudo isso, ao final.

- Criar o servidor
- Configurar o acesso via SSH
- Atualizar os pacotes e reiniciar

```
yum check-update  
yum update -y
```

Criar pasta para backup

```
mkdir /root/back
```

Desabilitar o SELinux

```
cp /etc/selinux/config /root/back/se_configORIG  
Mudar para Disabled  
reboot
```

Criar um usuário

```
useradd ribafs  
passwd ribafs
```

Adicionar este usuário ao sudo

```
cp /etc/sudoers /root/back/sudoersORIG  
nano /etc/sudoers
```

```
ribafs ALL=(ALL) NOPASSWD:ALL
```

Configurar o SSH e remover o acesso do root

```
cp /etc/ssh/sshd_config /root/back/sshd_configORIG
```

```
su - ribafs  
mkdir .ssh  
chmod 700 .ssh  
cd .ssh  
ssh-keygen -b 1024 -f id_ribafs -t dsa (Enter 2 vezes)  
cat ../ssh/id_ribafs*.pub > ../ssh/authorized_keys  
chmod 600 ../ssh/*  
exit
```

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

```
Port 65522  
logingrace 30  
permitirrootlogin no  
MaxAuthTries 3  
AllowUsers ribafs
```

```
service sshd restart
```

```
exit
```

Copiar a chave do SSH do desktop para o servidor
Caso ainda não tenha gerado a chave execute:
ssh-keygen -t rsa -b 4096

Apenas tecle Enter duas vezes.

Copiar a chave para o servidor:
ssh-copy-id ribafs@IP -p 65522

Na primeira vez ele pede sua senha do servidor, mas das próximas vezes não pedirá.

```
ssh -p 65522 ribafs@IP
```

Conecta sem pedir senha.

Para ogar com privilégios de root, se necessário, use:
sudo -i

Desabilitar autenticação de senha (recomendado)

```
sudo -i
```

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

```
PasswordAuthentication no
```

Instalação dos pacotes do LAMP

Parar, desabilitar e desinstalar o firewall:

```
service stop firewalld  
systemctl disable firewalld.service  
yum remove firewalld
```

Instalação de alguns pacotes básicos:

```
yum install -y wget mc unzip net-tools iptable-services yum-cron sshfs epel-release
```

```
yum install -y httpd mariadb-server mariadb openssl mod_ssl
```

```
wget https://rpms.remirepo.net/enterprise/remi-release-7.rpm  
rpm -Uvh remi-release-7.rpm
```

Configurar o repositório

```
cp /etc/yum.repos.d/remi.repo /root/back/remi.repoORIG  
nano /etc/yum.repos.d/remi.repo
```

Setar a primeira entrada para enable=1

```
[remi]
name=Remi's RPM repository for Enterprise Linux 7 - $basearch
#baseurl=http://rpms.remirepo.net/enterprise/7/remi/$basearch/
#mirrorlist=https://rpms.remirepo.net/enterprise/7/remi/httpsmirror
mirrorlist=http://rpms.remirepo.net/enterprise/7/remi/mirror
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
```

Instalando PHP 7.1

```
cp /etc/yum.repos.d/remi-php71.repo /root/back/remi-php71.repoORIG
```

```
nano /etc/yum.repos.d/remi-php71.repo
```

```
[remi-php71]
name=Remi's PHP 7.1 RPM repository for Enterprise Linux 7 - $basearch
#baseurl=http://rpms.remirepo.net/enterprise/7/php71/$basearch/
#mirrorlist=https://rpms.remirepo.net/enterprise/7/php71/httpsmirror
mirrorlist=http://rpms.remirepo.net/enterprise/7/php71/mirror
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
```

Instalar

```
yum install php php-pecl-ssh2 gcc php-devel php-pear php php-gd php-mysql php-mcrypt
php-mbstring
```

```
yum update -y
```

```
php -v
```

Configurações

```
systemctl enable yum-cron
systemctl enable iptables
systemctl start iptables
```

```
nano /etc/yum/yum-cron.conf
```

```
update_cmd = security
apply_updates = yes
```

```
systemctl start yum-cron
```

Lista de pacotes instalados
/var/log/yum.log

Configurar o IPTables

```
iptables -L > /root/back/iptablesORIG
```

```
iptables -F
```

```
# Drop NULL packets
```

```
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

```
# Block syn flood attack
```

```
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

```
# Block XMAS packets
```

```
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
```

```
# SSH Rate limit new connections (drop if more than 3 attempts in 60 seconds) and allow only established SSH connections
```

```
iptables -A INPUT -i eth0 -p tcp --dport 65522 -m state --state NEW -m recent --set --name SSH
```

```
iptables -A INPUT -i eth0 -p tcp --dport 65522 -m state --state NEW -m recent --update --seconds 300 --hitcount 4 --rttl --name SSH -j DROP
```

```
iptables -A INPUT -i eth0 -p tcp --dport 65522 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 65522 -m state --state ESTABLISHED -j ACCEPT
```

```
# Web Server (HTTP/HTTPS)
```

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

```
# Web Browsing
```

```
iptables -A INPUT -i eth0 -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -i eth0 -p tcp --sport 443 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
# Allow Inbound/Outbound to Localhost
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -o lo -j ACCEPT
```

```
#Allow SMTP outbound (E.g Sendmail)
```

```
iptables -A INPUT -i eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# Log all dropped packets
```

```
iptables -N LOGINPUT
```

```
iptables -N LOGOUTPUT
```

```
iptables -A INPUT -j LOGINPUT
```

```
iptables -A OUTPUT -j LOGOUTPUT
```

```
iptables -A LOGINPUT -m limit --limit 4/min -j LOG --log-prefix "DROP INPUT: " --log-level 4
```

```
iptables -A LOGOUTPUT -m limit --limit 4/min -j LOG --log-prefix "DROP OUTPUT: " --log-level 4
```

```
# Set policies to drop everything else
```

```
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -P OUTPUT DROP
```

Save and then restart:

```
iptables-save > /etc/sysconfig/iptables
```

```
systemctl restart iptables
```

Instalando fail2ban

```
yum install -y fail2ban
```

```
systemctl enable fail2ban
```

Criar uma configuração básica

```
cp /etc/fail2ban/jail.local /root/back/jail.localORIG
```

```
nano /etc/fail2ban/jail.local
```

Alterar

```
[DEFAULT]
```

```
# Set a 1 hour ban
```

```
bantime = 3600
```

```
# Override /etc/fail2ban/jail.d/00-firewalld.conf:
```

```
banaction = iptables-multiport
```

```
[sshd]
```

```
enabled = true
```

```
== MARIADB
```

```
systemctl enable mariadb
```

```
systemctl start mariadb
```

mysql_secure_installation

Conectar com
mysql -u root -p

Protegendo administrator com senha

Usando .htaccess

nano /portal/administrator/.htaccess

```
<Files wp-login.php>  
  order deny,allow  
  Deny from all  
  Allow from X.X.X.X  
</Files>
```

X.X.X.X - seu IP

Testar:

http://dominio/portal/
http://dominio/portal/administrator

Habilitar e configurar o SELinux

```
yum install -y policycoreutils policycoreutils-python selinux-policy selinux-policy-targeted  
libselinux-utils setroubleshoot-server setools setools-console mcstrans
```

Mudar para modo Permissive como primeiro passo

nano /etc/sysconfig/selinux

SELINUX=permissive

reboot

Consultar estado do SELinux:

sestatus

Configurado como permissive ele não nega nenhum acesso mas monitora via logs

Contexto e Rótulo do SELinux

Listar todos os tipos de contextos
seinfo -t

```
seinfo -t | grep httpd_sys
```

Mostra todos os contextos iniciados com httpd_sys

Label/Rótulo incorreto gera o erro:

Forbidden

You don't have permission to access / on this server.

Listar labels do /var/www

```
cd /var/www
```

```
ls -aZ
```

Labels usam o seguinte formato:

```
user:role:type:level
```

Listar todos

```
getsebool -a
```

Comando para mudar o estado

```
setsebool -P
```

```
semanage boolean -l | grep httpd
```

```
restorecon -Rv /var/www/html/portal
```

Permitir SSH em porta diferente da default

```
semanage port -a -t ssh_port_t -p tcp 65522
```

Permitir apache ler e escrever no /var/www

```
setsebool -P httpd_unified 1
```

Quando encontrar algum problema sem solução no SELinux faça o seguinte:

- Limpe o audit.log com:

```
> /var/log/audit/audit.log
```

```
reboot
```

Use o comando sealert

```
sealert -a /var/log/audit/audit.log
```

Sumário do audit.log:

```
aureport -a -ts today
```

Reforçar o SELinux

```
nano /etc/sysconfig/selinux
```

```
SELINUX=enforced  
reboot
```

Após o boot, acesse por ssh faça login e teste o sistema. Teste também o acesso ao site.

Ver este

<http://www.drupalwatchdog.com/volume-2/issue-2/using-apache-and-selinux-together>

Para permitir o httpd

```
semanage permissive -a httpd_t
```

Configurando o SELinux

Mantenha por enquanto ele desabilitado ou em permissive mode.

```
yum update -y
```

```
yum install -y polycoreutils polycoreutils-python selinux-policy selinux-policy-targeted  
libselinux-utils setroubleshoot-server setools setools-console mcstrans
```

Altere o SELinux para permissive mode e reinicie o servidor.

```
nano /etc/selinux/config
```

```
SELINUX=permissive
```

ou assim:

```
setenforce 0
```

```
reboot
```

Configurar corretamente o contexto para o diretório web

```
semanage fcontext -a -t httpd_sys_content_t "/var/www/html(/.*)?"  
restorecon -Rv /var/www/html
```

Permitir ssh em outra porta

```
semanage port -a -t ssh_port_t -p tcp 9922
```

Permitir que apache envie e-mail

```
setsebool -P httpd_can_sendmail 1
```

Permitir que apache leia e escreva em certo diretório

```
setsebool -P httpd_unified 1
```

Monitorar problemas

```
sestatus
```

Limpar logs e reinicie

```
> /var/log/audit/audit.log
```

```
reboot
```

Checar por problemas

```
sealert -a /var/log/audit/audit.log
```

Permitir que apache conecte via ssh

```
setsebool httpd_can_network_connect=1
```

Mudar para enforcing e reiniciar

```
nano /etc/sysconfig/selinux
```

```
SELINUX=enforced
```

```
reboot
```

<https://hostpresto.com/community/tutorials/install-and-secure-nginx-on-centos-7/>

Nginx é um software servidor web de alta performance. A versão em produção saiu em 2004.

Alguns dos recursos que oferece:

- Balanceamento de carga
- Pode manipular mais que 10.000 conexões simultâneas com pouca memória
- Suporte a SSL/OpenSSL
- Suporte a compressão/descompressão gzip
- Suporte a autenticação de acesso a páginas/proteção de diretório com senha

Criar diretório de backup

```
mkdir /root/back
```

Garantir que SELinux esteja desabilitado

```
cp /etc/selinux/config /root/back
```

```
nano /etc/selinux/config
```

Atualização

```
sudo yum update -y
```

```
reboot
```

Atualizar repositórios
sudo yum install epel-release

Instalar Nginx
sudo yum install nginx
sudo systemctl start nginx
sudo systemctl enable nginx

Segurança

Liberar porta 80
sudo firewall-cmd --permanent --add-port=80/tcp sudo firewall-cmd --permanent --add-port=443/tcp
sudo firewall-cmd --reload

Atualizar centos
sudo yum update -y

Ocultar cabeçalho do nginx

```
cp /etc/nginx/nginx.conf /root/back
```

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

```
http {  
    server_tokens off;  
}
```

Testando:

```
curl -I http://localhost
```

Desabilitar métodos não desejados

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

```
if ($request_method !~ ^(GET|HEAD|POST)$ )  
{  
    return 405;  
}
```

```
sudo systemctl restart nginx
```

```
telnet localhost 80
```

Mostrará que o 405 não é permitido

Combater ataques Clickjacking

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

Adicionar a seguinte linha ao bloco server:

```
add_header X-Frame-Options "SAMEORIGIN";
```

```
sudo systemctl restart nginx
```

Configurar autenticação

```
sudo yum install -y httpd-tools
```

Criar usuário ribafs e conceder senha para ele

```
sudo htpasswd -c /etc/nginx/.htpasswd ribafs
```

Visualizar

```
sudo cat /etc/nginx/.htpasswd
```

Para adicionar a autenticação ao diretório web, adicione auth_basic

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

```
...
server {
    listen    80 default_server;
    listen   [::]:80 default_server;
    server_name _;
    root     /usr/share/nginx/html;
    auth_basic "Private Property";
    auth_basic_user_file /etc/nginx/.htpasswd;
    ...
}
```

```
sudo systemctl reload nginx
```

Configurar o SSL para o Nginx

```
sudo yum install mod_ssl
```

```
sudo mkdir /etc/nginx/ssl/
```

Criar o certificado

```
sudo openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout
/etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt
```

Pode demorar

```
sudo openssl dhparam -out /etc/nginx/ssl/dhparam.pem 4096
```

Configurar o site default para usar SSL

```
cp /etc/nginx/sites-enabled/default /root/back
```

```
sudo nano /etc/nginx/sites-enabled/default
```

```

server {
...
    server_name localhost;
    ### SSL Config
    listen 443 ssl;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/ssl/dhparam.pem;
    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;
...

```

```
sudo systemctl reload nginx
```

Restringir acesso para somente certo IP

```
sudo nano /etc/nginx/sites-enabled/default
```

```

server {
...
    location /site-admin/ {
        allow 192.168.1.1/24;
        allow 10.0.0.1/24;
        deny all;
    }
...

```

Troque os IPs acima e máscaras pelos desejados

Testando

```
http://IP
```

Agora, depois de testar o nginx devemos habilitar o SELinux com a política Enforcing.

```
nano /etc/selinux/config
```

Enforcing

reboot

Acessar novamente e testar o nginx

Auditando logs do nginx

```
grep nginx /var/log/audit/audit.log | audit2allow
```

Criar módulo de política customizada

```
grep nginx /var/log/audit/audit.log | audit2allow -m nginx > nginx.te
cat nginx.te
```

```
module nginx 1.0;
```

```
require {
    type var_run_t;
    type user_home_dir_t;
    type httpd_log_t;
    type httpd_t;
    type user_home_t;
    type httpd_sys_content_t;
    type initrc_t;
    type http_cache_port_t;
    class sock_file write;
    class unix_stream_socket connectto;
    class dir { search getattr };
    class file { read write setattr };
    class tcp_socket name_connect;
}
```

```
#===== httpd_t =====
```

```
#!!! This avc is allowed in the current policy
allow httpd_t http_cache_port_t:tcp_socket name_connect;
allow httpd_t httpd_log_t:file setattr;
allow httpd_t httpd_sys_content_t:sock_file write;
allow httpd_t initrc_t:unix_stream_socket connectto;
```

```
#!!! This avc is allowed in the current policy
allow httpd_t user_home_dir_t:dir search;
```

```
#!!! This avc is allowed in the current policy
allow httpd_t user_home_t:dir { search getattr };
allow httpd_t user_home_t:sock_file write;
allow httpd_t var_run_t:file { read write };
```

```
grep nginx /var/log/audit/audit.log | audit2allow -M nginx
semodule -i nginx.pp
```

```
semodule -l
```

Para corregir todos os erros 502 do nginx execute como root

```
yum install -y policycoreutils-{python,devel}
grep nginx /var/log/audit/audit.log | audit2allow -M nginx
semodule -i nginx.pp
usermod -a -G git nginx
chmod g+rx /home/git/
```

Intrgrar mensagens de erro do SELinux com journald
 journalctl -r -o verbose -u nginx.service

SELinux em Servidores web

O SELinux pode ser muito trabalhoso em servidores web quando não instalado no diretório padrão. Ele pode não permitir ao Apache acessar seu conteúdo ou arquivos de log.

Ao invés de desabilitar o SELinux você deve criar uma política customizada que aplique o tipo de contexto apropriado para seus diretórios e arquivos.

Por default os arquivos apenas podem ser lidos e não alterados.
 Por default os diretórios tem permissão apenas de leitura.

Estou considerando que Apache e MySQL já estão instalados e configurados

Estrutura de diretórios do documentRoot:

```
/var/www/html
  sites
    site1
    site2
    ...
```

```
site1
  /administrator
  /administrator/logs
  /tmp
  /images
  configuration.php
```

Cada site deve ficar segregado em seu diretório
 Todos os arquivos devem ser read only a não ser que explícita permissão para o contrário

Criar nossa própria política. Garantir que semanage está instalado:

- Abrir o terminal como root
- Instalar o pacote polycycoreutils-python que contém o semanage
 yum yinstall -y polycycoreutils-python
- Para ajudar a resolver problemas instalar o pacote
 yum install -y setroubleshooting

Tipos de Contextos do Apache

httpd_sys_content_t Diretórios e arquivos read-only usados pelo Apache

httpd_sys_rw_content_t Arquivos e diretórios que podem ser lidos e alterados pelo Apache.

Atribuir este para diretórios onde arquivos podem ser criados ou modificados

que o `httpd_sys_content_t` pelo site ou atribuir este para arquivos e diretórios para permitir site modifique.

`httpd_log_t` Usado pelo Apache para gerar e anexar para os arquivos de logs do site

`httpd_cache_t` Atribuir para um diretório usado pelo Apache para caching, se você estiver usando o `mod_cache`.

Para uma lista completa de contextos execute:

```
man httpd_selinux
```

Para visualizar as políticas existentes conexto

```
semanage fcontext -l
```

Criando políticas

1) Criar uma política para atribuir o contexto `httpd_sys_content_t` context para o diretório `/var/www/html`

```
semanage fcontext -a -t http_sys_content_t "/var/www/html(/.*)?"
```

2) Criar uma política para atribuir ao contexto `httpd_log_t` para o diretório de logs de cada site. Neste caso será para o `site1`

```
semanage fcontext -a -t httpd_log_t "/var/www/html/site1/administrator/logs(/.*)?"
```

3) Criar uma política para atribuir ao contexto `httpd_cache_t` para os diretórios `tmp` de cada site. Agora para o `site1`

```
semanage fcontext -a -t httpd_cache_t "/var/www/html/site1/tmp(/.*)?"
```

Permitindo acesso de leitura e escrita

O Apache agora tem permissão para acessar o diretório do `site1` mas sem acesso `read` `write` para nada.

O seguinte deve atribuir ao Apache contexto de leitura e escrita, para que possa escrever ou modificar os arquivos.

`/tmp` e `/images` - Permitir envio de imagens para o `/images` e instalação de extensões através do `/tmp`

`configuration.php` - Este arquivo é alterado sempre que se altera alguma configuração do Joomla

Criar uma política para atribuir ao contexto `httpd_sys_rw_content_t` context para os diretórios `/tmp` e `/images` recursivamente

```
semanage fcontext -a httpd_sys_rw_content_t "/var/www/html/site1/tmp(/.*)?"
```

```
semanage fcontext -a httpd_sys_rw_content_t "/var/www/html/site1/images(/.*)?"
```

Criar uma política para atribuir ao contexto `httpd_sys_rw_content_t` context para que o Joomla possa alterar o arquivo `configuration`:

```
semanage fcontext -a httpd_sys_rw_content_t "/var/www/html/site1/configuration.php"
```

Aplicando as políticas do SELinux

As políticas foram criadas e estão prontas para serem aplicadas para seus respectivos diretórios.

Nós devemos usar o comando `restorecon` para aplicar então, se por alguma razão eles forem removidos ou corrompidos.

1) Aplicar as políticas do SELinux

```
restorecon -Rv /var/www/html
```

2) A estrutura de diretórios deve ter o seguinte contexto

```
/var/www/html (httpd_sys_content_t)
  /sites (httpd_sys_content_t)
    /site1 (httpd_sys_content_t)
      / (httpd_sys_content_t)
      /administrator (httpd_sys_content_t)
        /logs (httpd_log_t)
      /tmp httpd_sys_rw_content_t e (httpd_cache_t)
      /images httpd_sys_rw_content_t
      /index.php (httpd_sys_content_t)
      /configuration.php httpd_sys_rw_content_t
```

3) Para verificar o tipo de contexto:

```
ls -lZ /var/www/html
```

4) A saída deve mostrar o tipo de contexto

O SELinux é uma camada crucial da segurança do servidor que nunca deve ser desabilitado. Ele oferece proteção além do que o firewall e outras ferramentas podem oferecer.

Referências

Shane Rainville em

<http://www.serverlab.ca/tutorials/linux/web-servers-linux/configuring-selinux-policies-for-apache-web-servers/>

<https://www.digitalocean.com/community/tutorials/an-introduction-to-selinux-on-centos-7-part-1-basic-concepts>

<https://www.digitalocean.com/community/tutorials/an-introduction-to-selinux-on-centos-7-part-2-files-and-processes>

<https://www.digitalocean.com/community/tutorials/an-introduction-to-selinux-on-centos-7-part-3-users>

https://fedorapeople.org/~dwalsh/SELinux/Presentations/selinux_four_things.pdf

<https://www.drupalwatchdog.com/volume-2/issue-2/using-apache-and-selinux-together>

<http://www.serverlab.ca/tutorials/linux/administration-linux/troubleshooting-selinux-centos-red-hat/>

6.14 – Rede

Reforçar a segurança da rede configurando o sysctl

Para prevenir fontes de roteamento de pacotes de entrada e logs de IPs malformados

```
nano /etc/sysctl.conf
```

Descomente

```
# IP Spoofing protection
```

```
net.ipv4.conf.all.rp_filter = 1
```

```
net.ipv4.conf.default.rp_filter = 1
```

```
# Disable source packet routing
```

```
net.ipv4.conf.all.accept_source_route = 0
```

```
net.ipv6.conf.all.accept_source_route = 0
```

```
# Block SYN attacks
```

```
net.ipv4.tcp_syncookies = 1
```

```
# Log Martians
```

```
net.ipv4.conf.all.log_martians = 1
```

Adicione ao final:

```
# Ignore send redirects
```

```
net.ipv4.conf.all.send_redirects = 0
```

```
# Ignore ICMP broadcast requests
```

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

```
# Disable source packet routing
```

```
net.ipv4.conf.default.accept_source_route = 0
```

```
net.ipv6.conf.default.accept_source_route = 0
```

```
# Ignore send redirects
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Log Martians
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1

Reiniciar com
sysctl -p
```

Netstat

```
netstat -nat | awk '{print $6}' | sort | uniq -c | sort -n

netstat -nat | grep {IP-address} | awk '{print $6}' | sort | uniq -c | sort -n

netstat -nat | grep 202.54.1.10 | awk '{print $6}' | sort | uniq -c | sort -n
```

To print list of all unique IP address connected to server, enter:

```
# netstat -nat | awk '{ print $5}' | cut -d: -f1 | sed -e '/^$/d' | uniq
```

To print total of all unique IP address, enter:

```
# netstat -nat | awk '{ print $5}' | cut -d: -f1 | sed -e '/^$/d' | uniq | wc -l
```

If you think your Linux box is under attack, print out a list of open connections on your box and sorts them by according to IP address, enter:

```
# netstat -atun | awk '{print $5}' | cut -d: -f1 | sed -e '/^$/d' | sort | uniq -c | sort -n

# netstat -s | less
# netstat -t -s | less
# netstat -u -s | less
# netstat -w -s | less
# netstat -s
```

You can easily display dropped and total transmitted packets with netstat for eth0:

```
# netstat --interfaces eth0
```

Type the following command to see IPv4 port(s), enter:

```
# lsof -Pnl +M -i4
```

Type the following command to see IPv6 listing port(s), enter:

```
# lsof -Pnl +M -i6
```

Type the command as follows:

```
# netstat -tulpn
```

OR

```
# netstat -npl
```

/etc/services file

/etc/services is a plain ASCII file providing a mapping between friendly textual names for internet services, and their underlying assigned port numbers and protocol types. Every networking program should look into this file to get the port number (and protocol) for its service. You can view this file with the help of cat or less command:

```
$ cat /etc/services
```

```
$ grep 110 /etc/services
```

```
$ less /etc/services
```

Tcpdump

```
pkg install tcpdump
```

```
mkdir ~/scan_results/syn_scan
```

We can start a tcpdump capture and write the results to a file in our ~/scan_results/syn_scan directory with the following command:

```
sudo tcpdump host target_ip_addr -w ~/scan_results/syn_scan/packets
```

Pausar com Ctrl+Z

If we want to see the actual packet traffic that was sent to and received from the target, we can read the packets file back into tcpdump, like this:

```
sudo tcpdump -nn -r ~/scan_results/syn_scan/packets | less
```

This file contains the entire conversation that took place between the two hosts. You can filter in a number of ways.

For instance, to view only the traffic sent to the target, you can type:

```
sudo tcpdump -nn -r ~/scan_results/syn_scan/packets 'dst target_ip_addr' | less
```

Likewise, to view only the response traffic, you can change the "dst" to "src":

```
sudo tcpdump -nn -r ~/scan_results/syn_scan/packets 'src target_ip_addr' | less
```

Open TCP ports would respond to these requests with a SYN packet. We can search directly for responses for this type with a filter like this:

```
sudo tcpdump -nn -r ~/scan_results/syn_scan/packets 'src target_ip_addr and tcp[tcpflags] & tcp-syn != 0' | less
```

Start a tcpdump capture again. This time, write the file to the new ~/scan_results/udp_scan directory:

```
sudo tcpdump host target_ip_addr -w ~/scan_results/udp_scan/packets
```

Pause the process and put it into the background:

```
CTRL-Z
```

```
bg
```

Be sure to write the results to the ~/scan_results/udp_scan directory. All together, the command should look like this:

```
sudo nmap -sU -Pn -p- -T4 -vv --reason -oN ~/scan_results/udp_scan/nmap.results target_ip_addr
```

We can see how nmap had to send out many packets to the ports that were reported as open|filtered by asking to see the UDP traffic to one of the reported ports:

```
sudo tcpdump -nn -Q out -r ~/scan_results/udp_scan/packets 'udp and port 22'
```

Compare this to the results we see from one of the scanned ports that was marked as "closed":

```
sudo tcpdump -nn -Q out -r ~/scan_results/udp_scan/packets 'udp and port 53'
```

We can try to manually reconstruct the process that nmap goes through by first compiling a list of all of the ports that we're sending UDP packets to using something like this:

```
sudo tcpdump -nn -Q out -r ~/scan_results/udp_scan/packets "udp" | awk '{print $5;}' | awk 'BEGIN { FS = "." } ; { print $5 +0}' | sort -u | tee outgoing
```

Then, we can see which ICMP packets we received back saying the port was unreachable:

```
sudo tcpdump -nn -Q in -r ~/scan_results/udp_scan/packets "icmp" | awk '{print $10,$11}' | grep unreachable | awk '{print $1}' | sort -u | tee response
```

We can see then take these two responses and see which UDP packets never received an ICMP response back by typing:

```
comm -3 outgoing response
```

The nmap scan we need to use is triggered by the -sV flag. Since we already did SYN and UDP scans, we can pass in the exact ports we want to look at with the -p flag. Here, we'll look at 22 and 80 (the ports that were shown in our SYN scan):

```
sudo nmap -sV -Pn -p 22,80 -vv --reason -oN ~/scan_results/versions/service_versions.nmap target_ip_addr
```

The flag we need in order to perform operating system detection is -O (the capitalized letter "O"). A full command may look something like this:

```
sudo nmap -O -Pn -vv --reason -oN ~/scan_results/versions/os_version.nmap  
target_ip_addr
```

Prevenir IP Spoofing

Edite
nano /etc/host.conf

E deixe seu conteúdo assim:

```
order bind,hosts  
multi on  
nospoof on
```

6.15 - Mantendo Servidores web e de bancos de dados seguros

<https://www.acunetix.com/websitesecurity/webserver-security/>

Os sites são muito visados pelos invasores. A segurança dos mesmos é importante. Tanto o site ou aplicativo quanto o servidor precisam estar usando as melhores práticas e ferramentas para garantir a segurança do site.

Garantir a segurança de sites e servidores é uma tarefa que requer administradores dedicados e estudiosos.

- Remova serviços desnecessários, assim como usuários e processos desnecessários.
- Não use FTP para acessar o servidor mas somente SSH ou SFTP que são seguros
- Separar ambientes de teste e de produção. De preferência o servidor de testes deve ficar sempre sem acesso à internet. Apenas instale todos os pacotes necessários e desconecte.
- Sempre conceda o mínimo de privilégios para usuários e permissões para arquivos e diretórios
- Atualizar com frequência a distribuição.
- Monitorar e auditar o servidor
- Manter somente usuários necessários, os demais remova
- Remova todos os módulos e extensões do Apache/Nginx e PHP
- Use boas ferramentas para reforçar a segurança

- Mantenha-se informado, frequentando grupos da área e visitando portais de administração de servidores
- Use scanners web online para varrer seu site regularmente

Exemplo - <https://www.acunetix.com/vulnerability-scanner/>

Veja

<https://www.acunetix.com/websitesecurity/sql-injection/>

6.16 – SSH

Reforçando a segurança do SSH

Acessar o servidor como root ou sudo su

```
adduser ribafs
adduser ribafs admin
```

Configurar sudo

```
nano /etc/sudoers
```

Adicione a linha a seguir abaixo da linha do root
nomeuser ALL=(ALL) NOPASSWD:ALL

```
su - ribafs
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_nomeuser -t dsa (Enter 2 vezes)
cat ../ssh/id_nomeuser*.pub > ../ssh/authorized_keys
chmod 600 ../ssh/*
exit
```

Configuração do SSH

Escolha uma porta acima de 50000

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

```
Port 55522
LoginGraceTime 30
PasswordAuthentication yes
# A linha abaixo deve vir assim somente se associamos uma chave ssh na criação do
servidor, caso contrário use: no
```

```
PermitRootLogin without-password
```

Adicionar ao final:

```
AllowUsers nomeuser root
```

```
service ssh restart
```

Gerar chaves do SSH no desktop para enviar para o Servidor

Estando no desktop acesse o terminal em seu diretório home

Execute e tecele Enter duas vezes

```
ssh-keygen -t rsa -b 4096
```

Mostrar a chave

```
ssh-keygen -t rsa
```

Copiar a chave

```
cat ~/.ssh/id_rsa.pub
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQAC3uROa076+UUxs0bAZ1zdUABXbzSjKdKBw  
hoWohroM9z3KkVugeoc93go/X2Ce5yQ1KIUXFVwflx2ZjZGQbeTMrwHuhcYBN0E3vpIZk  
KYHlu9yFDtZJk5AuZwXkoRJMzfyOLCue/Se7hBpwZ2uC7XVc/EDeKb4thvSO18mSPSw  
lQi5oSRMSuDxWBIMWaRJPjYPxe7ilyxdzfTjVRoHJ5Glpf1uqWr2HwojB44xFDo+Otx1HyZ  
9gFKZ06gl9kpb9XGc5yR8SwWMTSWpzvoS/amPflNz6T51Olr6M6Upd4EBkrXDMf0h+tLz  
l0S02OR486fCLotbLn3OyhFJHFqXjy/ ribafs@ribaln
```

Copiar de ssh-rsa até ribafs@ribaln

```
ssh-copy-id -p 65522 ribafs@ip_servidor
```

Ele solicitará a senha na primeira vez mas após este comando acesse o servidor sem senha usando

```
ssh -p 55522 ribafs@ip_servidor
```

Também conecta com scp sem senha.

Sugestão

Criar um script para conectar ao servidor

```
sudo nano /usr/local/bin/server
```

```
ssh -p 65522 ribafs@128.199.63.251
```

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

Agora basta executar
server

A IANA - Internet Assigned Numbers Authority é responsável pela coordenação global da DNS Root, endereçamento IP e outros recursos de protocolo da Internet. É uma boa prática seguir suas diretrizes de atribuição de portas. Dito isto, os números das portas são divididos em três intervalos:

portas bem conhecidas - As Portos bem conhecidos são aqueles de 0 a 1023 e NÃO DEVEM ser usados

portas registradas - Portas registradas são de 1024 a 49151 também devem ser evitadas também

portas dinâmicas e / ou privadas - As portas dinâmicas e / ou privadas são de 49152 a 65535 e devem ser usadas.

Embora nada o impede de usar números de portas reservados, nossa sugestão é que para evitar problemas técnicos com a alocação de portas no futuro.

Crédito - http://linuxlookup.com/howto/change_default_ssh_port
Tradução livre com a ajuda do Google Translate

Permitir login do root sem senha
PermitRootLogin without-password

Permitir outros usuários
AllowUsers ribafs

Adicionar uma chave para SSH

- Caso queira adicionar uma chave para o DigitalOcean a ser associada a cada servidor que criar:

Clicuq em seu avatar/perfil - Settings - Security - Add SSH key
ou em
<https://cloud.digitalocean.com/settings/security?i=651c46>

Entre com o nome abaixo em Name

E cole a chave acima em SSH key content

Para criar a chave faça isso:

Acesse seu terminal no desktop e execute:

```
ssh-keygen -t rsa -b 4096
```

Apenas tecle enter duas vezes

Para visualizar a chave execute:

```
cat ~/.ssh/id_rsa.pub
```

Aparece algo assim:

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQCAQC1G6T7h0rVN0IbAuzg9EgGT5x7ECAhe/hfFg
5m3IDTiIKNTiQqj5u6A3EN2HQ87D0UJKh1otfh7JtBoZ/tNZFKdliO/StnZfN1U63y445e/8bX
02EB3SOIXFPoh0kIVuSTaC18y9RQ9TNfdsHdPkxRRnv1YB0/QiIM5o7ocJu65yJwzGely
nszsQpHiCnsztsG+WIIUkd9NXq78DI3CWNn7Cj86sEK+EIJonkxdURRCaWkNayZG5fPCn
V38ukH1a6R+fiYG3yD4oim8pn1+7kFMZLm5g/xwEvV2fGYXIA0sGB0skns3fqnr4u74dN+
kibjReY8GLn3zJU7VSz1dK8n3VZFuQZU5wKbo8xDIEhrYDNpvT6BbIMNqkMldXpaBjUBg
Xu8BJ/RUAgFeXXbLq02ysWD5ESS8yIYPMkamtVgkyUaL5hSV4DplbzPJxa+5XnGGz1+
WK+4S/ZyNOYwJhIT118hyfaQGONX+oKKhRyyMslx51UIIRT9voYCD/wvgyWUTuOxKmp0
uvZ3tsVgPogM37S8HnfyTrjgNmoMXgSWdA/9XIFTBvGusrVSEuQu9NzHsEYXxiAWidOty
mk0CLV1e7m6zoIXbbrx2dktEJx/boC9Ry/aSTrUH+5G6wxMT7slgJzbMtgIFwajqsjXb5NjT7
s9hf1Yr5HFjUMW9N0aQ== ola@ribafs.org
```

Copie desde ssh-rsa até ola@ribafs.org e cole no campo SSH key content

SSH

```
ssh -p yourport yourusername@yourserver
```

Rodando um comando no servidor remoto

```
ssh yourusername@yourserver updatedb
```

SCP

```
scp examplefile yourusername@yourserver:/home/yourusername/
```

```
scp yourusername@yourserver:/home/yourusername/examplefile .
```

```
scp -p yourport yourusername@yourserver:/home/yourusername/examplefile .
```

ou

```
scp -P yourport yourusername@yourserver:/home/yourusername/examplefile .
```

Copiar todo um diretório recursivamente

```
scp -r yourusername@yourserver:/home/yourusername/ .
```

SFTP

Ajustes no /etc/ssh/sshd_config

...

```
Match User sammyfiles
ForceCommand internal-sftp
PasswordAuthentication yes
ChrootDirectory /var/sftp
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

```
sftp -P 10522 user@slPouDominio
```

Após conectar efetue os comandos desejados:

ls - lista arquivos remotos

lls - lista arquivos locais. Para comandos locais adicione o prefixo l em cada comando.

Recebendo arquivos:

```
cd backup
```

```
get php.ini - copiará php.ini para o home ou onde estava quando conectou via sftp.
```

Sair - quit

! - abre o shell local. Para voltar exit

Copiar todo um diretório recursivamente

```
get -r diretorio
```

Enviando arquivos locais para o servidor remoto:

```
put arquivo.ext
```

cd - change directory on the ftp server to

lcd - change directory on your machine to

ls - list files in the current directory on the ftp server

lls - list files in the current directory on your machine

pwd - print the current directory on the ftp server

lpwd - print the current directory on your machine.

exit - exit from the sftp program.
Getting Files

The get command in sftp allows you to download files from the sftp server.

Usage: get remote-path [local-path]

Where remote-path is the file on the server you want to download, and the optional local-path is the path you want to put the file on your machine. It defaults to your current directory.

For example, to download a file named "foo.bar", the following command would be used:

```
sftp>get foo.bar
```

To download this file and save it as "readme.txt", the following command would be used:

```
sftp>get foo.bar readme.txt
```

Getting Multiple Files

To download more than one file from the sftp server use the mget command.

Usage: mget

mget works by expanding each filename listed and running a get command on each file. The files are copied into the local working directory, which can be changed with the lcd command.

For example, to download all the files in the remote working directory, the following command would be used:

```
sftp> mget ./*
```

To download all of the files ending with .txt the following command would be used:

```
sftp> mget *.*.txt
```

Recursive Copy with SCP

If you try to copy a folder using the get or mget commands, sftp will complain that it "Cannot download non-regular file: filename". This is because the basic sftp client doesn't allow for a recursive copy. However, the program scp will allow you to do this. The scp command will not allow you to see what's on the sftp server, so the files need to be located using the sftp client.

Note: scp is a separate program and must be executed from the Unix command line prompt. NOT within the SFTP client.

Usage: scp copy_from copy_to

For example, if you wanted to copy the file "foobar.txt" from the remote location to your own computer, use the command:

```
scp user@sftp.cae.wisc.edu:/path/to/foobar.txt /some/local/directory
```

Likewise, if you wanted to copy the file "foobar.txt" from your own computer to your CAE remote files, use the command:

```
scp /path/to/foobar.txt user@sftp.cae.wisc.edu:/some/remote/directory
```

In both examples, user is your CAE username. Enter your password when scp asks for it. scp works just like a get command in sftp.

To recursively copy files or directories from your CAE account, use the -r switch.

For example, to copy the entire directory "tutorial" from my CAE home directory to the home directory on your machine, the following command would be used:

```
ComputerName:~ # scp -r user@sftp.cae.wisc.edu:~/tutorial ~/
```

Where user is your CAE username.

Podemos restringir o acesso via scp ou sftp para apenas um IP ou rede

```
sshd: 192.168.1.1
```

Toda uma rede

```
sshd: 192.168.1.0/24
```

ou

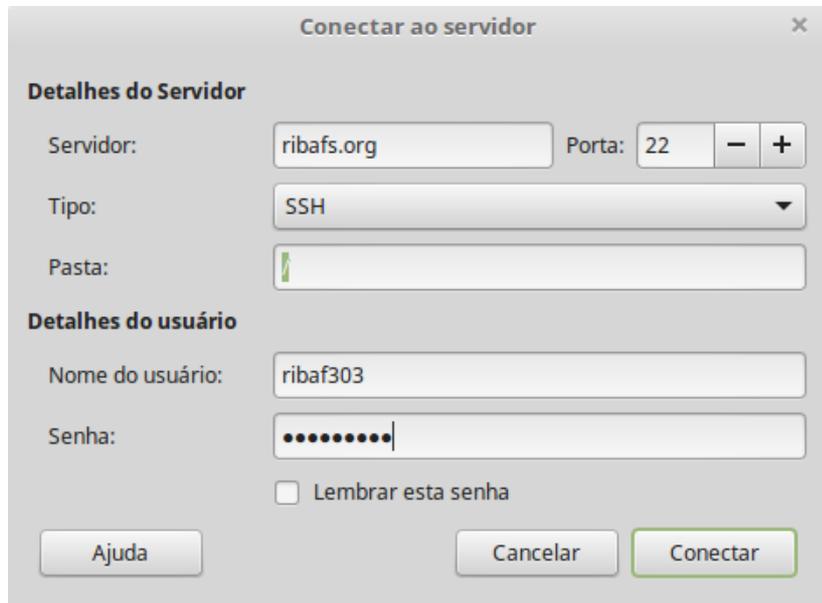
```
sshd: 192.168.1.0/255.255.255.0
```

em

ListemAddress?

USAR SSH, ou melhor SCP pelo Nautilus ou Nemo

<sftp://lotus@10.0.0.124:2222/home/lotus>



Configurar em diretório home do user.

Para cada site crie um usuário para administra o mesmo através do sftp. SSH deve ser desabilitado para estes usuários.

Criar usuário restrito

```
useradd ribafs -d /var/www/html/site1
```

Caso acuse que você já criou o diretório ignore

Caso o usuário já tenha sido criado apenas altere:

```
usermod -m -d /var/www/html/site1 ribafs
```

Criar um grupo chamado sshonly

```
groupadd sshonly
usermod -aG sshonly ribafs
```

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

Mude a linha do Subsystem para esta abaixo não permitindo ssh

```
Subsystem sftp internal-sftp
```

Adicione ao final do sshd_config

```
Match Group sshonly
```

```
ChrootDirectory %h  
ForceCommand internal-sftp  
X11Forwarding no  
AllowTcpForwarding no
```

```
systemctl restart sshd
```

Mude o grupo do diretório `we` e seus subdiretórios para `sshonly`

```
chgrp sshonly /var/www/html/ -R
```

Caso queira mudar algum usuário e seu diretório:

```
usermod -m -d /var/www/html/sitejoao/ joao
```

```
cd /var/www/html/sitejoao/  
chown joao * -R
```

Protegendo administrador do Joomla

```
nano /var/www/html/joomla/administrator/.htaccess
```

```
Order Deny,Allow  
Deny from all  
Allow from XX.XX.XX.XX  
Allow from XX.XX.XX.YY
```

How To Use SFTP to Securely Transfer Files with a Remote Server

<https://www.digitalocean.com/community/tutorials/how-to-use-sftp-to-securely-transfer-files-with-a-remote-server>

SFTP é um ftp seguro, usando o SSH.

Conexão com servidor remoto

SSH

```
ssh usuario@ip_ou_dominio
```

SFTP

```
sftp usuario@ip_ou_dominio
```

Conectando para uma porta customizada, não padrão

```
sftp -oPort=55522 usuario@ip_ou_dominio
```

Copiar para fora

```
scp -P 25522 arquivo.zip user@ip_ou_dominio:/home/ribafs
```

Copiar para cá

```
scp -P 25522 user@ip_ou_dominio:/home/user/arquivo.zip /home/ribafs
```

Ao conectar via sftp os comandos para o servidor local, seu desktop, começam com l:

Local Remoto

lls ls

lpwd pwd

lcd cd

Recebendo arquivos no desktop

```
get arquivo_remoto
```

Recebendo com outro nome

```
get arquivo_remoto arquivo2
```

Receber uma cópia recursiva

```
get -r someDirectory
```

Mantendo as permissões

```
get -Pr someDirectory
```

Enviar arquivos do desktop para o remoto

```
put localFile
```

```
put -r localDirectory
```

```
df -h
```

```
ldf -h
```

6.17 – AppArmor

Apparmor

No Debian não instalar.

É um software que melhora o kernel para isolamento de aplicativos. Este confinamento é provido por perfis de aplicativos do kernel.

Mais detalhes:

<https://wiki.ubuntu.com/AppArmor>

<https://help.ubuntu.com/lts/serverguide/apparmor.html>

<https://help.ubuntu.com/community/AppArmor>

Instalação

```
apt-get install apparmor apparmor-profiles
```

Checar funcionamento

```
apparmor_status
```

ou

```
sudo aa-status
```

6.18 – Bastille

Bastille

<https://help.ubuntu.com/community/BastilleLinux>

```
sudo apt-get install bastille
```

Revertendo alterações do Bastille

```
sudo RevertBastille
```

Reforçando a segurança do Ubuntu com Bastille

<https://www.unixmen.com/how-to-harden-your-linux-servers-security-with-bastille/>

<https://itandsecuritystuffs.wordpress.com/2014/04/08/hardening-linux-ubuntu-12-04-using-bastille/>

Atualmente o bastille suporta a maioria das distribuições

Testar antes numa box do vagrant

Execute

```
sudo netstat -pl
```

Varrer portas abertas

```
sudo nmap -n -sS -p1-65535 -sV --version-all -O -T5 -vv localhost
```

Usar o desktop

```
sudo nmap -n -sS -p1-65535 -sV --version-all -O -T5 -vv seusite.com
```

Instalação

```
sudo apt-get install bastille
```

- Internet Site - usar caso o servidor não seja servidor de e-mail

- dominio

Iniciar

```
sudo bastille -c
```

Checando configurações do firewall
`/etc/Bastille/bastille-firewall.cfg`

```
sudo iptables -L -n -v --line-numbers
```

Habilitar complexidade de senhas

```
nano /etc/pam.d/common-password
```

```
password    requisite          pam_cracklib.so retry=3 minlen=8 difok=3
```

Habilitar histórico de senhas

```
sudo sh -c 'cat /dev/null >> opasswd'
```

6.19 – fail2ban

O fail2ban deve ser instalado após a instalação do AMP/EMP

O fail2ban é mais eficiente que o denyhosts, pois ele estende a monitoração de logs para outros serviços além do ssh, como o apache, courier, ftp e mais.

O fail2ban escaneia arquivos de log e bane IPs que parecem suspeitos (muitas tentativas erradas de senha, procurando por exploits, etc)

Geralmente bloqueia através do firewall por um certo tempo que é configurável

Instalação

```
apt install fail2ban
```

Após instalar edite

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

E crie o filtro de regras requerido

Ative todos os serviços que deseja que o fail2ban monitore

Para que monitore o ssh, altere ou adicione

```
enable = true
```

OBS: atente para mudar de ssh para o número que escolheu, caso não use a 22.

```
[sshd]
```

```
enabled = true
port    = ssh
filter  = sshd
logpath = /var/log/auth.log
maxretry = 3
```

Caso o seu ssh esteja usando outra porta, mude port = sua porta

Checar status:

```
fail2ban-client status
```

Restartar

```
/etc/init.d/fail2ban restart
```

Desbloquear um certo IP bloqueado por engano

```
iptables -L -n
```

Checar porta 443

```
iptables -L -n | grep 443
```

Caso o comando acima mostre o IP 201.14.45.23 rodamos o seguinte comando para liberar:

```
iptables -D fail2ban-SSH -s 201.14.45.23 -j DROP
```

Comando mais específico:

```
fail2ban-client set ssh-iptables unbanip IpaRemove
```

Whitelisting

Whitelisting é configurada no jail.conf usando uma lista separada por espaço

```
[DEFAULT]
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
Ignoreip = 127.0.0.1 192.168.1.0/24 8.8.8.8
```

6.20 - RKHunter e CHKRootKit

Checar por RootKits

Rootkits e RKHunter basicamente fazem a mesma coisa, procuram rootkits no sistema. Nenhuma ofensiva aqui, apenas mostram o que veem.

Instalação

```
apt install rkhunter chkrootkit
```

Executando chkrootkit

```
chkrootkit
```

Atualizando e rodando rkhunter

No debian

```
nano /etc/rkhunter.conf
```

Mudar

```
UPDATE_MIRRORS=0 --> UPDATE_MIRRORS=1
```

```
MIRRORS_MODE=1 --> MIRRORS_MODE=0
```

```
WEB_CMD="/bin/false" --> WEB_CMD=""
```

```
rkhunter --update
```

```
rkhunter --propupd
```

```
rkhunter -check
```

6.21 - Detectar Intrusões com PSAD

PSAD é uma coleção de 3 pequenos daemons do sistema, que rodam para analisar mensagens de log do iptables para detectar scanneamento de portas e outros tráficos suspeitos.

Instalação

```
apt install psad
```

Configuração básica

```
nano /etc/psad/psad.conf
```

EMAIL_ADDRESSES – mude para seu e-mail

ENABLE_AUTO_IDS - se Y o psad agirá automaticamente

ENABLE_AUTO_IDS_EMAILS - se Y psad mandará um e-mail em cada suspeita

```
service psad restart
```

6.22 - Advanced Intrusion Detection Environment (AIDE)

<https://www.digitalocean.com/community/tutorials/how-to-install-aide-on-a-digitalocean-vps>

```
sudo su
```

```
apt install aide
```

```
aide --help
```

```
aide -v
```

```
aide --init
```

```
cd /var/lib/aide
```

```
ls -lt
```

```
mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

```
ls -lt
```

```
aide --check
```

Criar arquivo de teste

```
touch /usr/sbin/mytestfile.txt
```

```
aide --check
```

```
aide --update
```

```
ls -lt
```

```
mv aide.db.gz aide.db.gz-Marc152018`
```

```
mv aide.db.new.gz aide.db.gz
```

Automatizar

```
crontab -e
```

```
06 01 * * 0-6 /var/log/aide/chkaide.sh
```

```
cat /var/log/aide/chaide.sh
```

Configurações

```
/etc/aide.conf
```

6.23 - Usando DenyHosts

Scannear logs e banir hosts suspeitos

Denyhosts – bloqueia ataques de SSH adicionando entradas ao /etc/hosts.dny. Também avisa ao administrador sobre hosts suspeitos, ataques de usuários e logins suspeitos.

No Debian não está nos repositórios

```
apt install denyhosts
```

Após instalar edite o

```
nano /etc/denyhosts.conf
```

E atualize seu e-mail e outras configurações que desejar.

```
ADMIN_EMAIL = ribafs@gmail.com
SMTP_HOST = localhost
SMTP_PORT = 25
#SMTP_USERNAME=foo
#SMTP_PASSWORD=bar
SMTP_FROM = DenyHosts nobody@localhost
#SYSLOG_REPORT=YES
service denyhosts restart
```

6.24 - Melhorando a segurança com Lynis

Executa diversos testes a procura de vulnerabilidade no sistema.

Instalação (abaixo é uma só linha em cada)

Não instala no Debian

```
wget -O - http://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add - > /dev/null
```

```
echo "deb [arch=amd64] https://packages.cisofy.com/community/lynis/deb/ trusty main" | sudo tee -a /etc/apt/sources.list.d/cisofy-lynis.list
```

```
apt-get update
```

```
apt install lynis
```

Atualização

```
lynis --help
lynis update info
```

Executando

```
lynis audit system
```

Guarda os relatórios em

```
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
```

Dica: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

Audit remoto

lynis audit system remote ribafs.org

How to perform a remote scan:

=====

Target : ribafs.org

Command : ./lynis audit system --quick ribafs.org

* Step 1: Create tarball

mkdir -p ./files && cd .. && tar czf ./lynis/files/lynis-remote.tar.gz --exclude=files/lynis-remote.tar.gz ./lynis && cd lynis

* Step 2: Copy tarball to target ribafs.org

scp -q ./files/lynis-remote.tar.gz ribafs.org:~/tmp-lynis-remote.tgz

* Step 3: Execute audit command

ssh ribafs.org "mkdir -p ~/tmp-lynis && cd ~/tmp-lynis && tar xzf ../tmp-lynis-remote.tgz && rm ../tmp-lynis-remote.tgz && cd lynis && ./lynis audit system --quick ribafs.org"

* Step 4: Clean up directory

ssh ribafs.org "rm -rf ~/tmp-lynis"

* Step 5: Retrieve log and report

scp -q ribafs.org:/tmp/lynis.log ./files/ribafs.org-lynis.log

scp -q ribafs.org:/tmp/lynis-report.dat ./files/ribafs.org-lynis-report.dat

* Step 6: Clean up tmp files (when using non-privileged account)

ssh ribafs.org "rm /tmp/lynis.log /tmp/lynis-report.dat"

Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

Referências

<https://geek.linuxman.pro.br/geek/ubuntu-pronto-para-guerra>

<https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1604-lts-server-part-1-basics>

<https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/>

<https://hostpresto.com/community/tutorials/how-to-install-and-use-lynis-on-ubuntu-14-04/>

CentOS

<https://tecadmin.net/install-lamp-apache-mysql-and-php-on-centos-rhel-7/>

<https://www.rayheffer.com/building-secure-wordpress-server-lamp-centos-7-selinux/>

<https://www.godaddy.com/garage/how-to-install-and-configure-nginx-on-centos-7/>

Fedora

Install Apache/PHP 7.2.3 on Fedora 27/26, CentOS/RHEL 7.4/6.9

<https://www.if-not-true-then-false.com/2010/install-apache-php-on-fedora-centos-red-hat-rhel/>

Ubuntu

<https://www.howtoforge.com/tutorial/perfect-server-ubuntu-with-nginx-and-ispconfig-3/>

WordPress

<https://www.digitalocean.com/community/tutorials/how-to-install-wordpress-with-nginx-on-ubuntu-14-04>

ModSecurity

<https://www.hugeserver.com/kb/install-modsecurity-nginx-centos/>

<https://tecadmin.net/install-modsecurity-with-apache-on-centos-rhel/>

MySQL

<https://www.digitalocean.com/community/tutorials/how-to-set-up-master-slave-replication-in-mysql>

Nginx

<https://www.digitalocean.com/community/tutorials/como-instalar-o-nginx-no-ubuntu-16-04-pt>

<https://www.tecmint.com/install-php-7-in-centos-7/>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-nginx-server-blocks-virtual-hosts-on-ubuntu-16-04>

<https://www.howtoforge.com/tutorial/installing-nginx-with-php7-fpm-and-mysql-on-ubuntu-16.04-lts-lemp/>

PostgreSQL

<https://www.digitalocean.com/community/tutorials/how-to-set-up-master-slave-replication-on-postgresql-on-an-ubuntu-12-04-vps>

FocaLinux

http://www.guiafoca.org/?page_id=51

Livros free

<http://ribafs.org/portal/curriculo/livros/administracao-de-servidores-linux.html>

<http://ribafs.org/portal/curriculo/livros/servidores-web-linux-tipo-vps.html>

CENTOS 7

<https://www.hostinger.com/tutorials/how-to-install-lemp-centos7>

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-nginx-mysql-php-lemp-stack-on-centos-7>

[https://github.com/terrylino00/daily/wiki/Install-Nginx,-PHP-7,-MariaDB-10-\(LEMP\)-on-CentOS-7](https://github.com/terrylino00/daily/wiki/Install-Nginx,-PHP-7,-MariaDB-10-(LEMP)-on-CentOS-7)

<https://www.vultr.com/docs/initial-setup-of-a-centos-7-server>

<https://linode.com/docs/databases/mysql/how-to-install-mysql-on-centos-7/>

<http://acrelinux.org/nginx-php7-centos7/>

https://www.howtoforge.com/perfect-server-centos-7-x86_64-nginx-dovecot-ispconfig-3

Debian

<https://fatorbinario.com/tutorial-debian-8-x64-com-ispconfig-e-nginx-instalacao-do-site/>

<https://www.howtoforge.com/tutorial/perfect-server-debian-jessie-nginx-bind-dovecot-ispconfig-3.1/>

<https://www.howtoforge.com/tutorial/perfect-server-debian-9-stretch-apache-bind-dovecot-ispconfig-3-1/>

Iptables

<https://www.vivaolinux.com.br/artigo/IPTABLES-Conceitos-e-aplicacao>

<https://www.vultr.com/docs/easy-iptables-configuration-and-examples-on-ubuntu-16-04>

UFW

<https://linuxconfig.org/how-to-install-and-use-ufw-firewall-on-linux>

Nginx

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-nginx-mysql-php-lemp-stack-on-centos-7>

<https://www.hostinger.com/tutorials/how-to-install-lemp-centos7>

<https://www.digitalocean.com/community/tutorials/how-to-install-nginx-on-ubuntu-16-04>

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-nginx-mysql-php-lemp-stack-in-ubuntu-16-04>

<https://linuxconfig.org/basic-php-7-and-nginx-configuration-on-ubuntu-16-04-linux>

SSL

<https://www.digitalocean.com/community/tutorials/how-to-create-an-ssl-certificate-on-nginx-for-ubuntu-14-04>

Instalação do Joomla pela linha de comando

<http://joomlaresources.com/joomla-tutorials/install-joomla-using-the-ssh-command-line>

Tools

Putty - <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

WinSCP - <https://winscp.net/eng/download.php>

Teamviewer - <https://www.teamviewer.com/pt/>

Skype - <https://www.skype.com/pt-br/>

Vagrant

Virtualbox - <https://www.virtualbox.org/wiki/Downloads>

Extensões -

https://download.virtualbox.org/virtualbox/5.2.6/Oracle_VM_VirtualBox_Extension_Pack-5.2.6-120293.vbox-extpack

Git - <https://git-scm.com/>

Vagrant - <https://www.vagrantup.com/downloads.html>

Boxes - <https://app.vagrantup.com/boxes/search>

Formatador de pendrive e instalador de ISO

<https://etcher.io/>

<https://github.com/perusio/drupal-with-nginx/commits/D7>

7 – Ferramentas

7.1 – Backup

Soluções para backup

- Disco inteiro ou partição - Full
<http://clonezilla.org/>

- Duplicati - incremental backup of your system's and server's and store the data on cloud in encrypted format.
<http://www.elinuxbook.com/install-duplicati-backup-app-in-ubuntu-16-04-a-best-free-backup-software-for-linux/>

Simples de instalar e funcional.

Backup Your Entire Linux System Using Rsync
<https://www.ostechnix.com/backup-entire-linux-system-using-rsync/>

- Backup do disco inteiro com rsync
 Inserir pendrive ou HD e montar
 sudo mount /dev/sdb1 /mnt

Como root execute
 sudo rsync -aAXv /
 --exclude={"/dev/*","/proc/*","/sys/*","/tmp/*","/run/*","/mnt/*","/media/*","/lost+found"} /mnt

rsync – A fast, versatile, local and remote file-copying utility
 -aAXv – The files are transferred in “archive” mode, which ensures that symbolic links, devices, permissions, ownerships, modification times, ACLs, and extended attributes are preserved.

/ – Source directory

–exclude – Excludes the given directories from backup.

/mnt – It is the backup destination folder.

Alerta: Isso excluirá tudo do destino

- Bacula

- <https://sourceforge.net/projects/backuppc/>

- <https://www.urbackup.org/download.html>

Ubuntu

```
sudo add-apt-repository ppa:uroni/urbackup
sudo apt update
sudo apt install urbackup-server
```

<https://www.urbackup.org/ServerAdminGuide-v2.2.pdf>

- <https://labs.riseup.net/code/projects/backupninja>

- **ShadowProtect**

- **Amanda backup**

- Backup e restore

<http://relax-and-recover.org/>

- <https://www.vembu.com/vembu-networkbackup/> for windows

- <http://www.linuxandubuntu.com/home/10-best-linux-backup-solutions>

- LuckyBackup

https://sourceforge.net/projects/luckybackup/files/0.4.9/ubuntu-16.10/luckybackup_0.4.9-1_amd64.deb/download

Duplicacy

<https://www.digitalocean.com/community/tutorials/manage-backups-cloud-duplicacy>

Backup com Duplicati

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

<http://www.elinuxbook.com/install-duplicati-backup-app-in-ubuntu-16-04-a-best-free-backup-software-for-linux/>

```
sudo apt-get update
```

```
wget https://updates.duplicati.com/beta/duplicati_2.0.2.1-1_all.deb # Download the Package
```

```
sudo dpkg -i duplicati_2.0.2.1-1_all.deb
```

```
sudo apt-get install -f
```

```
sudo dpkg -l duplicati
```

```
duplicati
```

ou abrir pela web

```
http://localhost:8200/ngax/index.html#/
```

Desinstalar

```
sudo dpkg -r duplicati
```

Backup incremental com Rsync

O objetivo é efetuar backup de uma pasta do desktop para um servidor remoto. Ideal para quando temos dois desktops de trabalho, um em casa e outro no trabalho. Executar o script em cada um irá levar apenas as alterações do dia. Melhor ainda se adicionado ao crontab.

No computador desktop acessar o terminal em seu diretório home e executar o comando abaixo para gerar a chave do SSH

```
ssh-keygen -t rsa
```

Copiar a chave para o servidor remoto, cuja porta do SSH é 55522

```
ssh-copy-id -p 55522 ribafs@ip_servidor
```

Após entrar com sua senha do servidor teste:

```
ssh -p 55522 user@ip_ou_dominio
```

Assim o script poderá funcionar sem solicitar senha

Agora o script para Backup com rsync incremental

Este script efetuar o backup da pasta local
backup/0ribamar/Projetos/1Livros/VPS/

Para o servidor em
/home/ribafs/backup/VPS/

As opções

-a - archive, semelhante a usar todos estes: -rlptgoD:

r - Recursive

l - copia Links simbólicos

p - preserva Permissões

t - preserva modificações do tempo

g - preserva grupo

o - preserva dono (owner)

D - preserva arquivos de dispositivos (somente root) e arquivos especiais

--delete - remove arquivo do destino quando foi removido na origem

-e - conexão via SSH

```
nano /usr/local/bin/backup_rsync.sh
```

```
#!/bin/sh
```

```
# Backup de uma pasta local para um servidor remoto
```

```
# https://www.aprendendolinux.com/sincronizando-com-o-rsync/
```

```
echo "=== BACKUP INCREMENTAL USANDO RSYNC E CRON ===";
echo "";
echo "";
```

```
rsync -av --delete -e 'ssh -p 65522' --delete /backup/Oribamar/Projetos/1Livros/VPS/
ribafs@165.227.227.139:/home/ribafs/backup/VPS/
```

```
chmod +x /usr/local/bin/backup_rsync.sh
```

Adicionar ao cron

```
crontab -e
```

```
10 09 * * * root /usr/local/bin/backup_rsync.sh
```

Restore do servidor remoto para o desktop local

```
nano /usr/local/bin/restore_rsync.sh
```

```
#!/bin/bash
echo "Obrigatoriamente o diretório para restore precisa terminar com /. Ex:
restore_rsync.sh /backup/VPS/";
echo "Aperte qualquer tecla para continuar";
echo "";
echo "";
read n;
if [ ! "$1" ]; then
    echo "Sintaxe: $0 /diretorio/";
    echo "";
    echo "Entre com o nome do script e o diretório com barra ao final"
    exit 1
else
    rsync -av --delete -e 'ssh -p 65522' --delete
ribafs@165.227.227.139:/home/ribafs/backup/VPS/Dicas/ $1;
fi
```

```
chmod +x /usr/local/bin/restore_rsync.sh
```

Antes de executar

Remover a pasta local ou renomear

Executando. Lembre de deixar uma barra ao final da pasta, para que traga a própria pasta e não somente os arquivos dela

```
sh restore_rsync.sh /backup/VPS/
```

Script de Backup

```
#!/bin/sh

# Backup para servidor remoto
# https://www.aprendendolinux.com/sincronizando-com-o-rsync/
rsync -avz --delete -e 'ssh -p 65522' --delete /backup/Oribamar/Projetos/1Livros/VPS/
ribafs@165.227.227.139:/home/ribafs/backup/VPS/

# Adicionar ao crontab
# crontab -e
# Efetuar o backup incrementar todos os dias as 14:00
# 00 14 * * * /usr/local/bin/backup_rsync.sh
```

Exemplos

```
# Com logs do remoto para o desktop
# touch /var/log/rsync.log
#rsync -arlpgo --delete --log-file=/var/log/rsync.log -e "ssh -p 65522"
ribafs@165.227.227.139:/home/ribafs/backup/ /backup/Oribamar/Projetos/1Livros/VPS/
```

Incremental (a), compactado (z) e verbose (v)
rsync -azv /etc/sysconfig /backup/

Envia do desktop para o servidor remoto
rsync -ravzX --delete /home/laytonjb/TEST/SOURCE/
laytonjb@test8:/home/laytonjb/TEST/

Usar --delete com bastante cuidado, pois pode remover tudo do destino ou da origem em caso contrário. Usar com cautela.

Run the following command as root to make sure that rsync can access all system files and preserve the ownership:

```
rsync -aAXv
--exclude={"/dev/*","/proc/*","/sys/*","/tmp/*","/run/*","/mnt/*","/media/*","/lost+found"} /
/path/to/backup/folder
```

Dicas

```
rsync -av -e 'ssh -p 65522' --progress --delete-after /backup/transp/rsync/
ribafs@178.62.122.149:/home/ribafs/rsync/
```

Com porta diferente da 22
rsync -arvz -e 'ssh -p <port-number>' --progress --delete user@remote-
server:/path/to/remote/folder /path/to/local/folder

Do desktop para o server

```
rsync -avz -e 'ssh -p 65522' --progress /backup/transp/rsync/  
ribafs@178.62.122.149:/home/ribafs/rsync/
```

Passar a senha pelo cron

```
ssh-keygen
```

```
ssh-copy-id -i ~/.ssh/id_rsa.pub ribafs@192.168.200.10 -p 65522
```

```
sudo crontab -e
```

```
30 12 * * * rsync -aq -e 'ssh -p 65522' /backup/transp/rsync/  
ribafs@178.62.122.149:/home/ribafs/rsync/
```

Podemos adicionar ao crontab assim, para executar com o root:

```
30 3 * * * /usr/bin/rsync -avz --delete -e "ssh -i /root/.ssh/id_rsa_backup"  
/var/www/wordpress backup@backup.example.com:/home/backup/sync
```

7.2 – Painel de Controle Web

VestaCP

VESTACP

<https://vestacp.com>

Documentação

<https://vestacp.com/docs/>

Versões free e comercial/suporte e plugins

Serviços disponíveis

- Domínios
- DNS
- E-mail e webmail: spamassassin, clamav, dovecot, exim, roundcub
- Bancos de dados (My ou PG)
- Cron Jobs
- Backup - apenas para o próprio vesta e sua estrutura
- vsFTPd ou proFTPd
- Web - nginx ou apache/php
- Gráficos
- Estatísticas e logs
- Firewall - iptables/fail2ban
- Aplicativos/Softaculous
- Filemanager - plugin comercial

Alternativamente podemos instalar o eXtplorer

- Chroot no SFTP - plugin comercial

OBS: Me parece que 1GB de RAM é pouco para instalar o pacote completo, especialmente com antivírus e antispam.

Suporta Ubuntu, Debian, RedHat e CentOS

Instalar

OBS: Instalar somente em servidor limpo e recém instalado

```
# Connect to your server as root via SSH
ssh -p 65522 ribafs@ribafs.org
```

```
# Download installation script
curl -O http://vestacp.com/pub/vst-install.sh
```

```
# Run it
```

```
bash vst-install.sh --nginx yes --phpfpm yes --apache no --named yes --remi yes --vsftpd
yes --proftpd no --iptables yes --fail2ban yes --quota yes --exim yes --dovecot yes
--spamassassin yes --clamav yes --softaculous yes --mysql yes --postgresql no
--hostname ribafs.org --email ribafs@gmail.com
```

Acusou erro: user admin já existe.

Usuário não existe mas grupo sim:
groupdel admin

Refiz e instalou.

<https://138.68.191.87:8083>

Mas a porta acima é bloqueada em meu trabalho, então pesquisei.

Para alterar a porta
nano /usr/local/vesta/nginx/conf/nginx.conf

```
...
# Vhost
server {
    listen    443;
...

```

service vesta restart

<https://138.68.191.87>

A 443 é a default do SSL e liberada aqui.

7.3 - Soluções para Administração Web de Servidor

Atomia DNS

<http://atomiadns.com/>

AlternC

<https://alternc.com/Install-en>

Webmin

<http://www.webmin.com/>

Virtualmin

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

CentOS Web Panel

<http://centos-webpanel.com/>

Sentora

<http://sentora.org/>

Server Pilot

<https://serverpilot.io>

Ajenti

<http://ajenti.org/>

VESTACP

<https://vestacp.com>

Suporta Ubuntu, Debian, RedHat e CentOS

Instalar

OBS: Instalar somente em servidor limpo e recém instalado

```
# Connect to your server as root via SSH  
ssh -p 65522 ribafs@ribafs.org
```

```
# Download installation script  
curl -O http://vestacp.com/pub/vst-install.sh
```

```
# Run it
```

```
bash vst-install.sh --nginx yes --phpfpm yes --apache no --named yes --remi yes --vsftpd  
yes --proftpd no --iptables yes --fail2ban yes --quota yes --exim yes --dovecot yes  
--spamassassin yes --clamav yes --softaculous yes --mysql yes --postgresql no  
--hostname ribafs.org --email ribafs@gmail.com
```

Cockpit

<http://cockpit-project.org/>

ZPanel

Ubuntu LTS Server:

```
bash <(curl -Ss https://raw.githubusercontent.com/zpanel/installers/master/install/Ubuntu-  
12_04/10_1_1.sh)
```

ISPConfig

<https://www.ispconfig.org/>

Rolekit

<https://github.com/libre-server/rolekit>
Roda no Fedora

Cockpit

<http://cockpit-project.org/>

Starting containers, storage administration, network configuration, inspecting logs and so on.

A service started via Cockpit can be stopped via the terminal. Likewise, if an error occurs in the terminal, it can be seen in the Cockpit journal interface.

You can monitor and administer several servers at the same time. Just add it easily and your server will look after its buddies.

```
sudo yum update
sudo yum install cockpit
sudo service start cockpit
```

Configuração

```
cp /etc/cockpit/cockpit.conf /root/backup
```

```
nano /etc/cockpit/cockpit.conf
```

```
[WebService]
```

```
Origins = https://somedomain1.com https://somedomain2.com:9090
```

```
/etc/systemd/system/cockpit.socket.d/listen.conf
```

```
sudo semanage port -a -t websm_port_t -p tcp 9999
```

```
sudo semanage port -m -t websm_port_t -p tcp 443
```

```
sudo firewall-cmd --permanent [--zone=ZONE] --add-port=443/tcp
```

```
sudo systemctl enable cockpit.socket
```

Customizar privilégios

Para que um usuário tenha privilégios para gerenciar as atividades do cockpit ele precisa pertencer ao grupo wheel

```
cp -Ra /etc/polkit-1/rules.d /root/backup
```

```
nano /etc/polkit-1/rules.d
```

Exemplo: placing the following polkit rule to `/etc/polkit-1.rules.d/10-operators.rule` allows all users in the operators group to start, stop, restart and otherwise manage systemd services:

```
polkit.addRule(function(action, subject) {
  if (action.id == "org.freedesktop.systemd1.manage-units") {
    if (subject.isInGroup("operators")) {
      return polkit.Result.YES;
    }
  }
});
```

In order to allow a certain group to perform any administrative action you could add a rule like this:

```
polkit.addAdminRule(function(action, subject) {
    return ["unix-group:operators"];
});
```

Cockpit provides a standard shell in a terminal. This shell and the processes running in it have the same privileges as if the user had logged in via SSH.

Para limpar todas as informações de problemas do SELinux

```
sudo killall setroubleshootd
sudo rm -rf /var/lib/setroubleshoot/*
```

7.4 – Testes de Stress para Servidor Web

AB - Apache HTTP server benchmarking tool

<https://httpd.apache.org/docs/current/pt-br/programs/ab.html>

ab is a tool for benchmarking your Apache Hypertext Transfer Protocol (HTTP) server. It is designed to give you an impression of how your current Apache installation performs. This especially shows you how many requests per second your Apache installation is capable of serving.

```
ab [ -A auth-username:password ] [ -b window-size ] [ -B local-address ] [ -c concurrency ] [
-C cookie-name=value ] [ -d ] [ -e csv-file ] [ -f protocol ] [ -g gnuplot-file ] [ -h ] [ -H custom-
header ] [ -i ] [ -k ] [ -l ] [ -m HTTP-method ] [ -n requests ] [ -p POST-file ] [ -P proxy-auth-
username:password ] [ -q ] [ -r ] [ -s timeout ] [ -S ] [ -t timelimit ] [ -T content-type ] [ -u
PUT-file ] [ -v verbosity ] [ -V ] [ -w ] [ -x <table>-attributes ] [ -X proxy[:port] ] [ -y <tr>-
attributes ] [ -z <td>-attributes ] [ -Z ciphersuite ] [http[s]://]hostname[:port]/path
```

```
sudo apt-get update
sudo apt-get install apache2-utils
```

A URL precisa terminar com /

Exemplos:

```
ab -n 10000 -c 50 -k google.com.br/
```

10 mil requisições e 50 usuários, 200 requisições por usuário, o que é um pouco absurdo, mas a ideia do teste é exatamente essa, ver os limites, claro que para um bom teste deve verificar o que quer testar e de acordo com a necessidade prevista para o seu site.

Você quer simular, um acesso com 10 usuários usando ao mesmo tempo seu site ou o mais próximo disso e cada um visitou 20 páginas ou fez 20 requisições ao seu site:

```
ab -n 200 -c 10 -k seusite.com.br/
```

Testando com 100 conexões em modo "Keep Alive" e com tempo de 30 segundos para ser realizado o teste.

```
ab -kc 100 -t 30 http://127.0.0.1/
```

Aumentando o número de requisições para 10000, sendo 100 usuários concorrentes.

```
ab -n 10000 -c 100 http://localhost/
```

The simplest test you can do is to perform 1000 requests, 10 at a time (which approximately simulates 10 concurrent users getting 100 pages each - over the length of the test).

```
ab -n 1000 -c 10 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/
```

```
ab -l -r -n 100 -c 10 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/
```

-n 1000 is the number of requests to make.

-c 10 tells AB to do 10 requests at a time, instead of 1 request at a time, to better simulate concurrent visitors (vs. sequential visitors).

-k sends the KeepAlive header, which asks the web server to not shut down the connection after each request is done, but to instead keep reusing it.

This is 100 sequential page loads by a single user:

```
ab -l -r -n 100 -c 1 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/blog/
```

This is 50 page loads (total) by 5 different concurrent users, each user is doing 10 sequential pages loads.

```
ab -l -r -n 50 -c 5 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/blog/
```

This is 100 page loads by 10 different concurrent users, each user is doing 10 sequential pages loads.

```
ab -l -r -n 100 -c 10 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/blog/
```

This is 600 page loads by 30 different concurrent users, each user is doing 20 sequential pages loads.

```
ab -l -r -n 600 -c 30 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/blog/
```

This is 2700 page loads by 90 different concurrent users, each user is doing 30 sequential pages loads.

```
ab -n 2700 -c 90 -k -H "Accept-Encoding: gzip, deflate" http://www.example.com/blog/
```

```
ab -n 100 -c 10 -k -H "Accept-Encoding: gzip, deflate" http://localhost:yourport/
```

```
#!/bin/sh
```

```
ab -n 100 -c 10 http://127.0.0.1:8300/test.cfm > test1.txt &
ab -n 100 -c 10 http://127.0.0.1:8300/scribble.cfm > test2.txt &
```

Usage: ab [options] [http[s]://]hostname[:port]/path

Options are:

- n requests Number of requests to perform
- c concurrency Number of multiple requests to make
- t timelimit Seconds to max. wait for responses
- b windowsize Size of TCP send/receive buffer, in bytes
- p postfile File containing data to POST. Remember also to set -T
- T content-type Content-type header for POSTing, eg.
 'application/x-www-form-urlencoded'
 Default is 'text/plain'
- v verbosity How much troubleshooting info to print
- w Print out results in HTML tables
- i Use HEAD instead of GET
- x attributes String to insert as table attributes
- y attributes String to insert as tr attributes
- z attributes String to insert as td or th attributes
- C attribute Add cookie, eg. 'Apache=1234. (repeatable)
- H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
 Inserted after all normal header lines. (repeatable)
- A attribute Add Basic WWW Authentication, the attributes
 are a colon separated username and password.
- P attribute Add Basic Proxy Authentication, the attributes
 are a colon separated username and password.
- X proxy:port Proxyserver and port number to use
- V Print version number and exit
- k Use HTTP KeepAlive feature
- d Do not show percentiles served table.
- S Do not show confidence estimators and warnings.
- g filename Output collected data to gnuplot format file.
- e filename Output CSV file with percentages served
- r Don't exit on socket receive errors.
- h Display usage information (this message)
- Z ciphersuite Specify SSL/TLS cipher suite (See openssl ciphers)
- f protocol Specify SSL/TLS protocol (SSL2, SSL3, TLS1, or ALL)

Performance Gains

For top performance gains use –

1. Apache's mod_cache module to cache page requests/results. This will produce 5-10x the performance gains over all other methods combined.

2. PHP's Zend OPcache extension to cache PHP scripts as compiled objects. This will produce a 3-5x Requests Per Second speed up.

3. memcached + php_memcache setup to cache PHP script's or web-app's internal data and results. This can produce a good 50%-100% performance gain.

4. Cache plugins and/or setting adjustments specific to the web-app: Cache plugins for WordPress, Speedup tips for PrestaShop, etc.

5. mod_expires to make the client's (visitor's) Browser cache pages and page assets for a given time, instead of re-getting those pages and assets on each page load.

* Some of these are more difficult to configure and set up than others.

Also, in my experience, the switch from 32 bit to 64 bit Apache, PHP, and MySQL versions only provides limited/marginal performance gains (and in some cases it's even negative).

To sum everything up, 99% of all performance gains will come from utilizing Apache's caching mechanisms (via mod_cache), using PHP Zend OPcache (extension), and afterwards (once the bottleneck is moved from Apache with PHP to MySQL), improving MySQL performance by tuning my.ini settings, and optimizing/restructuring MySQL queries by utilizing MySQL's Slow Query log (to see what the problem is).

Having said that, there are also performance robing issues that can exist on the OS, in the Apache/MySQL/PHP settings, and even the client's Browser, that are covered here – <http://www.devside.net/wamp-server/wamp-is-running-very-slow>

<https://www.devside.net/wamp-server/load-testing-apache-with-ab-apache-bench>

<https://www.codemarket.com.br/site/usando-o-ab-apachebench-para-teste-de-desempenho-e-stress>

<https://ikvasnica.com/blog/load-test-multiple-api-endpoints-concurrently-use-this-simple-shell-script/>

7.5 - Configurações da Rede do VirtualBox

Rede tipo Host Only

- Abrir o Virtualbox
- Arquivo - Preferências
- Rede
- Clicar no sinal de + à direita
- É criada uma interface com nome NatNetwork
- Clicar no botão de editar abaixo do sinal de +
- Entre com o IP e máscara da rede

Ao criar a(s) VM(s) use esta interface

Podemos criar uma rede dentro do Virtualbox, sendo cada VM com duas placas, uma NAT (acessa internet) e outra host only (se comunica com as demais VMs)

Rede em modo 'NAT': utilizada para ativar uma placa de rede na Máquina Virtual (MV) com a finalidade de conectá-la à Internet (ou à rede local) através da Máquina Física. Ou seja, a MV terá como Gateway Padrão a própria Máquina Física (o sistema hospedeiro).

Rede em modo 'Bridge': utilizada para ter acesso à rede local, sem a necessidade de ter a Máquina Física como Gateway Padrão. Ou seja, a nossa Máquina Virtual será vista na Rede Local como se fosse mais uma Máquina Física.

Rede em modo 'Rede Interna (intnet)': utilizada para simular uma Rede Local somente entre as Máquinas Virtuais (MVs). Ou seja, com essa opção pode-se realizar a comunicação entre as Máquinas Virtuais, simulando situações de uma ou mais redes locais.

Rede em modo 'host-only': a placa fica para uso exclusivo do hospedeiro, ou seja, a interface servirá apenas para comunicação entre Máquina Virtual (que é o hóspede) e a Máquina Física (que é o hospedeiro).

A Máquina Física possui 3 (três) Máquinas Virtuais simulando um ambiente de Rede Completo. No VirtualBox as configurações das interfaces de rede poderiam ser as seguintes para simulação:

Máquina Virtual Servidor: 2 placas de rede habilitadas, sendo uma como 'NAT' (Internet) e outra como 'Rede Interna' (comunicação com a rede local simulada);

Máquina Virtual 1: 1 placa de rede habilitada como 'Rede Interna', terá a MV Servidor como Gateway Padrão;

Máquina Virtual 2: 1 placa de rede habilitada como 'Rede Interna', terá a MV Servidor como Gateway Padrão. Pode-se colocá-la em outra rede para simular a comunicação entre redes locais passando pelo Servidor (Firewall).

Enfim, pode-se fazer diversas combinações híbridas para simular ambientes de rede, desenvolvimento, bancos de dados, etc.

== Adicionais para Convidado

É um pacote especial de software fornecido pelo VirtualBox para ser instalado no sistema convidado.

== Tipos de Rede

NAT (Network Address Translation)

É o modo padrão de rede no VirtualBox. Com este modo, o VirtualBox age como um roteador, mapeando o tráfego, mascarando os IPs e possibilitando a comunicação da VM com a rede externa. O sistema convidado recebe um endereço IP que não faz parte da rede externa, do servidor DHCP integrado ao VirtualBox, e portando, durante todo o tráfego, os endereços e portas são traduzidos. Cada máquina virtual terá um roteador particular e elas não farão parte de uma mesma rede, impossibilitando a comunicação entre elas.

Este modo é necessário quando não é possível a máquina virtual obter um endereço IP real da rede externa. Ou quando deseja tornar a VM invisível e inalcançável pela rede externa, pelo menos não diretamente.

Placa Em Modo Bridge

Neste modo, o VirtualBox usa um driver de dispositivo para interceptar e injetar dados no adaptador de rede físico, tornando-se um adaptador de rede por software. O sistema convidado, usando este adaptador de rede por software, consegue conectar-se diretamente na rede externa e assim receber um endereço IP válido na rede externa.

O sistema hospedeiro e também todas as máquinas da rede, na qual a máquina hospedeira pertence, enxergarão normalmente a VM pela rede como se a VM fosse uma máquina real.

É um modo geralmente utilizado em sistemas convidados que são servidores de rede. Este modo possui algumas limitações dependendo do sistema operacional hospedeiro.

Rede Interna

Este modo é utilizado para criar uma rede por software onde somente as máquinas virtuais selecionadas ficarão visíveis entre elas. Nenhuma máquina da rede externa, nem mesmo o próprio hospedeiro enxergará as VMs da rede interna. Desta forma, todo o tráfego ficará restrito à rede interna e completamente isolado e escondido da rede externa.

É um modo seguro de se fazer rede entre as VMs, pois será impossível capturar pacotes pela rede externa.

Placa De Rede Exclusiva De Hospedeiro

Neste modo, o VirtualBox monta uma rede contendo somente o hospedeiro e um conjunto de máquinas virtuais, sem a necessidade do adaptador de rede físico do hospedeiro. É um modo híbrido entre o modo bridge e o modo de rede interna, as VMs se enxergarão entre si e ao hospedeiro, como se estivessem conectadas a uma mesma rede física, porém, como a rede interna está conectada somente à interface virtual do hospedeiro, o acesso a rede externa não é possível.

O VirtualBox cria no sistema hospedeiro uma interface virtual de rede, semelhante a interface de loopback. Esta interface proporciona a conectividade entre as VMs e o sistema hospedeiro.

Driver Genérico

Este modo é raramente usado. Permite ao usuário selecionar um driver que pode ser incluído no VirtualBox, numa recompilação, ou fornecido por um pacote de extensão.

Possui submodos os quais permitem que máquinas virtuais, em hospedeiros distintos, fiquem conectadas numa mesma infraestrutura de rede. Em outras palavras, permite a conexão em rede de sistemas convidados que estão em diferentes sistemas hospedeiros.

Generalizando, é uma parte opcional do VirtualBox que só está incluída no código fonte. O pacote fornecido pela Oracle não inclui os drivers necessários.

Não conectado

O adaptador está instalado, mas simula que o cabo está desconectado. Veremos que o loopback e o localhost, assim como as configurações TCP/IP estarão disponíveis.

NAT

Esse é o modo padrão do VirtualBox, quando ele toma emprestada a conexão do host com a Internet e a entrega para o guest. Todo o restante da rede fica transparente para a VM, mas acessamos a Internet nela normalmente, inclusive com IP automático, fornecido por um DHCP - Dynamic Host Configuration Protocol - próprio do VirtualBox.

Placa em modo bridge

Neste modo o adaptador faz uma ponte com a interface "real" do host, conectando-se diretamente à rede deste. Passamos a ter mais um computador na rede do host, inclusive obtendo IP dinamicamente, caso a rede possua essa capacidade. Teremos uma rede entre host, guest e todos os equipamentos da rede como modem, switch, proxy, gateway padrão, etc...

Rede interna

Aqui o VirtualBox monta uma rede totalmente virtual entre todas as máquinas virtuais que estão em funcionamento, independente da rede real ou do host. Ótimo para estudar e testar redes sem interferir na rede "verdadeira". Lembre-se que neste modo o VirtualBox não disponibiliza o DHCP, portanto as configurações TCP/IP devem ser feitas manualmente.

Placa de rede exclusiva do hospedeiro (host-only)

Este modo é um pouco mais complexo: ele faz uma rede entre a interface "real" do host e as máquinas virtuais, mas não dá acesso à rede "real" em que o host está conectado, ou seja, o host se comunica com as VMs e vice-versa, mas as VMs não se comunicam com outros computadores da rede "real" do host. É um híbrido entre "Placa em modo bridge" e "Rede interna".

8 – Shell Scripts

Alguns exemplos de scripts funcionais

admin.sh – Menu usando a biblioteca dialog para mostrar atividades para administradores

```
#!/bin/bash
#
# Criado/adaptado por Ribamar FS - http://ribafs.org
#
#apt-get install dialog;
#
menu="DNOCS"
while :
do
clear
servico=$(dialog --stdout --backtitle 'Equipe de TI do DNOCS - Administração dos
Servidores' \
--menu "$menu" 12 65 0 \
1 'Backup de um banco mysql' \
2 'Backup de um banco PostgreSQL' \
3 'Backup dos arquivos do site do DNOCS (arquivos)' \
4 'Backup dos arquivos de um aplicativo' \
0 'Sair' )
case $servico in
1) clear;
# Backup de banco de dados mysql
DIALOG=${DIALOG=dialog}
tempfile=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
trap "rm -f $tempfile" 0 1 2 5 20

$DIALOG --title "Nome do banco de dados em MySQL" --clear \
--inputbox "Digite o nome do banco de dados\n
Lembre que sempre o backup do banco será criado em /var/www/backup\n\n
Digite abaixo o nome do banco\n\nE Aguarde o backup ..." 14 80 2> $tempfile

retval=$?
BD=`cat $tempfile`;
DATA=`/bin/date +%Y-%m-%d`;
BACK="/var/www/html/backup/my";
case $retval in
0)
mysqldump -uroot -pmysql $BD > "$BACK/$BD$DATA.sql";
echo "O backup foi criado em:/var/www/html/backup/$BD$DATA.sql";
echo "Acesse pleo navegador em http://localhost/backup/$BD$DATA.sql\nTecle
enter para continuar"
read n;;
1)
```

```

        echo "Cancelado.";;
    esac;;
2) clear;
   # Backup de banco de dados PostgreSQL
   dialog \
       --title 'Backup de banco PostgreSQL' \
       --msgbox 'Entre banco, esquema e tabela a seguir. \nObserve que
somente o banco é obrigatório' \
           6 80
   echo "Digite o nome do banco de dados abaixo e tecle Enter\n\n";
   read BD;

   echo "Digite o nome do [esquema] abaixo e tecle Enter\n\n";
   read ESQ;

   echo "Digite o nome da [tabela] abaixo e tecle Enter.\n\n";
   read TB;

   pgback.sh $BD $ESQ $TB;
   echo "Backup concluído. Confira com http://localhost/backup/pg\nTecle enter";
   read n;;
3) clear;
   # Backup de arquivos do site
   dialog \
       --title 'Backup de arquivos do site do DNOCS' \
       --msgbox 'Digite o diretório abaixo' \
           6 80
   DIALOG=${DIALOG=dialog}
   tempfile=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
   trap "rm -f $tempfile" 0 1 2 5 20

   DATA=`/bin/date +%Y-%m-%d`;

   $DIALOG --title "Diretório do site" --clear \
       --inputbox "O diretório default é /var/www/html\n" 14 80 2> $tempfile
   retval=$?
   diretorio=`cat $tempfile`

   BACK="/var/www/html/backup";
   case $retval in
   0)
       tar czpvf "$BACK/site-$DATA.tar.gz" $diretorio;
       clear;
       echo "Backup concluído.\n\nConfira em http://localhost/backup\n\nAperte
qualquer tecla";
       read n;;
   1)
       echo "Cancelado.";
   esac;;
4) clear;

```

```

# Backup de arquivos de aplicativo
dialog \
    --title 'Backup de arquivos de um aplicativo' \
    --msgbox 'Digite o diretório abaixo' \
    6 80
DIALOG=${DIALOG=dialog}
tempfile=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
trap "rm -f $tempfile" 0 1 2 5 20

DATA=`/bin/date +%Y-%m-%d`;
BACK="/var/www/html/backup/";

$DIALOG --title "Diretório do aplicativo" --clear \
    --inputbox "Digite o diretório completo relativo ao /var/www/html\n
    Exemplo: se em /var/www/html/app1 basta digitar app1\n" 14 80 2> $tempfile
retval=$?
diretorio=`cat $tempfile`
case $retval in
0)
    tar czpvf "$BACK/$diretorio-$DATA.tar.gz" "/var/www/html/$diretorio";
    clear;
    echo "Backup concluído.\n\nConfira em http://localhost/backup\n\nAperte
qualquer tecla";
    read n;;
1)
    echo "Cancelado.";
esac;;
0) clear;
exit;;
esac
done

```

devel.sh – menu usando a lib dialog para mostrar atividades do grupo devel

```

#!/bin/bash
#
# Criado/adaptado por Ribamar FS - http://ribafs.org
#
#apt-get install dialog;
#
menu="Menu Principal\n\nUse as setas do teclado ou o mouse para selecionar uma
opção\nEntão tecle Enter ou clique em OK"
while :
do
clear
servico=$(dialog --stdout --backtitle 'Equipe de TI do DNOCS - Ambiente de
Desenvolvimento' \
    --menu "$menu" 12 65 0 \
    1 'Criar Aplicativo para a Intranet' \

```

```

2 'Gerar CRUG com o Bake' \
3 'Atualizar Aplicativo com o Composer' \
4 'Saber versão do Cake de um Aplicativo' \
5 'Corrigir erro de permissão em aplicativo' \
0 'Sair' )
case $servico in
1) clear;
  DIALOG=${DIALOG=dialog}
  tempfile=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
  trap "rm -f $tempfile" 0 1 2 5 20

```

```

  $DIALOG --title "Diretório do Aplicativo" --clear \
  --inputbox "Digite o diretório onde será criado o aplicativo\n

```

Lembre que seu diretório atual é o /var/www/html\n\n

Por exemplo, para criar o aplicativo cake3-dnocs em /var/www/html/modelos/\n

Solte o mouse e digite abaixo: modelos/cake3-dnocs \n\nE Aguarde a criação ..." 14 80 2> \$tempfile

```

retval=$?
dir1=`cat $tempfile`
case $retval in
0)
  comp "/var/www/html/$dir1";
  dialog \
  --title 'Acesse pelo NetBeans ou pelo navegador em:' \
  --msgbox "http://10.0.0.4/$dir1

```

\n\nClique com o botão direito sobre o link acima\n e então em Abrir link.\n" \

```
10 80;;
```

```

1)
  echo "Cancelado.";;
esac;;

```

```

2) clear;
# diretório do aplicativo
DIALOG=${DIALOG=dialog}
tempfile=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
trap "rm -f $tempfile" 0 1 2 5 20

```

```

  $DIALOG --title "Gerar CRUD" --clear \
  --inputbox "Digite o diretório do aplicativo\n

```

Lembre que seu diretório atual é o /var/www/html\n\n

Digite o diretório \n\nE Aguarde a criação ..." 14 80 2> \$tempfile

```

retval=$?
diretorio=`cat $tempfile`

```

```

# tabela para gerar o crud
DIALOG=${DIALOG=dialog}
tempfile2=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
trap "rm -f $tempfile2" 0 1 2 5 20

```

```
$DIALOG --title "Gerar CRUD" --clear \
--inputbox "Digite o nome da tabela\n" 14 80 2> $tempfile2
```

```
retval=$?
tabela=`cat $tempfile2`
```

```
case $retval in
0)
    cd $diretorio
    bin/cake bake all $tabela;
    dialog \
    --title 'Gerar CRUD' \
    --msgbox "Código Gerado. Confira abrindo no navegador\n" \
    10 80;;
1)
    echo "Cancelado.";;
255)
esac;;
```

```
3) clear;
DIALOG=${DIALOG=dialog}
tempfile=`tempfile 2>/dev/null` || tempfile=/tmp/test$$
trap "rm -f $tempfile" 0 1 2 5 20
```

```
$DIALOG --title "Atualização de Aplicativo com o Composer" --clear \
--inputbox "Digite o diretório do aplicativo\n
Lembre que seu diretório atual é o /var/www/html\n\n
Digite e Aguarde a atualização ..." 14 80;;
```

```
4) clear;
echo "== Diretório do Aplicativo ==";
echo "";
echo "Digite o diretório do aplicativo e aperte qualquer tecla para continuar";
echo "Somente a partir de '/var/www/html.'.";
echo "Exemplo: para '/var/www/html/teste', digite apenas 'teste' e tecla Enter.";
echo "";
echo "";
read DIR
/var/www/html/$DIR/bin/cake;
echo "Veja a versão acima em 'Welcome to CakePHP v'. Aperte qualquer tecla
para voltar."
```

```
read n;;
5) clear;
# Antes adicionar todos os desenvolvedores ao sudo sem senha
echo '== Corrigir erro de permissão em aplicativo ==';
echo ";
echo 'Digite o diretório do aplicativo. Lembre que é relativo.';
echo "Para '/var/www/html/modelos/aplicativo1', digite apenas
'modelos/aplicativo1' e tecla Enter.";
echo ";
echo ";
```

```

        read APP;
        sudo perms $APP;
        echo "Permissões corrigidas. Acesse o navegador e atualize com F5. Aperte
qualquer tecla para voltar."
        read n;;
    0) clear;
        exit;;
    esac
done

```

pgback.sh – script para efetuar backup de banco do postgresql

```

#!/bin/sh
#/usr/local/sbin/pgback.sh

# Adaptado de - http://www.sertoriopen.com.br/?p=55

# Documentação: https://www.postgresql.org/docs/9.3/static/app-pgdump.html
# Uso: pgback.sh nomebanco nomeesquema

if [ "$1" = "-h" ] || [ "$1" = "--help" ] || [ -z "$1" ]
then
    echo "Sintaxe correta:\n\npgback.sh banco [esquema] [tabela]"
    exit 1
fi

DATA=`/bin/date +%d-%m-%Y`

# diretório de backup
DIR="/backup/pg_backup/"

if [ ! -d "$DIR" ]
then
    mkdir -p "$DIR"
fi

ARQUIVO="$DIR$1-$2-$DATA.sql"
#echo $ARQUIVO;

# variáveis
HOST="localhost"
USER="postgres"
export PGPASSWORD="postgres"

# backup
# --no-owner = sem owner, --inserts = com inserts, -Fp = customizado com plain text,
# Customizado permite restore de apenas uma tabela, ou um esquema
# $1 - nome do banco, $2 - nome do esquema, -t = tabela

```

```

if [ ! -z $3 ]
then
  /usr/bin/psql -U $USER -c "alter user postgres set search_path to "$2
  /usr/bin/pg_dump -h $HOST -U $USER -n $2 -t $3 --no-owner --inserts -Fp $1 -f
$ARQUIVO
  gzip -9 $ARQUIVO
  exit 1
elif [ ! -z $2 ]
then
  /usr/bin/psql -U $USER -c "alter user postgres set search_path to "$2
  /usr/bin/pg_dump -h $HOST -U $USER -n $2 --no-owner --inserts -Fp $1 -f $ARQUIVO
  gzip -9 $ARQUIVO
  exit 1
else
  /usr/bin/pg_dump -h $HOST -U $USER --no-owner --inserts -Fp $1 -f $ARQUIVO
  gzip -9 $ARQUIVO
fi

```

mint_lamp72.sh – script com a dialog para instalação do LAMP em desktop Mint

```

#!/bin/bash
#
# Criado/adaptado por Ribamar FS - http://ribafs.org
#
apt-get install dialog;
#
while :
do
  clear
servico=$(dialog --stdout --backtitle 'Instalação de pacotes no Ubuntu Server 16.04 LTS -
64' \
  --menu 'Selecione a opção com a seta ou o número e tecle Enter\n' 0 0 0 \
  1 'Atualizar repositórios' \
  2 'Instalar LAMP e outros' \
  0 'Sair' )
  case $servico in
    1) apt-get update;;
    2) clear;
# "Instalar pacotes básicos. Tecla Enter para instalar!";
apt-get -y install apache2 libapache2-mod-php7.2 aptitude git mc;

# "Instalar Apache e módulos. Tecla Enter para instalar!";

a2dismod php7.2;
a2enmod rewrite;

# Instalar SGBDs somente para testes locais. Visto que o servidor é outro: 10.0.0.60
debconf-set-selections <<< 'mysql-server mysql-server/root_password password root';

```

```
debconf-set-selections <<< 'mysql-server mysql-server/root_password_again password
root';

apt-get -y install mysql-server postgresql;

# "Instalar PHP 7 e extensões. Tecla Enter para instalar!";
apt-get -y install php7.2-bcmath php7.2-mcrypt php7.2-gd php7.2-mysql php7.2-pgsql;
apt-get -y install php-pear php7.2-xml php7.2-xsl curl php7.2-curl phpunit php-xdebug
php7.2-intl composer;
apt-get -y install php7.2-zip php7.2-mbstring php-gettext php-mbstring php7.2-fpm php7.2-
sqlite3 php-redis;
phpenmod mbstring;

# "Instalar suporte a cache no PHP. Tecla Enter para instalar!";
apt-get -y install php-apcu;

wget http://ftp.ussg.iu.edu/linux/ubuntu/pool/main/m/memcached/memcached_1.4.25-
2ubuntu1_amd64.deb;
dpkg -i memcached_1.4.25-2ubuntu1_amd64.deb;
apt-get -y install php-memcache;

echo "Configurar php (display_errors = On)
date.timezone = America/Fortaleza
Aperte ENTER para abrir o php.ini";
read n;
nano /etc/php/7.0/apache2/php.ini;

echo "Desabilitar o xdebug. Comentar a linha";
read n;
nano /etc/php/7.0/mods-available/xdebug.ini
service apache2 restart;

clear;

echo "Configurar .htaccess no Apache 2.4 trocando None por All
<Directory />
    Options Indexes FollowSymLinks Includes ExecCGI
    AllowOverride All
    Order deny,allow
    Allow from all
</Directory>

ServerName localhost

Adicionar ao final:
<FilesMatch \.php$>
SetHandler application/x-httpd-php
</FilesMatch>";
echo "";
echo "";
```

```
echo "Qualuer tecla para continuar";  
read n;
```

```
nano /etc/apache2/apache2.conf;
```

```
a2dismod mpm_event;  
a2enmod mpm_prefork;  
a2enmod php7.2;
```

```
apt-get install -y alarm-clock-applet clamav clamav-daemon clamtk gparted shutter  
wireshark pgadmin3 lynis rkhunter mc nmap clonezilla partimage deborphan bleachbit  
myspell-pt-br deborphan kalgebra kig gcompris marble traceroute geogebra python3-smbc  
tff-mscorefonts-installer rar unrar zip unzip p7zip-full ubuntu-restricted-extras k3b  
kolourpaint4 gnome-search-tool shutter;
```

```
apt-get -y update;  
apt-get -y upgrade;;  
    0) clear;exit;;  
    esac  
done
```

9 – Servidores

9.1 – CentOS EMP

Projeto

Instalação do CentOS 7 com nginx, mysql 5.7 e php 7.1

IP

- Criação do servidor, com 1GB de RAM, 1 vCPU e 25GB SSD
- Configurar o DNS e apontar seu domínio para os nameservers
- Ajuste do hostname. Idealmente crie o nome do servidor como sendo o seu domínio para facilitar
- Atualização do servidor
- Reiniciar para garantir que novo kernel seja usado
- Criação de usuário comum com poderes de sudo e acesso via ssh
- Instalação do restante do LEMP
- Configuração da segurança, firewall com firewalld, melhora do ssh e outros cuidados com a segurança

Criação de um Servidor com Ubuntu 16.04 64 e LEMP no DigitalOcean

IP - 46.101.58.212

- Após criar o servidor/droplet
- Abra a droplet criada
- Clique em Access - Reset Root Password

- O acesso pelo terminal do desktop é bloqueado pelo ufw
- Acessar pela console com root e a senha recebida por e-mail
- Parar o ufw
ufw disable
- Acesse pelo terminal do seu desktop
ssh root@IP

Criar diretório de backup

```
mkdir /root/backup
```

É importante se acostumar a fazer sempre backup de scripts ou do site (banco e arquivos) antes de efetuar alterações, pois perder informações é bem ruim.

Ao acessar recebe-se o aviso alterado pela DigitalOcean

```
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-109-generic x86_64)
```

```
Thank you for using DigitalOcean's LEMP Application.
```

Your web root is located at `/var/www/html` and can be seen from
`http://46.101.58.212`

The details of your PHP installation can be seen at
`http://46.101.58.212/info.php`

The "ufw" firewall is enabled. All ports except for 22, 80, and 443 are BLOCKED

You are encouraged to run `mysql_secure_installation` to ready your server for production. The passwords for MySQL have been saved to:
`/root/.digitalocean_password`

Let's Encrypt has been pre-installed for you. If you have a domain name, and you will be using it with this 1-Click app, please see: <http://do.co/le-nginx>

You can learn more about using this image here: <http://do.co/lemp>

To delete this message of the day: `rm -rf /etc/update-motd.d/99-one-click`
Last login: Tue Mar 6 18:32:29 2018 from 177.14.224.187
`ribafs@lempub16:~$`

Para remover esta mensagem execute:
`rm -rf /etc/update-motd.d/99-one-click`

Atualizar Servidor

```
apt update
apt upgrade
reboot
```

Instalar pacotes básicos

```
apt install unzip mc aptitude
```

Criar um usuário comum

```
adduser ribafs
```

- Adicionar ao sudoers

```
cp /etc/sudoers /root/backup
nano /etc/sudoers
```

Adicione abaixo da linha com root esta linha:

```
ribafs  ALL=(ALL) NOPASSWD:ALL
```

- Adicionar o ribafs ao ssh e efetuar ajustes

```
cp /etc/ssh/sshd_config /root/backup  
nano /etc/ssh/sshd_config
```

Altere as linhas:

```
Port 55522  
LoginGraceTime 30  
PermitRootLogin no
```

Adicione ao final:

```
AllowUsers ribafs
```

```
Reiniciar o SSH  
service ssh restart
```

Acessar pelo terminal do desktop

```
ssh -p 55522 ribafs@46.101.58.212
```

Ajustes no UFW

```
ufw enable
```

```
ufw delete allow 22  
ufw allow 55522  
ufw allow http  
ufw allow https
```

```
ufw status verbose
```

Adicionar partição de swap com 2GB

```
dd if=/dev/zero of=/swapfile bs=1M count=2048  
mkswap /swapfile  
chmod 600 /swapfile  
swapon /swapfile
```

```
nano /etc/fstab  
/swapfile swap swap defaults 0 0
```

```
Testar  
free -m
```

Exportar a chave do ssh do desktop para o servidor

Acessar o servidor como ribafs e execute:

```
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_ribafs -t dsa (Enter 2 vezes)
cat ../.ssh/id_ribafs*.pub > ../.ssh/authorized_keys
chmod 600 ../.ssh/*
exit
```

Acessar o desktop

```
ssh-copy-id ribafs@ip -p porta
```

Criar script para limpar o cache da RAM

```
nano /usr/local/bin/m

sysctl -w vm.drop_caches=3
swapoff -a
swapon -a
```

```
chmod +x /usr/local/bin/m
```

Rodar como root

```
m
```

Antes de rodar o "m" havia 64 MB free
Após ficou com 709 MB.

Criar um script para configurar as permissões do /var/www/html

Adicionar ribafs ao www-data
adduser ribafs www-data

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

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

```
echo "Concluído!";
```

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

Executando no diretório /var/www/html/portal
perms portal

Executando no diretório /var/www/html
perms

Executo sempre que faço alguma alteração como root no /var/www/html

Agora vou criar o banco e instalar um site em Joomla com o arquivo
2joomla

Instalar um site em Joomla na pasta /var/www/html/portal

Instalar algumas extensões

Como o servidor LEMP criado é apenas padrão e não contém todas as extensões necessárias para um site com Joomla, então instalaremos mais algumas.

```
apt install -y php-bcmath
```

O Akeeba acusou a falta da extensão mbstring

```
apt install -y php-mbstring php-simplexml php-zip php-xml
```

```
service apache2 restart
```

Configurações no php.ini

```
nano /etc/php/7.0/apache2/php.ini
```

```
date.timezone = America/Fortaleza
```

```
service apache2 restart
```

== Enviar o arquivo portal.zip gerado pelo Akeeba Backup do desktop para a pasta /tmp do servidor

No desktop copiar os dois arquivos para a pasta /home/ribafs
scp -P porta portal* ribafs@IP:/tmp

No servidor

```
cd /tmp
```

Criar o banco e um usuário dono dele

Executar para mostrar a senha do mysql. Efetuar um duplo clique apenas sobre o que tá entra aspas

```
cat /root/.digitalocean_password
```

Execute

```
mysql_secure_installation
```

Quando ele mostrar:

```
Enter password for user root:
```

Efetue o duplo clique sobre a senha e apenas tecele Shift+Insert

Veja minhas respostas resumidas que foram praticamente todas y, exceto a primeira que foi n

```
root@lamp-ub:/tmp# mysql_secure_installation
```

```
Securing the MySQL server deployment.
```

```
Enter password for user root:
```

```
VALIDATE PASSWORD PLUGIN can be used to test passwords
```

```
...
```

```
Press y|Y for Yes, any other key for No: n
```

```
Change the password for root ? ((Press y|Y for Yes, any other key for No) : y
```

```
New password:
```

```
Re-enter new password:
```

```
Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
```

```
Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
```

```
Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
```

```
Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
```

```
All done!
```

Criar o banco de dados do site e um usuário para o mesmmo

```
mysql -uroot -p
```

```
create database portal;
```

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'  
WITH GRANT OPTION;  
\q
```

Descompactar o arquivo

```
unzip portal.zip -d /var/www/html/portal
```

Setar corretamente as permissões
perms portal

Efetuar ajustes no /var/www/html/portal/configuration.php se necessário.

Instalar o restore do Akeeba

http://IP

Lembre de desabilitar o SSL caso esteja habilitado, visto que ainda não habilitamos o SSL neste servidor.

Melhorando a segurança do site em Joomla

Para melhorar a segurança vamos mover o configuration.php para a pasta /var/www e com nome cfg.php

```
mv /var/www/html/portal/configuration.php /var/www/cfg.php
```

Em seu lugar criemos um arquivo apenas com um require para ele
nano /var/www/html/portal/configuration.php

```
<?php  
require_once( dirname( __FILE__ ) . '/../..'/cfg.php' );
```

Configurando o Apache para mod_rewrite

```
nano /etc/apache2/apache2.conf
```

Onde tem None abaixo mudar para All

```
<Directory />  
    Options FollowSymLinks  
    AllowOverride All  
    Require all denied  
</Directory>
```

```
<Directory /usr/share>  
    AllowOverride All
```

```
    Require all granted
</Directory>
```

```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

Salvar e habilitar

```
a2enmod rewrite
```

Alterar o php.ini

```
Display_errors = Off
output_buffering = Off
```

```
service apache2 restart
```

Testando

```
http://IP/portal
```

Apareceu normalmente o site.

Editei o php.ini

```
nano /etc/php/7.0/apache2/php.ini
```

E mudei o display_errors para Off

Após reiniciar o Apache

```
service apache2 restart
```

Redirecionar acesso ao raiz para /portal

Removi index.html e info.php do raiz

```
nano /var/www/html/index.php
```

```
<?php
header('location: portal');
```

Depois de testado o site e configurado novamente para proteger o administrador com SSL então efetuar um backup full com o Akeeba Backup para guardar.

Backup e Restore

Agora faça um backup completo com o akeeba e quando terminar restaure por exemplo para a pasta
/var/www/html/portal2

Crie o banco portal2, pode ser o mesmo user e senha

Restaure pela web:

http://IP/portal2

Agora vou implementar o SSL para usar no administrator usando o arquivo

3ssl_nginx

Aplicando SSL ao Nginx

Para ocultar cabeçalhos do nginx
nano /etc/nginx/nginx.conf

```
http {
...
    # Descomentar a linha abaixo
    server_tokens off;
...
}
```

service nginx restart

mkdir /etc/nginx/ssl/

```
openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout
/etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt
```

Responda às perguntas:

Country Name (2 letter code) [XX]:BR
 State or Province Name (full name) []:Ceará
 Locality Name (eg, city) [Default City]:Fortaleza
 Organization Name (eg, company) [Default Company Ltd]:FreeLancer
 Organizational Unit Name (eg, section) []:Free
 Common Name (eg, your name or your server's hostname) []:ribafs.org
 Email Address []:ribafs@gmail.com

ls /etc/nginx/ssl/nginx.crt

```
openssl dhparam -out /etc/nginx/ssl/dhparam.pem 4096
```

This is going to take a long time
Aguarde um bom tempo...

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

Adicione para o bloco server inicial

```
server {
    ...
    server_name IP; # ou ribafs.org www.ribafs.org

    ### SSL Config
    listen 443 ssl;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/ssl/dhparam.pem;
    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;

    if ($request_method !~ ^(GET|HEAD|POST)$ )
    {
        return 405;
    }

    ...
}
```

Proteção contra ataques Clickjacking
nano /etc/nginx/nginx.conf

Adicionar ao bloco http
add_header X-Frame-Options "SAMEORIGIN";

```
service nginx restart
```

Testar

```
https://IP
```

```
https://IP/administrator
```

Logs

Em caso de problema ver logs

```
tail -f /var/log/nginx/error.log
```

Agora proteger diretório administrador com senha usando o arquivo

```
4senha_diretorio
```

Proteger diretório com senha pelo Nginx

Instalar

```
apt install apache2-utils
```

```
htpasswd -c /etc/nginx/.htpasswd ribafs
```

```
cat /etc/nginx/.htpasswd
```

Editar o arquivo do site default e alterar assim deixando como abaixo:

```
nano /etc/nginx/sites-available/ribafs.conf
```

```
server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /var/www/html;
    index index.php index.html index.htm;

    auth_basic "Área Restrita";
    auth_basic_user_file /etc/nginx/.htpasswd;

    # Make site accessible from http://localhost/
    server_name 46.101.58.212;

    ### SSL Config
    listen 443 ssl;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/ssl/dhparam.pem;
    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;

    if ($request_method !~ ^(GET|HEAD|POST)$ )
    {
        return 405;
    }

    location / {
        auth_basic off;
```

```

    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    #try_files $uri $uri/ =404;
    try_files $uri $uri/ /portal/index.php?$args;
    # Uncomment to enable naxsi on this location
    # include /etc/nginx/naxsi.rules
}

error_page 404 /404.html;
error_page 500 502 503 504 /50x.html;
location = /50x.html {
    root /usr/share/nginx/html;
}

#Adicionar para o administrator, para que somente meus dois IPs possam acessar
location /portal/administrator/ {
    auth_basic "Restrito";
    auth_basic_user_file /etc/nginx/.htpasswd;
}

location ~ /\.php$ {
    auth_basic off;
    include snippets/fastcgi-php.conf;
    fastcgi_pass unix:/run/php/php7.0-fpm.sock;
}

# deny access to .htaccess files, if Apache's document root
# concurs with nginx's one
#
#location ~ /\.ht {
#    deny all;
#}
}

```

Reiniciar o nginx
 service nginx restart

Testar:

<https://IP/administrator>

Precisei entrar com login e senha duas vezes mas funcionou.

Crédito

<https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/>

Agora vou efetuar uma nova cópia dos scripts de configuração para a pasta /root/backup

cd /root/backup

```
tar czpvf lempub1604.tar.gz *
cp ub1604lemp.tar.gz /home/ribafs
chown ribafs /home/ribafs/ub1604lemp.tar.gz
```

No desktop

```
scp -P porta ribafs@IP:/home/ribafs/ub1604* .
```

Guardar bem estes scripts para em caso de alteração com problema poder restaurar.

Subdomínio

Caso haja a necessidade de adicionar um subdomínio

Adicionar um Subdomínio

Para criar um subdomínio chamado php

Criar o Virtual Host no Apache

```
mkdir /var/www/html/php
cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/php.conf
nano /etc/apache2/sites-available/php.conf
```

Adicione logo abaixo da linha com ServerAdmin:

```
DocumentRoot /var/www/html/php
ServerName php.ribafs.org
```

```
a2ensite php
```

```
service apache2 restart
```

Criar arquivo para teste:

```
nano /var/www/html/php/index.html
<h1>Curso de PHP</h1>
```

Adicione registro CNAME ao DNS

| Type | Hostname | Value | TTL |
|-------|----------------|-------------|-------|
| CNAME | php.ribafs.org | ribafs.org. | 43200 |

O site deve ficar na pasta /var/www/html/php

9.2 – CentOS LAMP

Criação de um Servidor na DigitalOcean

Claro que este servidor pode ser criado em qualquer hospedagem e até em seu server particular.

Tipo One-click-apps

LAMP on 16.0

1GB

London

lamp-ub

159.65.93.252

1 GB Memory / 25 GB Disk / LON1 - Ubuntu LAMP on 16.04

Associei a uma chave SSH que havia criado no trabalho

Como associei o servidor a uma chave, não sei porque, mas ele não permitiu o acesso do meu desktop via ssh, mostrando a mensagem:

```
ssh root@159.65.89.220
```

```
The authenticity of host '159.65.89.220 (159.65.89.220)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:Z+EL5v6LJZ31PEBpHMPNvbWk9p813GP4CN/G9IMevSo.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '159.65.89.220' (ECDSA) to the list of known hosts.
```

```
Permission denied (publickey).
```

Então destruí o servidor e criei outro semelhante mas sem a chave

Após criar o servidor o DO envia um e-mail com um link para LAMPs:

[https://www.digitalocean.com/community/tags/lamp-stack?](https://www.digitalocean.com/community/tags/lamp-stack?utm_source=Customerio&utm_medium=Email_Internal&utm_campaign=Email_LAMPWelcome&mkt_tok=eyJpIjoiTWpReVpqWmpNV1kxWWpjNSIsInQiOiJESmRUbXVqVWhQOEdbzVaZXNydkNNRUJIME9XSzRhTXhqMFB6UCs2RTVvb0Vja1wvVGpoMnJiVEh1M0lnbjRMK2FNZkFBbzQxZlZzS1FhXC9oakdQdHZjS3RcL2RITVRkZUxxZ3g1dFFxOVlcL2VxY2RXYVdac2tOaDV6TjhhUzE0WnMifQ%3D%3D)

https://www.digitalocean.com/community/tags/lamp-stack?utm_source=Customerio&utm_medium=Email_Internal&utm_campaign=Email_LAMPWelcome&mkt_tok=eyJpIjoiTWpReVpqWmpNV1kxWWpjNSIsInQiOiJESmRUbXVqVWhQOEdbzVaZXNydkNNRUJIME9XSzRhTXhqMFB6UCs2RTVvb0Vja1wvVGpoMnJiVEh1M0lnbjRMK2FNZkFBbzQxZlZzS1FhXC9oakdQdHZjS3RcL2RITVRkZUxxZ3g1dFFxOVlcL2VxY2RXYVdac2tOaDV6TjhhUzE0WnMifQ%3D%3D

Um link sobre um LAMP

[https://www.digitalocean.com/community/tutorials/how-to-launch-your-site-on-a-new-ubuntu-14-04-server-with-lamp-sftp-and-dns?](https://www.digitalocean.com/community/tutorials/how-to-launch-your-site-on-a-new-ubuntu-14-04-server-with-lamp-sftp-and-dns?utm_source=Customerio&utm_medium=Email_Internal&utm_campaign=Email_LAMPWelcome&mkt_tok=eyJpIjoiTWpReVpqWmpNV1kxWWpjNSIsInQiOiJESmRUbXVqVWhQOEdbzVaZXNydkNNRUJIME9XSzRhTXhqMFB6UCs2RTVvb0Vja1wvVGpoMnJiVEh1M0lnbjRMK2FNZkFBbzQxZlZzS1FhXC9oakdQdHZjS3RcL2RITVRkZUxxZ3g1dFFxOVlcL2VxY2RXYVdac2tOaDV6TjhhUzE0WnMifQ%3D%3D)

https://www.digitalocean.com/community/tutorials/how-to-launch-your-site-on-a-new-ubuntu-14-04-server-with-lamp-sftp-and-dns?utm_source=Customerio&utm_medium=Email_Internal&utm_campaign=Email_LAMPWelcome&mkt_tok=eyJpIjoiTWpReVpqWmpNV1kxWWpjNSIsInQiOiJESmRUbXVqVWhQOEdbzVaZXNydkNNRUJIME9XSzRhTXhqMFB6UCs2RTVvb0Vja1wvVGpoMnJiVEh1M0lnbjRMK2FNZkFBbzQxZlZzS1FhXC9oakdQdHZjS3RcL2RITVRkZUxxZ3g1dFFxOVlcL2VxY2RXYVdac2tOaDV6TjhhUzE0WnMifQ%3D%3D

Um link para efetuar perguntas

https://www.digitalocean.com/community/questions/new?utm_source=Customerio&utm_medium=Email_Internal&utm_campaign=Email_LAMPWelcome&mkt_tok=eyJpIjoiTWpReVpqWmpNV1kxWWpjNSIsInQiOiJESmRUbXVqVWVhQOEEdNbzVaZXNydkNNRUJIME9XSzRhTXhqMFB6UCs2RTVvb0Vja1wvVGpoMnJiVEh1M0InbjRMK2FNZkFBbzQxZlZzS1FhXC9oakdQdHZjS3RcL2RITVRkZUxxZ3g1dFFxOVlcL2VxY2RXYVdac2tOaDV6TjhhUzE0WnMifQ%3D%3D

Citando outros

How To Create Your First DigitalOcean Droplet

<https://www.digitalocean.com/community/tutorials/how-to-create-your-first-digitalocean-droplet>

Initial Server Setup with Ubuntu 14.04

<https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-14-04>

How To Install Linux, Apache, MySQL, PHP (LAMP) stack on Ubuntu 14.04

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu-14-04>

How To Set Up a Host Name with DigitalOcean

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-host-name-with-digitalocean>

An Introduction to DNS Terminology, Components, and Concepts

<https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts>

How To Use SFTP to Securely Transfer Files with a Remote Server

<https://www.digitalocean.com/community/tutorials/how-to-use-sftp-to-securely-transfer-files-with-a-remote-server>

How To Use Filezilla to Transfer and Manage Files Securely on your VPS

<https://www.digitalocean.com/community/tutorials/how-to-use-filezilla-to-transfer-and-manage-files-securely-on-your-vps>

How To Install Wordpress on Ubuntu 14.04

<https://www.digitalocean.com/community/tutorials/how-to-install-wordpress-on-ubuntu-14-04>

Outros Tutriais

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

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

- Após criar o servidor/droplet
- Abra a droplet criada
- Clique em Access - Reset Root Password

- O acesso pelo terminal do desktop é bloqueado pelo ufw

- Acessar pela console com root e a senha recebida por e-mail

Veja que ele mostra avisos importantes:

- Os pacotes estão todos atualizados
- O site já está no ar:
<http://159.65.93.252>
- O arquivo em PHP:
<http://159.65.93.252/info.php>
- O ufw está habilitando e bloqueando todas as portas, exceto a 22, 80 e 443
- Recomenda proteger o mysql com `mysql_secure_installation` e que a senha do mysql está no arquivo:

`/root/.digitalocean_password`

- Diz que o Let's Encrypt foi pré-instalado. Sugere <http://do.co/le-apache>
- Sugere How To Install Linux, Apache, MySQL, PHP (LAMP) stack on Ubuntu 14.04
<http://do.co/lamp1404>
- Para remover este aviso execute:
`rm -rf /etc/update-motd.d/99-one-click`

Parar temporariamente o UFW

- Parar o ufw
`ufw disable`
- Acesse pelo terminal do seu desktop
`ssh root@IP`

Testar pela web

<http://159.65.93.252>

Criar diretório de backup

`mkdir /root/backup`

É importante se acostumar a fazer sempre backup de scripts ou do site (banco e arquivos) antes de efetuar alterações, pois perder informações é bem ruim.

Ao acessar recebe-se o aviso alterado pela DigitalOcean

Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-109-generic x86_64)

Thank you for using DigitalOcean's LEMP Application.

Your web root is located at /var/www/html and can be seen from
<http://46.101.58.212>

The details of your PHP installation can be seen at
<http://46.101.58.212/info.php>

The "ufw" firewall is enabled. All ports except for 22, 80, and 443 are BLOCKED

You are encouraged to run `mysql_secure_installation` to ready your server for production. The passwords for MySQL have been saved to:
`/root/.digitalocean_password`

Let's Encrypt has been pre-installed for you. If you have a domain name, and you will be using it with this 1-Click app, please see: <http://do.co/le-nginx>

You can learn more about using this image here: <http://do.co/lemp>

To delete this message of the day: `rm -rf /etc/update-motd.d/99-one-click`

Last login: Tue Mar 6 18:32:29 2018 from 177.14.224.187

`ribafs@lempub16:~$`

Para remover esta mensagem execute:

`rm -rf /etc/update-motd.d/99-one-click`

Criar diretório de backup para scripts

`mkdir /root/backup`

Copiar inicialmente todos os scripts importantes de configuração para esta pasta:

`cd /root/backup`

`cp /etc/php/7.0/apache2/php.ini .`

`cp /etc/apache2/apache2.conf .`

`cp /etc/apache2/sites-available/000-default.conf .`

`cp /etc/apache2/sites-available/default-ssl.conf .`

Ao final, após tudo configurado, instalado e o site instalado então efetuar novamente o backup dos scripts mas com prefixo OH

`cd /root/backup`

`cp /etc/php/7.0/apache2/php.ini OKphp.ini`

`cp /etc/apache2/apache2.conf OKapache2.conf`

`cp /etc/apache2/sites-available/000-default.conf OK000-default.conf`

`cp /etc/apache2/sites-available/default-ssl.conf OKdefault-ssl.conf`

Em caso de algum problema e se perder o controle podemos restaurar o respectivo script.

Instalar pacotes básicos

```
apt install unzip mc aptitude
```

Criar um usuário comum

```
adduser ribafs
```

- Adicionar ao sudoers

```
cp /etc/sudoers /root/backup  
nano /etc/sudoers
```

Adicione abaixo da linha com root esta linha:

```
ribafs ALL=(ALL) NOPASSWD:ALL
```

- Adicionar o ribafs ao ssh e efetuar ajustes

```
cp /etc/ssh/sshd_config /root/backup  
nano /etc/ssh/sshd_config
```

Altere as linhas:

```
Port 55522  
LoginGraceTime 30  
PermitRootLogin no
```

Adicione ao final:

```
AllowUsers ribafs
```

```
Reiniciar o SSH  
service ssh restart
```

Acessar pelo terminal do desktop

```
ssh -p 55522 ribafs@159.65.93.252
```

Ajustes no UFW

```
ufw enable
```

```
ufw delete limit in 22  
ufw allow 55522  
ufw allow http  
ufw allow https
```

```
ufw status verbose
```

Adicionar partição de swap com 2GB

```
dd if=/dev/zero of=/swapfile bs=1M count=2048
mkswap /swapfile
chmod 600 /swapfile
swapon /swapfile
```

```
nano /etc/fstab
/swapfile swap swap defaults 0 0
```

Testar
free -m

Exportar a chave do ssh do desktop para o servidor

Acessar o servidor como ribafs e execute:

```
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_ribafs -t dsa (Enter 2 vezes)
cat ../.ssh/id_ribafs*.pub > ../.ssh/authorized_keys
chmod 600 ../.ssh/*
exit
```

Acessar o desktop

```
ssh-copy-id ribafs@ip -p porta
```

Criar script para limpar o cache da RAM

```
nano /usr/local/bin/m

sysctl -w vm.drop_caches=3
swapoff -a
swapon -a
```

```
chmod +x /usr/local/bin/m
```

Executar com root
m

Antes de rodar o "m" havia 64 MB free
Após ficou com 709 MB.

Criar um script para configurar as permissões do /var/www/html

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

```
#!/bin/sh  
clear;  
echo "Aguarde enquanto configuro as permissões do /var/www/html/$1";  
echo "";  
chown -R www-data:www-data /var/www/html/$1;  
find /var/www/html/$1 -type d -exec chmod 755 {} \;  
find /var/www/html/$1 -type f -exec chmod 654 {} \;  
echo "";  
echo "Concluído!";
```

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

Executando no diretório /var/www/html/portal
perms portal

Executando no diretório /var/www/html
perms

Executo sempre que faço alguma alteração como root no /var/www/html

Agora vou criar o banco e instalar um site em Joomla com o arquivo
2joomla

Instalar um site em Joomla na pasta /var/www/html/portal

Instalar algumas extensões

Como o servidor LEMP criado é apenas padrão e não contém todas as extensões necessárias para um site com Joomla, então instalaremos mais algumas.

```
apt install php-bcmath
```

O Akeeba acusou a falta da extensão mbstring

```
apt install php-mbstring
```

```
service nginx restart  
service php7.0-fpm restart
```

Mais acusadas pelo Akeeba no restore

```
apt install php-zip
```

Enviar os arquivos portal.zip e portal.sql para a pasta /tmp do servidor

No desktop copiar os dois arquivos para a pasta /home/ribafs
scp -P porta portal* ribafs@IP:/tmp

No servidor
cd /tmp

Criar o banco e um usuário dono dele

```
mysql -uroot -p
create database portal;
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'
WITH GRANT OPTION;
\q
mysql -uroot -p portal < portal.sql
```

Descompactar os arquivos

```
unzip portal.zip -d /var/www/html/portal
perms portal
```

Para melhorar a segurança vamos mover o configuration.php para a pasta /var/www e com nome cfg.php

```
mv /var/www/html/portal/configuration.php /var/www/cfg.php
```

Em seu lugar criemos um arquivo apenas com um require para ele
nano /var/www/html/portal/configuration.php

```
<?php
require_once( dirname( __FILE__ ) . '/../../cfg.php' );
```

Mudar site disponível

Quando criamos um servidor com Ubuntu 16.04 tipo LEMP no DigitalOcean o default site-available/site-enabled chama-se digitalocean

Quero renomear para ribafs.conf
Como fazer isso?

Renomear arquivo para ribafs.conf
mv /etc/nginx/sites-available/digitalocean /etc/nginx/sites-available/ribafs.conf

Remover o link simbólico de
rm /etc/nginx/sites-enabled/digitalocean

Criar o ribafs.conf

```
cd /etc/nginx/sites-enabled  
ln -s /etc/nginx/sites-available/riabafs.conf .
```

```
service nginx restart
```

Testando

http://IP/portal

Apareceu simplesmente na tela
Error

Editei o php.ini
nano /etc/php/7.0/fpm/php.ini

E mudei o display_errors para On

E
timezone para
timezone America/Fortaleza

```
output_buffering = Off
```

Após reiniciar o nginx
service nginx restart/
service php7.0-fpm restart/

Continuou a mensagem

Então reiniciei o php-fpm
service php7.0-fpm restart

Agora apareceu o erro
Error: Call to undefined function Joomla\CMS\Language\simplexml_load_file(): Call to undefined function Joomla\CMS\Language\simplexml_load_file()

Então instalei a extensão:
aptitude install php7.0-simplexml

```
service nginx restart  
service php7.0-fpm restart
```

Agora o site apareceu.

Mas ao clicar num dos links do site aparece o erro 404

OK. Então basta adicionar uma linha ao bloco location /

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

O bloco estava assim:

```
location / {
    try_files $uri $uri/ =404;
}
```

Como o site está na pasta portal, mudei para isso:

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

```
service nginx restart
```

Agora ao clicar nos links funciona.

Erro ao acessar o administrator

Quando fui abrir o administrator ele não encontra a página. Percebi que havia deixado o administrator forçando SSL e como ainda não instalei o SSL não funciona.

Então editei

```
nano /usr/share/nginx/html/configuration.php
```

E alterei a linha abaixo para 0

```
public $force_ssl = '0';
```

Agora acessei normalmente o administrator.

Redirecionar acesso ao raiz para /portal

Removi index.html e info.php do raiz

```
nano /var/www/html/index.php
```

```
<?php
header('location: portal');
```

Depois de testado o site e configurado novamente para proteger o administrator com SSL então efetuar um backup full com o Akeeba Backup para guardar.

Alerta do Akeeba

A Akeeba faz um alerta sobre o diretório media/com_akeeba

WARNING

Akeeba Backup could not determine the permissions of the media/com_akeeba directory.

Please do one of the following:

Activate Joomla!'s FTP mode in Global Configuration

Change the permissions of the media/com_akeeba directory and all of its subdirectories to 0755 and all of its files to 0644 using your FTP client.

Akeeba Backup will most likely not work at all if you do not perform these steps. Do not ask for support if you can see this message. All the information you need is already on this message.

Mas não há problema aqui. O que acontece é que as permissões concedidas para todos os

diretórios é de 775
arquivos é de 664

E ele espera 755 e 644, mas funciona sem problema.

Backup e Restore

Agora faça um backup completo com o akeeba e quando terminar restaure por exemplo para a pasta
/var/www/html/portal2

Crie o banco portal2, pode ser o mesmo user e senha

Restaure pela web:

http://IP/portal2

Agora vou implementar o SSL para usar no administrador usando o arquivo

3ssl_nginx

Aplicando SSL ao Apache

a2enmod ssl

```
service apache2 restart
```

```
mkdir /etc/apache2/ssl
```

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
```

Responda às perguntas:

```
Country Name (2 letter code) [XX]:BR
State or Province Name (full name) []:Ceará
Locality Name (eg, city) [Default City]:Fortaleza
Organization Name (eg, company) [Default Company Ltd]:FreeLancer
Organizational Unit Name (eg, section) []:Free
Common Name (eg, your name or your server's hostname) []:ribafs.org
Email Address []:ribafs@gmail.com
```

```
nano /etc/apache2/sites-available/default-ssl.conf
```

Remover todo o conteúdo e deixar somente:

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin ribafs@gmail.com
    ServerName 159.65.93.252 #ribafs.org
    #ServerAlias www.ribafs.org
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
    <FilesMatch "\.(cgi|shtml|phtml|php)$">
      SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
      SSLOptions +StdEnvVars
    </Directory>
    BrowserMatch "MSIE [2-6]" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
    BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
  </VirtualHost>
</IfModule>
```

```
a2ensite default-ssl.conf
```

```
service apache2 restart
```

Testar

`https://IP/administrator`

Agora proteger diretório administrator com senha usando o arquivo

`4senha_diretorio`

Referências

<https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-ubuntu-14-04>

Proteger diretório com senha pelo Nginx

```
htpasswd -c /etc/apache2/.htpasswd ribafs
cat /etc/apache2/.htpasswd
```

Editar o arquivo do site default e alterar assim deixando como abaixo:

```
nano /etc/apache2/sites-available/000-default.conf
```

Adicione ao final do arquivo, antes de `</VirtualHost>`

```
<Directory "/var/www/html">
  AuthType Basic
  AuthName "Restricted Content"
  AuthUserFile /etc/apache2/.htpasswd
  Require valid-user
</Directory>
```

Para que fique assim

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined

  <Directory "/var/www/html/portal/administrator">
    AuthType Basic
    AuthName "Acesso Restritot"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
  </Directory>
</VirtualHost>
```

Testar sintaxe
 apache2ctl configtest

Agora abra o default-ssl.conf

nano /etc/apache2/sites-available/default-ssl.conf

Adicione ao final do arquivo, antes de </VirtualHost>

```
<Directory "/var/www/html">
  AuthType Basic
  AuthName "Restricted Content"
  AuthUserFile /etc/apache2/.htpasswd
  Require valid-user
</Directory>
```

Para que fique assim

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin ribafs@gmail.com
    ServerName 159.65.93.252
    #ServerAlias www.ribafs.org
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
    <FilesMatch "\.(cgi|shtml|phtml|php)$">
      SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
      SSLOptions +StdEnvVars
    </Directory>
    BrowserMatch "MSIE [2-6]" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
    BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
  <Directory "/var/www/html/portal/administrator">
    AuthType Basic
    AuthName "Acesso Restritot"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
  </Directory>
</VirtualHost>
</IfModule>
```

Reiniciar o Apache
service apache2 restart

Adicionar o ServerName

```
nano /etc/apache2/apache2.conf
```

Adicionar a linha

```
ServerName localhost
```

Testar:

```
https://IP/administrator
```

Precisei entrar com login e senha duas vezes mas funcionou.

Crédito

<https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/>

Agora vou efetuar uma nova cópia dos scripts de configuração para a pasta /root/backup

```
cd /root/backup  
cp /etc/php/7.0/apache2/php.ini OKphp.ini  
cp /etc/apache2/apache2.conf OKapache2.conf  
cp /etc/apache2/sites-available/000-default.conf OK000-default.conf  
cp /etc/apache2/sites-available/default-ssl.conf OKdefault-ssl.conf
```

```
cd /root/backup  
tar czpvf ublamp1604.tar.gz *  
cp ublamp1604.tar.gz /home/ribafs  
chown ribafs /home/ribafs/ublamp1604.tar.gz
```

No desktop

```
scp -P porta ribafs@IP:/home/ribafs/ub1604* .
```

Guardar bem estes scripts para em caso de alteração com problema poder restaurar.

Em caso de algum problema e se perder o controle podemos restaurar o respectivo script.

```
htpasswd -c /etc/apache2/.htpasswd ribafs
```

Alterar a configuração do site default

```
sudo nano /etc/apache2/sites-enabled/000-default.conf
```

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/html/portal/administrator">
        AuthType Basic
        AuthName "Acesso Restrito"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>
```

```
service apache2 restart
```

Caso use SSL também deve adicionar

```
<Directory "/var/www/html/portal/administrator">
    AuthType Basic
    AuthName "Acesso Restrito"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
</Directory>
```

Ao seu script de configuração

Para dar suporte aos .htaccess:

```
sudo nano /etc/apache2/apache2.conf
```

```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

Salve e feche

Add .htaccess file to protect folder:

```
nano /var/www/html/.htaccess
```

```
# Add the following
AuthType Basic
AuthName "Restricted Content"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
```

```
service apache2 restart
```

<https://askubuntu.com/questions/879409/how-to-create-protect-folder-in-ubuntu-server-16-04#879435>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-password-authentication-with-apache-on-ubuntu-14-04>

Firewalld

Firewalld

```
sudo su
```

```
firewall-cmd --state
```

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

```
firewall-cmd --zone=public --permanent --add-service=http
firewall-cmd --zone=public --permanent --add-service=https
firewall-cmd --zone=public --permanent --remove-service=ssh
firewall-cmd --zone=public --permanent --add-rich-rule='rule family="ipv4" source
address="177.CASA.IP" port port="65522" protocol="tcp" accept'
firewall-cmd --zone=public --permanent --add-rich-rule='rule family="ipv4" source
address="177.14.224.187" port port="65522" protocol="tcp" accept'
```

```
firewall-cmd --zone=public --permanent --list-services
```

```
firewall-cmd --reload
systemctl restart firewalld.service
```

```
firewall-cmd --zone=public --remove-port=65522/tcp --permanent
```

SSHGuard no CentOS

SSHGuard – Block Brute Force Attack in RHEL/CentOS 7.x
<https://lintut.com/sshguard-block-brute-force-attack-on-rhel-centos/>

by Rasho · 07/12/2014

SSHGuard is an intrusion prevention system written in C language. SSHGuard parses server logs, determines malicious activity, and then bans malicious users via firewall rules. SSHGuard protects many services out of the box:

sshd

```
rpm -ivh https://centos.pkgs.org/7/lux/sshguard-2.1.0-1.el7.lux.x86_64.rpm.html
```

Criar novo chain para o SSHGuard no iptables

```
iptables -N sshguard
```

Bloquear todo o tráfico de abusos

```
iptables -A INPUT -j sshguard
```

Bloquear outros serviços

```
iptables -A INPUT -m multiport -p tcp --destination-ports 22 -j sshguard
```

Salvar as regras

```
service iptables save
```

Mais informações em

<http://www.sshguard.net/>

9.3 – Debian com LEMP

Instalação e Configuração de Servidor Linux
 Usando Debian 9.4 64 bit
 Servidor da DigitalOcean
 5 \$/mês

IP do Servidor - 138.68.176.116
 IP do trabalho - 177.14.224.187

No desktop

ssh root@138.68.176.116

Ajustes niciais

```
df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            488M   0 488M   0% /dev
tmpfs           100M  3.1M  97M   4% /run
/dev/vda1       25G  953M  23G   4% /
tmpfs           499M   0 499M   0% /dev/shm
tmpfs           5.0M   0 5.0M   0% /run/lock
tmpfs           499M   0 499M   0% /sys/fs/cgroup
tmpfs           100M   0 100M   0% /run/user/0
```

free -m

```
free -m
total      used      free     shared  buff/cache   available
Mem:      996        32      882         3         82        852
Swap:      0          0         0
```

IP do Servidor - 138.68.176.116
 IP do trabalho - 177.14.224.187

Atualizar

```
apt update
apt upgrade -y
reboot
```

Enviar do desktop para o servidor em /tmp script **debian9_lemp.sh (ao final)**

E executar

```
no servidor
cd /tmp
```

```
sh debian9_1emp.sh
```

Testar

```
http://138.68.176.116
```

Após instalar rodar:

```
mysql_secure_installation
```

Enter na primeira pergunta e adicione uma senha ao root.

```
service php7.0-fpm restart
service nginx restart
service mysql restart
```

Fuso horário

```
dpkg-reconfigure tzdata
```

```
date
```

Dados do LEMP

IP do Servidor - 138.68.176.116

IP do trabalho - 177.14.224.187

A ser feito backup ao final

```
/var/www/html
```

```
/etc/nginx/nginx.conf
```

```
/etc/nginx/sites-available/default
```

```
/etc/php/7.0/fpm/pool.d/www.conf
```

```
/etc/php/7.0/fpm/php.ini
```

Suporte ao PHP e ao Joomla! no nginx

```
server {
    listen 80 default_server;

    root /var/www/html;
    index index.php index.html index.htm;

    # Make site accessible from http://localhost/
    server_name 138.68.176.116;
    server_name_in_redirect off;

    location / {
        autoindex on;
    }
}
```

```

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

    error_page 404 /404.html;
    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
        root /var/www/html;
    }

    location ~ /\.php$ {
        try_files $uri =404;
        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_intercept_errors on;
    }

    location ~ /\.ht {
        deny all;
    }
}

```

Testando

```
service nginx restart
```

```
nano /var/www/html/i.php
```

```
<?php
phpinfo();
```

OK

Aplicando SSL ao Nginx

```
mkdir /etc/nginx/ssl/
```

```
openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout
/etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt
```

Responda às perguntas:

```
Country Name (2 letter code) [XX]:BR
State or Province Name (full name) []:Ceará
Locality Name (eg, city) [Default City]:Fortaleza
Organization Name (eg, company) [Default Company Ltd]:FreeLancer
Organizational Unit Name (eg, section) []:Free
Common Name (eg, your name or your server's hostname) []:ribafs.org
```

Email Address []:ribafs@gmail.com

ls /etc/nginx/ssl/nginx.crt

openssl dhparam -out /etc/nginx/ssl/dhparam.pem 4096

This is going to take a long time

Aguarde um bom tempo... pode demorar de 10 minutos até uma hora ou pouco mais

nano /etc/nginx/sites-available/default

Adicione para o bloco server inicial

```
server {
    ...
    server_name IP; # ou ribafs.org www.ribafs.org

    ### SSL Config
    listen 443 ssl;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/ssl/dhparam.pem;
    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;

    if ($request_method !~ ^(GET|HEAD|POST)$ )
    {
        return 405;
    }

    ...
}
```

nginx -t

Proteção contra ataques Clickjacking

nano /etc/nginx/nginx.conf

Adicionar ao bloco http

```
add_header X-Frame-Options "SAMEORIGIN";
```

Descomente a linha

```
server_tokens off;
```

service nginx restart

service php7.0-fpm restart

Testar

`https://138.68.176.116`

Logs

Em caso de problema ver logs

```
tail -f /var/log/nginx/error.log
```

Instalar um site em Joomla na pasta /var/www/html/portal

IP do Servidor - 138.68.176.116

IP do trabalho - 177.14.224.187

Enviar o arquivo de backup criado pelo Akeeba Backup do desktop para a pasta /tmp do servidor

Este site será instalado no raiz /var/www/html/portal

No desktop copiar os dois arquivos (portal.zip e portal.sql) para a pasta /home/ribafs
`scp -P porta portal* ribafs@138.68.176.116:/tmp`

No servidor

```
cd /tmp
```

Criar o banco e um usuário dono dele

```
mysql -uroot -p
create database portal;
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'
WITH GRANT OPTION;
\q
```

```
mysql -uroot -p portal < portalxxx.sql
```

Descompactar o arquivo

```
cd /tmp
```

```
unzip portal*.zip -d /var/www/html/portal
```

Ajustar permissões do /var/www/html/portal

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

```
#!/bin/sh
clear;
echo "Aguarde enquanto configuro as permissões do /var/www/html/$1";
echo "";
chown -R www-data:www-data /var/www/html/$1;
find /var/www/html/$1 -type d -exec chmod 755 {} \;
find /var/www/html/$1 -type f -exec chmod 644 {} \;
echo "";
echo "Concluído!";
```

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

Executando no diretório /var/www/html/portal
perms portal

Executando no diretório /var/www/html
perms

Executo sempre que faço alguma alteração como root no /var/www/html

Ajustes no php.ini

```
nano /etc/php/7.0/fpm/php.ini
```

```
date.timezone = America/Fortaleza
output_buffering = Off
```

Efetuar ajustes no /var/www/html/portal/configuration.php se necessário.

Instalar o site em

Ajustar para o Joomla

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

Altere o location / para

```
location /portal {
    autoindex on;
    try_files $uri $uri/ /portal/index.php?$args;
}
```

service nginx restart

<http://159.65.91.104/portal>

Acusou erro

An error occurred while restoring the database. The error message can be found below. Click on the × button at the top right of this dialog message to close it and return to the database restoration page.

Database server error reply:

ErrNo #1071

Specified key was too long; max key length is 767 bytes

```
SQL=CREATE TABLE `mxj6w_akeeba_common` ( `key` varchar(192) COLLATE utf8mb4_unicode_ci NOT NULL, `value` longtext COLLATE utf8mb4_unicode_ci NOT NULL, PRIMARY KEY (`key`)) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci
```

Vou tentar um backup feito com o simplebackup

enviarei os dois arquivos, o zip e o sql

Criarei novamente o banco e importarei o script assim

```
mysql -u root -p < portal.sql
```

```
rm -rf /var/www/html/portal
```

```
cd /tmp
```

```
unzip portal.zip -d /var/www/html/portal
```

<http://138.68.176.116/portal>

Funcionou legal.

Criar outro site instalando o WordPress

Criar o banco e o user

```
mysql -uroot -p
```

```
create database blog;
```

```
GRANT ALL PRIVILEGES ON blog.* TO blog@localhost IDENTIFIED BY 'senhaforte' WITH GRANT OPTION;
```

```
\q
```

```
cd /tmp
```

```
wget -c https://br.wordpress.org/wordpress-4.9.4-pt_BR.zip
```

```
unzip wordpress* /var/www/html
mv /var/www/html/wordpress /var/www/html/blog

perms blog
```

Instalar

<http://138.68.176.116/blog>

Instalou normalmente

```
service nginx restart
```

```
nano /etc/php/7.0/fpm/php.ini
```

Mudar

```
output_buffering = Off
```

```
service php7.0-fpm restart
service nginx restart
```

Redirecionar acesso ao raiz para /portal

Removi index.html e i.php do raiz

```
rm /var/www/html/i.*
```

```
nano /var/www/html/index.php
```

```
<?php
header('location: portal');
```

Depois de testado o site e configurado novamente para proteger o administrator com SSL então efetuar um backup full para guardar. Usarei o componente SimpleBackup

Backup e Restore

Agora faça um backup completo com o akeeba e quando terminar restaure por exemplo para a pasta
`/var/www/html/portal2`

Crie o banco portal2, pode ser o mesmo user e senha

Restaure pela web:

<http://138.68.176.116/portal2>

Agora implementar a autenticação

Proteger diretório com nhinx

Instalar

```
apt install -y apache2-utils
```

```
htpasswd -c /etc/nginx/.htpasswd ribafs
```

```
cat /etc/nginx/.htpasswd
```

Para o Wordpress

Autenticação

```
htpasswd -bc /etc/nginx/.htpasswd ribafs senhaforte
```

No default

```
location ^~ /wp-login.php {
    auth_basic      "Área Restrita";
    auth_basic_user_file /etc/nginx/.htpasswd;
}
```

Editar o default.conf e alterar assim deixando assim:

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

```
#/etc/nginx/sites-available/default
```

```
server {
    listen 80 default_server;

    root /var/www/html;
    index index.php index.html index.htm;

    auth_basic      "Administrator's Area";
    auth_basic_user_file /etc/nginx/.htpasswd;

    # Make site accessible from http://localhost/
    server_name 167.99.80.172;
    server_name_in_redirect off;

    listen 443 ssl;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/ssl/dhparam.pem;
```

```

ssl_certificate /etc/nginx/ssl/nginx.crt;
ssl_certificate_key /etc/nginx/ssl/nginx.key;

if ($request_method !~ ^(GET|HEAD|POST)$ )
{
    return 405;
}

location / {
    auth_basic off;
    autoindex on;
    try_files $uri $uri/ /index.php?$args;
}

error_page 404 /404.html;
error_page 500 502 503 504 /50x.html;
location = /50x.html {
    root /var/www/html;
}

location ~ \.php$ {
    auth_basic off;
    try_files $uri =404;
    include /etc/nginx/fastcgi_params;
    fastcgi_pass unix:/run/php/php7.0-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    fastcgi_intercept_errors on;
}

location /portal/administrator {
    auth_basic "Restrito";
    auth_basic_user_file /etc/nginx/.htpasswd;
}

location /blog/wp-login.php {
    auth_basic "Restrito";
    auth_basic_user_file /etc/nginx/.htpasswd;
}

location ~ /\.ht {
    deny all;
}
}

service nginx restart
service php7.0-fpm restart

```

Crédito

<https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/>

Nesta fase backup:

- Dos scripts originais e alterados
- Dos bancos de dados dos sites

```
mysqldump -uroot -p blog > blog_09032018.sql
mysqldump -uroot -p portal > portal_09032018.sql
```

- Dos arquivos e diretórios do site

```
tar zcpvf blog_09032018.tar.gz /var/www/html/blog
tar zcpvf portal_09032018.tar.gz /var/www/html/portal
```

A guardarei com cuidado.

Script **debian9_lemph.sh** de instalação do servidor LEMP

```
#!/bin/bash
#
# Criado/adaptado por Ribamar FS - http://ribafs.org
#
apt-get install dialog;
#
while :
do
clear
servico=$(dialog --stdout --backtitle 'Instalação de pacotes no Ubuntu Server 16.04 LTS -
64' \
--menu 'Selecione a opção com a seta ou o número e tecla Enter\n' 0 0 0 \
1 'Atualizar repositórios' \
2 'Instalar Servidor Web e cia' \
3 'Efetuar o Upgrade da distribuição' \
0 'Sair' )
case $servico in
1) apt update;;
2) clear;
echo "Instalar pacotes básicos. Tecla Enter para instalar!";
apt install -y aptitude unzip mc;

clear;
echo "Instalar Apache e módulos. Tecla Enter para instalar!";
apt install -y nginx php7.0-fpm;

clear;
# Instalar SGBDs somente para testes locais. Visto que o servidor é outro: 10.0.0.60
apt install -y mysql-server;

clear;
echo "Instalar PHP 5 e extensões. Tecla Enter para instalar!";
```

```
apt install -y php7.0 php7.0-bcmath php7.0 php-mbstring mcrypt mcrypt php7.0-mcrypt  
php7.0-mysqlnd php7.0-gd php-pear curl php7.0-curl;  
apt install -y php-gettext php-auth php7.0-xml php7.0-xsl;  
apt install -y php7.0-zip;
```

```
clear;  
echo "Instalar soporte a cache no PHP. Tecle Enter para instalar!";  
# Cache de php  
apt -y install php-apcu;
```

```
wget http://ftp.ussg.iu.edu/linux/ubuntu/pool/main/m/memcached/memcached_1.4.25-  
2ubuntu1_amd64.deb;  
dpkg -i -y memcached_1.4.25-2ubuntu1_amd64.deb;  
apt -y install php-memcache;
```

```
service nginx restart;
```

```
clear;;
```

```
    3) clear;  
apt -y update;  
apt -y upgrade;;  
    0) clear;exit;;  
esac  
done
```

9.4 – Fedora

Criei um servidor no Vultr com Fedora 27

1024 MB Server - 144.202.38.148
Has been successfully created!
IP Address: 144.202.38.148
OS: Fedora 27 x64
RAM: 1024 MB
Storage: 25 GB SSD
Location: Miami
Label: fedora

Lembrou o Ubuntu, pois conectou com o root de primeira via ssh.

Troquei a senha do root com

```
passwd
```

Adicionei o usuário ribafs

```
adduser ribafs  
passwd ribafs
```

Adicionei para o grupo do root

```
gpasswd -a ribafs wheel
```

Fiz ajustes no ssh

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

Efetuei logoff e voltei para meu desktop
exit

Configurei para salvar a chave do ssh e não pedir senha:
ssh-copy-id ribafs@server_ip -p 15522

Não funcionou e quando quiz voltar com o root também não voltou mais, deu o erro:
No route to host

Já suspeitei do firewall. Vejamos. Vou agora acessar pela console como root para ver.

```
Executei  
service iptables stop
```

Disse que iptables.service não estava presente

Então experimentei

```
service firewalld status
```

E tava lá. O Fedora 27 também, como o CentOS 7 usa o firewalld. Como não quero aprender outra ferramenta vou remover e usar o iptables.

Não estava conseguindo nem parando o firewalld, nem com iptables -F, dava conexão recusada.

Então deveria haver algo mais recusando a conexão. Executei

```
sestatus
```

E tava lá o SELinux habilitado.

```
nano /etc/selinux/config
```

```
SELINUX=disabled
```

```
reboot
```

Após o boot disse que não tinha rota para o host. Então agora é com o firewalld

```
service firewalld stop
```

Agora foi.

Configurar o timezone

```
ls -sf /usr/share/zoneinfo/America/Fortaleza /etc/localtime
```

Mas vou querer aprender a usar o selinux, que deve reforçar bem a segurança.

```
yum provides semanage
```

```
yum install policycoreutils-python-utils-2.7-4.fc27.x86_64
```

Atualizei com

```
yum update
```

```
reboot
```

Demorou mais que Centos7, Debian9 e Ubuntu 16.04 para atualizar

Resolvi, por enquanto, desabilitar firewalld e selinux e instalar iptables-services e o habilitar e iniciar.

Então usar minhas regras.

Após o boot ainda travou o acesso via ssh.

Fui verificar e o firewalld estava no ar.

Desabilitei, parei e desinstalei:

```
service firewalld stop
```

```
systemctl disable firewall
yum remove firewalld
```

Instalar

```
dnf install -y unzip mc wget
```

Instalei LAMP sem dificuldades.

Vejamos agora com o LEMP

```
nano /etc/php-fpm.d/www.conf
```

```
listen.mode = 0750
listen.owner = nginx
listen.group = nginx
```

Ainda tive problema após reiniciar o sistema.

Não mais tive acesso via ssh.

Mudei a rede para IP estático

Então resolvi desinstalar o iptables e instalar o firewalld. Experimentei mas nada, somente acesso quando paro o firewalld.

Vou desinstalar o firewalld e voltar ao iptables:

```
systemctl stop firewalld
systemctl disable firewalld
```

```
dnf remove firewalld
```

Assim, sem firewall algum acesso, mas não é interessante.

reboot

```
yum install iptables-services
systemctl enable iptables.service
service iptables start
iptables -L
iptables -F
```

Copiei as minhas regras

```
systemctl restart iptables
```

Antes após este comando o terminal já travava. Agora não travou.

reboot

Mesmo após o reboot consegui acessar. O problema parece que eram 3 regras que estava instando e barravam meu acesso.

Mas o nginx com php não rola. Somente nginx funciona, mas com php não. Beleza. É importante ler os comentários encontrados pois podem ajudar.

Acabei removendo todos os pacotes php:

```
yum remove php*
```

E instalando apenas estes:

```
dnf install php php-fpm php-mysqlnd php-gd
```

E após reiniciar o nginx e o php-fpm funcionou:

```
service nginx restart  
service php-fpm restart
```

```
http://localhost/info.php
```

LAMP com Fedora

Criar o servidor

Acessar via ssh com root

```
ssh root@IP
```

Criar uma pasta para guardar um backup de todo script que precisar alterar

```
mkdir /root/back
```

Desabilitar inicialmente o SELinux

```
cp /etc/selinux/config /root/back
```

```
nano /etc/selinux/config
```

Mudar para Disabled

```
reboot
```

Criar usuário comum

```
adduser ribafs
```

```
passwd ribafs
```

Adicionar ao grupo do root

```
gpasswd -a ribafs wheel
```

Copiar a chave pública do ssh do seu desktop para o servidor

```
exit
```

```
ssh-copy-id ribafs@IP
```

Ele pedirá a senha de ribafs no servidor

Acesse agora sem senha com

```
ssh ribafs@IP
```

Mude para root

```
su
```

Atualiza o Fedora

```
dnf update
```

```
dnf install nano mc unzip mlocate
```

Atualizar o banco de dados do locate

```
updatedb
```

Desabilite login do root via ssh e faça outros ajustes

```
cp /etc/ssh/sshd_config /root/back
```

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

```
PermitRootLogin no
```

```
PasswordAuthentication no
```

```
LoginGrace 30
```

Adicionar ao final

```
AllowUsers ribafs
```

```
systemctl reload sshd
```

Configurar timezone

```
ls /usr/share/zoneinfo/
```

```
ln -sf /usr/share/zoneinfo/America/Fortaleza /etc/localtime
```

Usar um Firewall

Decidir se firewalld ou iptables

Se iptables:

```
dnf install -y iptables-services
```

```
systemctl enable iptables
```

```
systemctl start iptables
```

```
iptables -L
```

Inicialmente deve mostrar:

```
Chain INPUT (policy ACCEPT)
```

```
target prot opt source
```

```
destination
```

```
ACCEPT all -- anywhere
```

```
anywhere
```

```
state RELATED,ESTABLISHED
```

```
ACCEPT icmp -- anywhere
```

```
anywhere
```

```
ACCEPT all -- anywhere
```

```
anywhere
```

```
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited
```

Chain FORWARD (policy ACCEPT)

```
target prot opt source destination
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited
```

Chain OUTPUT (policy ACCEPT)

```
target prot opt source destination
```

Para guardar permanentemente estas regras:
 /usr/libexec/iptables/iptables.init save

Permitir portas 80 e 443

```
cp /etc/sysconfig/iptables /root/back
```

```
nano /etc/sysconfig/iptables
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

```
/usr/libexec/iptables/iptables.init save
```

```
systemctl restart iptables
```

Instalar Apache

```
dnf update
dnf install httpd
systemctl start httpd.service
```

Testar

```
http://IP
```

MariaDB

```
Instalar
dnf install mysql mysql-server
systemctl start mariadb.service
dnf install mysql mysql-server
systemctl start mariadb.service
```

PHP

Instalar

```
dnf install php php-mysqlnd
dnf search php-
```

Outros pacotes

```
php-bcmath php mcrypt mcrypt php-mcrypt php-mysqlnd php php-gd php-pear curl php-
curl;
php-zip php-gettext php-fpm php-auth php-xml php-xsl;
```

```
systemctl restart httpd.service
```

Testando

```
nano /var/www/html/info.php
```

```
<?php
phpinfo();
```

```
http://IP
```

<https://www.itzgeek.com/how-tos/linux/fedora-how-tos/nginx-php-fpm-mariadb-on-fedora-21.html>

<https://www.if-not-true-then-false.com/2011/install-nginx-php-fpm-on-fedora-centos-red-hat-rhel/>

Criar o servidor

Acessar via ssh

```
ssh root@IP
```

Adicionar usuário comum ribafs

Sair e logar como ribafs

```
sudo -i
ou
su
```

```
dnf update
```

Dependências para Fedora 27/26/25

```
rpm -Uvh http://download1.rpmfusion.org/free/fedora/rpmfusion-free-release-
stable.noarch.rpm
```

```
rpm -Uvh http://download1.rpmfusion.org/nonfree/fedora/rpmfusion-nonfree-release-
stable.noarch.rpm
```

Fedora 27

```
rpm -Uvh http://rpms.famillecollet.com/fedora/remi-release-27.rpm
```

```
dnf --enablerepo=remi --enablerepo=remi-php72 install nginx php-fpm php-common
```

```
mkdir /root/back
```

MariaDB

Instalar

```
dnf -y install mariadb mariadb-server
```

```
systemctl start mariadb
```

```
systemctl enable mariadb
```

Nginx

Instalar

```
dnf -y install nginx
```

```
systemctl start nginx
```

Firewall

```
firewall-cmd --permanent --add-service=http
```

```
firewall-cmd --reload
```

SELinux

Caso receba algum erro do SELinux no log veja:

<http://axilleas.me/en/blog/2013/selinux-policy-for-nginx-and-gitlab-unix-socket-in-fedora-19/>

```
setenforce 0
```

Testando

```
http://IP
```

O diretório web default do nginx no Fedora é
`/usr/share/nginx/html`

E o diretório de configurações é:

```
/etc/nginx
```

```
systemctl enable nginx
```

PHP-FPM

Instalar os seguintes módulos do php

OPcache (php-opcache) – The Zend OPcache provides faster PHP execution through opcode caching and optimization.

APCu (php-pecl-apcu) – APCu userland caching

CLI (php-cli) – Command-line interface for PHP

PEAR (php-pear) – PHP Extension and Application Repository framework

PDO (php-pdo) – A database access abstraction module for PHP applications

MySQL (php-mysqlnd) – A module for PHP applications that use MySQL databases

PostgreSQL (php-pgsql) – A PostgreSQL database module for PHP

MongoDB (php-pecl-mongodb) – PHP MongoDB database driver

Redis (php-pecl-redis) – Extension for communicating with the Redis key-value store

Memcache (php-pecl-memcache) – Extension to work with the Memcached caching daemon

Memcached (php-pecl-memcached) – Extension to work with the Memcached caching daemon

GD (php-gd) – A module for PHP applications for using the gd graphics library

XML (php-xml) – A module for PHP applications which use XML

MBString (php-mbstring) – A module for PHP applications which need multi-byte string handling

MCrypt (php-mcrypt) – Standard PHP module provides mcrypt library support

Instalar

```
dnf --enablerepo=remi --enablerepo=remi-php72 install php-opcache php-pecl-apcu php-cli php-pear php-pdo php-mysqlnd php-pecl-redis php-pecl-memcache php-pecl-memcached php-gd php-mbstring php-mcrypt php-xml php-fpm
```

```
systemctl stop httpd.service  
systemctl disable httpd.service
```

```
systemctl start nginx.service  
systemctl enable nginx.service
```

```
systemctl start php-fpm.service  
systemctl enable php-fpm.service
```

Configurar

```
cp /etc/php.ini /root/back
```

```
nano /etc/php.ini
```

Mudar

```
cgi.fix_pathinfo=0
```

```
cp /etc/php-fpm.d/www.conf /root/back
```

```
nano /etc/php-fpm.d/www.conf
```

Mudar

```
listen = /run/php-fpm/www.sock
para
listen = 9000
```

Garanta que as duas linhas abaixo estão descomentadas

```
pm.min_spare_servers = 5
...
pm.max_spare_servers = 35
```

```
systemctl enable php-fpm
```

Criar um virtualHost

```
ServerName: server.ribafs.local
DocumentRoot: /usr/share/nginx/html/ribafs.local
```

Criar o arquivo

```
nano /etc/nginx/conf.d/virtual.conf
```

Adicione:

```
server {
    server_name server.ribafs.local;
    root /usr/share/nginx/html/ribafs.local;

    location / {
        index index.html index.htm index.php;
    }

    location ~ \.php$ {
        include /etc/nginx/fastcgi_params;
        fastcgi_pass 127.0.0.1:9000;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME
/usr/share/nginx/html/ribafs.local$fastcgi_script_name;
    }
}
```

Adicionar ao hosts

```
cp /etc/hosts /root/back
```

```
nano /etc/hosts
```

```
127.0.0.1 localhost.localdomain localhost server.ribafs.local
```

```
mkdir /usr/share/nginx/html/ribafs.local
```

```
nano /usr/share/nginx/html/ribafs.local/index.php
```

```
<?php  
phpinfo();
```

```
systemctl restart nginx  
systemctl restart php-fpm
```

```
http://server.ribafs.local
```

Caso receba erro 403 forbidden

```
chcon -R -t httpd_sys_content_t /usr/share/nginx/html/ribafs.local
```

ou algum aplicativo foi negado

```
chcon -R -t httpd_sys_rw_content_t /usr/share/nginx/html/ribafs.local
```

Habilitar porta 80

```
nano -w /etc/sysconfig/iptables
```

Adicionar

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

```
iptables-service save  
service iptables restart
```

Ou para o caso de usar o firewalld

```
firewall-cmd --permanent --zone=public --add-port=80/tcp
```

```
systemctl restart firewalld.service
```

Testar conexão remota

9.5 – OpenBSD

Criação de Servidor OpenBSD 6.2 no Vultr

512 MB Server - 45.77.195.154
Has been successfully created!
IP Address: 45.77.195.154
OS: OpenBSD 6 x64
RAM: 512 MB
Storage: 20 GB SSD
Location: Miami
Label: ribafs

45.77.195.154

uname -r

openbsd 6.2

Tamanho - 512MB de RAM

ssh root@45.77.195.154

passwd

vi /etc/ssh/sshd_config

vi /etc/rc.conf
sshd_enable="YES"

/etc/rc.d/sshd restart

adduser

Timezone
cd /usr/share/zoneinfo
ls -l
cp /usr/share/zoneinfo/America/Fortaleza /etc/localtime

ou
export TZ=America/Fortaleza

date

vi /etc/installurl

<https://mirror.esc7.net/pub/OpenBSD/>

```
pkg_add -v -i links
```

-v : Verbose mode (display more information)

-i : Interactive installation. It may ask you question such as which version you would like to install and so on.

```
pkg_add nano
```

```
pkg_add sudo
```

```
pkg_delete pkgNameHere
```

```
vi /etc/sudoers
```

```
sudo usermod -G wheel ribafs
```

```
pkg_info
```

Atualização de pacotes existentes

```
pkg_add -u links
```

Atualização de todos os pacotes

```
pkg_add -u
```

Ports

```
cd /home/ribafs
```

```
wget http://ftp.usa.openbsd.org/pub/OpenBSD/$(uname -r)/ports.tar.gz
```

```
wget http://ftp.usa.openbsd.org/pub/OpenBSD/$(uname -r)/SHA256.sig
```

```
signify -C -p /etc/signify/openbsd-62-base.pub -x SHA256.sig ports.tar.gz
```

```
tar -zxvf ports.tar.gz -C /usr/
```

```
cd /usr/ports/lang/php/7.0/
```

```
make install clean
```

```
cd /usr/ports
```

```
make search key=php-gd-7
```

Parar sendmail

```
/etc/rc.d/sendmail stop
```

```
nano /etc/rc.conf
```

```
sendmail_enable="NONE"
```

```
sendmail_submit_enable="NO"
```

```
sendmail_outbound_enable="NO"
```

```
sendmail_msp_queue_enable="NO"
```

```
nano /etc/hosts
```

```
Adicionar
```

```
45.77.195.154      www.ribafs.org    www
```

Timezone

```
bsdconfig
```

Firewall

```
nano /etc/pf.conf
```

```
ifconfig
```

```
vio0
```

```
Adicionar
```

```
## Início ##
```

```
me="vio0"
```

```
table <bruteforcers> persist
```

```
table <trusted> persist file "/etc/trusted"
```

```
icmp_types = "echoreq"
```

```
junk_ports="{ 135,137,138,139,445,68,67,3222 }"
```

```
junk_ip="224.0.0.0/4"
```

```
set loginterface vtnet0
```

```
scrub on vio0 reassemble tcp no-df random-id
```

```
# ---- First rule obligatory "Pass all on loopback"
```

```
pass quick on lo0 all
```

```
# ---- Block junk logs
```

```
block quick proto { tcp, udp } from any to $junk_ip
```

```
block quick proto { tcp, udp } from any to any port $junk_ports
```

```
# ---- Second rule "Block all in and pass all out"
```

```
block in log all
```

```
pass out all keep state
```

```
##### FIREWALL #####
```

```
# ---- Allow all traffic from my Home
```

```
pass quick proto {tcp, udp} from 45.77.195.154 to $me keep state
```

```
# ---- block SMTP out
```

```
block quick proto tcp from $me to any port 25
```

```
# ---- Allow incoming Web traffic
pass quick proto tcp from any to $me port { 80, 443 } flags S/SA keep state

# ---- Allow my team member SSH access
pass quick proto tcp from 45.77.195.154 to $me port 65522 flags S/SA keep state

# ---- Block bruteforcers
block log quick from <bruteforcers>

# ---- Allow SSH from trusted sources, but block bruteforcers
pass quick proto tcp from <trusted> to $me port 65522 \
flags S/SA keep state \
(max-src-conn 10, max-src-conn-rate 20/60, \
overload <bruteforcers> flush global)

# ---- Allow ICMP
pass in inet proto icmp all icmp-type $icmp_types keep state
pass out inet proto icmp all icmp-type $icmp_types keep state
## Final ##
```

Criar o arquivo

```
nano /etc/trusted
```

Adicionar os IPs

```
#Casa
177.130.208.59
```

```
#DNOCS
```

Habilitar e desabilitar PF

```
pfctl -e
pfctl -d
```

```
pfctl -f /etc/pf.conf Load the pf.conf file
pfctl -nf /etc/pf.conf Parse the file, but don't load it
pfctl -sr          Show the current ruleset
pfctl -ss          Show the current state table
pfctl -si          Show filter stats and counters
pfctl -sa          Show EVERYTHING it can show
```

```
reboot
```

```
tcpdump -n -e -ttt -i pflog0
```

```
tcpdump -n -e -ttt -r /var/log/pflog
```

```
pfctl -t bruteforcers -T show
```

```
pfctl -t bruteforce -T expire 86400
```

```
pkg_add pftop
```

```
pftop
```

```
pftop - visualizar tráfego pelo pf
```

Instalar Apache

Já estava instalado

Criar o arquivo

```
nano /etc/httpd.conf
```

```
server "default" {
    listen on egress port 80
    root "/wordpress"
    directory index index.php

    location "*.php*" {
        fastcgi socket "/run/php-fpm.sock"
    }
}

types {
    text/css          css
    text/html         html htm
    text/txt          txt
    image/gif         gif
    image/jpeg        jpeg jpg
    image/png         png
    application/javascript js
    application/xml   xml
}
```

FILES

/etc/httpd.conf - Default configuration file.

/etc/ssl/private/server.key - Default SSL/TLS server key.

/etc/ssl/server.crt - Default SSL/TLS server certificate.

/var/run/httpd.sock - UNIX-domain socket used for communication with httpd.

/var/www/logs/access.log - Default access log file.

/var/www/logs/error.log - Default error log file.

```
/etc/rc.d/httpd -f start
```

Instalar MariaDB

```
pkg_add mariadb-server
```

The following new rcscripts were installed: /etc/rc.d/mysqld
See rcctl(8) for details.
Look in /usr/local/share/doc/pkg-readmes for extra documentation.

```
mysql_install_db
```

```
nano /etc/rc.conf
```

```
mysql_server_enable=YES
```

```
/etc/rc.d/mysqld start
```

```
mysql_secure_installation
```

Instalar PHP

```
pkg_info php
```

```
pkg_add php
```

```
5.6 e 7.0
```

```
Instalar a 7.0
```

The following new rcscripts were installed: /etc/rc.d/php70_fpm
See rcctl(8) for details.
Look in /usr/local/share/doc/pkg-readmes for extra documentation.

```
nano /etc/httpd.conf
```

```
server "default" {  
    listen on egress port 80  
    directory index index.php  
  
    location "*.php*" {  
        fastcgi socket "/run/php-fpm.sock"  
    }  
}
```

```
}
```

```
types {  
    text/css          css  
    text/html        html htm
```

```
text/txt      txt
image/gif     gif
image/jpeg    jpeg jpg
image/png     png
application/javascript js
application/xml xml
}
```

```
mkdir /var/www/htdocs/portal
```

```
nano /var/www/htdocs/portal/info.php
```

```
<?php
phpinfo();
```

```
/etc/rc.d/php70_fpm start
/etc/rc.d/httpd restart
```

Testar

```
http://45.77.195.154/portal/info.php
```

Ao tentar criar o banco o mysql apresentou:
ERROR 2006 (HY000) at line 764: MySQL server has gone away

```
nano /etc/my.cnf
```

```
Mudei a linha
max_allowed_packet = 4M
```

```
/etc/rc.d/mysqld restart
/etc/rc.d/php70_fpm restart
```

Quando instalei o site em Joomla na pasta
/var/www/htdocs/portal

Criei o banco e chamei pelo navegador após ter reiniciado
Apareceu o erro 500.

```
Então
/etc/rc.d/php70_fpm restart
```

```
E aproveitei e adicionei no
nano /etc/rc.conf
php70_fpm_enable=YES
```

Via ports

```
cd /usr/ports/lang/php/7.0/
make install clean
```

Demora muito, mais de 2 horas em servidor com 512MB de RAM

make check

Instalou o php 7 e o apache 2.4.47

Testar

<http://45.77.195.154>

Algumas vantagens do OpenBSD

- Muito seguro
- Leve e limpo

Recuperar senha do root

Efetue um reboot em single user mode

Quando aparecer o prompt

boot -s

monte as partições / e /usr

fsck -p / && mount -uw /

fsck -p /usr && mount /usr

E mude a senha com
passwd root

Usando OpenNTP

Para ajustar o tempo no servidor

pool.ntp.org

In -fs /usr/share/zoneinfo/America/Fortaleza /etc/localtime

Codificação de Caractres

nano ~/.profile

export LC_CTYPE="en_US.UTF-8"

```
nano /etc/hosts
```

```
:::1          localhost localhost.ceph ceph
127.0.0.1    localhost localhost.ceph ceph
108.61.178.110 ceph.domain1.com  ceph
```

```
server "owncloud.example.com" {
    listen on $ext_if port 80
    listen on $ext_if tls port 443
    directory index "index.php"
    root "/owncloud"

    # Set max upload size to 513M (in bytes)
    connection max request body 537919488

    # First deny access to the specified files
    location "/db_structure.xml" { block }
    location "/.ht*"           { block }
    location "/README"         { block }
    location "/data*"          { block }
    location "/config*"        { block }

    location "/*.php*" {
        fastcgi socket "/run/php-fpm.sock"
    }
}
```

SSL

```
server "owncloud.example.com" {
    listen on $ext_if port 80
    listen on $ext_if tls port 443

    tls {
        certificate "/etc/ssl/example.crt"
        key "/etc/ssl/private/example.key"
    }

    # ...
}
```

Install Apache, MySQL And PHP On OpenBSD 5.4

<https://www.unixmen.com/install-apache-mysql-php-openbsd-5-4/>

```
export PKG_PATH=http://ftp.bit.nl/pub/OpenBSD/5.4/packages/`machine`-a`/
```

Apache

```
pkg_add -u apache-httpd
```

MySQL

```
pkg_add mysql-server
```

```
mysql_install_db
```

Criar uma nova senha

```
mysqld_safe
```

```
/usr/local/bin/mysqladmin -u root password "senhaforte"
```

PHP com MySQL

```
pkg_add php-mysql
```

```
ln -sf /var/www/conf/modules.sample/php-5.3.conf /var/www/conf/modules/php.conf
```

Criou-se o arquivo recomendado
/etc/php-5.3.ini

```
ln -sf /etc/php-5.3.sample/mysql.ini /etc/php-5.3/mysql.ini
```

Configurando Apache com PHP

```
nano /var/www/conf/httpd.conf
```

Altere
DirectoryIndex index.php index.html

Adicionar ao rc.conf

```
nano /etc/rc.conf
```

```
mysqld_flags=""  
httpd_flags=""  
pkg_scripts="mysqld"
```

Testando

```
http://IP
```

Apache + PHP + MySQL + ftpd no OpenBSD

<https://www.vivaolinux.com.br/artigos/impressora.php?codigo=8734>

```
export PKG_PATH=ftp://ftp.openbsd.org/pub/OpenBSD/4.3/packages/^ uname -m`
```

MySQL

```
pkg_add mysql-server
```

```
mysql_install_db
```

```
mysqld_safe
```

```
mysqladmin -u root password 'senha_forte'
```

rc.conf

```
nano /etc/rc.conf
```

```
mysql=YES
```

```
httpd_flags=""
```

rc.local

```
nano /etc/rc.local
```

Adicionar

```
if [ X"${mysql}" == X"YES" -a -x /usr/local/bin/mysqld_safe ]; then
  echo -n " mysqld"; /usr/local/bin/mysqld_safe --user=_mysql --log --open-files-limit=256
&
  for i in 1 2 3 4 5 6; do
    if [ -S /var/run/mysql/mysql.sock ]; then
      break
    else
      sleep 1
      echo -n "."
    fi
  done
fi
```

Apache

```
mkdir -p /var/www/var/run/mysql
```

```
ln -f /var/run/mysql/mysql.sock /var/www/var/run/mysql/mysql.sock
```

PHP

```
pkg_add -v php5-core-5.2.3.tgz
```

```
pkg_add -v php5-gd-5.2.3.tgz
pkg_add -v php5-mysql-5.2.3.tgz
pkg_add -v php5-odbc-5.2.3.tgz
```

Ativar os módulos (no 6.2 não requer)

```
phpxs -a gd
phpxs -a mysql
phpxs -a odbc
```

```
cp /usr/local/share/examples/php5/php.ini-recommended /var/www/conf/php.ini
```

Configurar Apache

```
nano /var/www/conf/httpd.conf
```

```
# pra carregar o módulo do php5
LoadModule php5_module /usr/local/lib/php/libphp5.so
AddType application/x-httpd-php .php .php4 .php3 .htm .html
AddType application/x-httpd-php-source .phps
```

```
DirectoryIndex index.html index.htm index.php index.php5 index.php4 index.php3
```

```
apachectl restart
```

```
echo "<? echo phpinfo(); ?>" > /var/www/htdocs/phpinfo.php
```

```
http://localhost/phpinfo.php
```

Procurar pacotes

Informações e busca

```
pkg_info -Q nome
```

Instalar

```
pkg_add pkglocatedb
```

```
pkglocate nome
```

Atualizando pacotes instalados

```
pkg_add -u nome
```

Removendo

```
pkg_delete nome
```

Checar pacotes

```
pkg_check
```

Mirror de pacotes

Existem dois lugares de onde o pkg traz seus pacotes, o installurl e da variável de ambiente PKG_PATH

```
nano /etc/installurl
```

```
http://ftp.openbsd.org/pub/OpenBSD
```

Setando manualmente

```
export PKG_PATH=scp://user@company-build-server/usr/ports/packages/  
%a/all:https://trusted-public-server/%m:installpath
```

```
df -H
```

```
fdisk sd0
```

Interativamente podendo alterar

```
fdisk -e sd0
```

Script de permissão

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

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

Firewall com PF

How to Install and Use the PF Firewall on FreeBSD — BIN63

<http://bin63.com/how-to-install-and-use-the-pf-firewall-on-freebsd>

No OpenBSD o pf é habilitado por default

Para desabilitar:

```
rcctl disable pf
```

Reboot para surtir efeito

Configurar

```
nano /etc/blocked_ips.conf
```

```
# IPs bloqueados
```

```
12.12.12.12
```

```
34.34.34.34
```

```
56.56.56.56
```

```
ifconfig
```

```
nano /etc/pf.conf
```

```
udp_services = "{ ntp }"
```

```
tcp_services = "{ smtp, ssh, http }"
```

```
local_host="123.123.123.123"
```

```
table <blockedips> persist file "/etc/blocked_ips.conf"
```

```
interface="re0"
```

```
set block-policy return
```

```
set skip on lo0
```

```
scrub in all
```

```
block all
```

```
block drop in log quick on $interface from <blockedips> to any
```

```
pass out on $interface inet from $local_host to any
```

```
pass in on $interface inet proto tcp from any to $local_host port $tcp_services
```

```
pass in on $interface inet proto udp from any to $local_host port $udp_services
```

```
pass in on $interface inet proto icmp from any to $local_host icmp-type echoreq
```

```
nano /etc/rc.conf
```

```
pf_enable="YES"
```

```
pf_rules="/etc/pf.conf"
```

```
pf_flags=""
```

```
pflog_enable="YES"
pflog_logfile="/var/log/pflog"
pflog_flags=""
```

O arquivo pf.conf tem várias seções:

```
Macros
Tables
Options
Filter Rules
```

Carregando regras

```
nano /etc/pf.conf
Gravar regras
```

```
pfctl -vnf /etc/pf.conf
```

Habilitar

Antes de habilitar devemos carregar as regras para efetuar correções com:

```
pfctl -vnf /etc/pf.conf
```

```
pfctl -e
```

Desabilitar

```
pfctl -d
```

```
reboot
```

Controle

```
pfctl -f /etc/pf.conf      Load the pf.conf file
pfctl -nf /etc/pf.conf     Parse the file, but don't load it
pfctl -sr                 Show the current ruleset
pfctl -ss                 Show the current state table
pfctl -si                 Show filter stats and counters
pfctl -sa                 Show EVERYTHING it can show
```

Listas

Uma lista permite especificar vários critérios similares com uma regra

Exemplo

```
block out on fxp0 from { 192.168.0.1, 10.5.32.6 } to any
```

Quando for interpretado será expandido para duas regras

```
block out on fxp0 from 192.168.0.1 to any
block out on fxp0 from 10.5.32.6 to any
```

Múltiplas listas podem ser especificadas com uma regra

```
match in on fxp0 proto tcp to port { 22 80 } rdr-to 192.168.0.6
block out on fxp0 proto { tcp udp } from { 192.168.0.1, 10.5.32.6 } \
  to any port { ssh https }
```

Listas também podem conter outras listas aninhadas

```
trusted = "{ 192.168.1.2 192.168.5.36 }"
pass in inet proto tcp from { 10.10.0.0/24 $trusted } to port 22

pass in on fxp0 from { 10.0.0.0/8, !10.1.2.3 }
```

Macros

Macros são variáveis definidas pelo usuário que podem manipular IP, portas, interfaces, etc.

Podem reduzir a complexidades das regras do PF e tornar a manutenção mais fácil.

Nomes de macros precisam iniciar com uma letra e deve conter letras, dígitos e sublinhados. Não podem usar palavras reservadas como pass ou queue.

Exemplos:

```
ext_if = "fxp0"
```

```
block in on $ext_if from any to any
```

Ao referir para uma macro precedemos seu nome com \$, como acima.

Também podem expandir para listas

```
friends = "{ 192.168.1.1, 10.0.2.5, 192.168.43.53 }"
```

Macros também podem ser preenchidas por um arquivo texto contendo uma lista de IPs e redes:

```
table <spammers> persist file "/etc/spammers"
block in on fxp0 from <spammers> to any
```

O arquivo /etc/spammers deve conter uma lista de IPs e/ou blocos de rede CIDR um por linha

Exemplo

```
pre = "pass in quick on ep0 inet proto tcp from "
```

```
post = "to any port { 80, 6667 }"
```

```
$pre 198.51.100.80 $post
```

```
$pre 203.0.113.79 $post
```

```
$pre 203.0.113.178 $post
```

Manipulação com pfctl

Tables podem ser manipuladas usando pfctl(8):

Para adicionar entradas para a tabela <spammers> criada acima:

```
pfctl -t spammers -T add 203.0.113.0/24
```

Isto também criará a tabela <spammers> caso não exista

Listar os endereços na tabela

```
pfctl -t spammers -T show
```

O -V pode ser também usado com o -T para mostrar estatística para cada entrada na tabela.

Para remover endereços de uma tabela

```
pfctl -t spammers -T delete 203.0.113.0/24
```

Ou

```
pfctl -t spammers -T del 203.0.113.0/24
```

Uma limitação quando especificando endereços é que 0.0.0.0/0 e 0/0 não devem funcionar em tabelas.

Na criação de uma tabela é permitido

```
table <goodguys> { 172.16.0.0/16, !172.16.1.0/24, 172.16.1.100 }
```

```
block in on dc0
```

```
pass in on dc0 from <goodguys>
```

Esta relação de regras

```
block in quick on egress inet from 127.0.0.0/8 to any
```

```
block in quick on egress inet from 192.168.0.0/16 to any
```

```
block in quick on egress inet from 172.16.0.0/12 to any
```

```
block in quick on egress inet from 10.0.0.0/8 to any
```

```
block out quick on egress inet from any to 127.0.0.0/8
```

```
block out quick on egress inet from any to 192.168.0.0/16
```

```
block out quick on egress inet from any to 172.16.0.0/12
```

```
block out quick on egress inet from any to 10.0.0.0/8
```

Pode ser simplificada com estas duas listas:

```
block in quick on egress inet from { 127.0.0.0/8, 192.168.0.0/16, \
172.16.0.0/12, 10.0.0.0/8 } to any
block out quick on egress inet from any to { 127.0.0.0/8, \
192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 }
```

Critério

O critério usado pelo PF quando inspeciona pacotes é baseado nos cabeçalhos das camada 3 (IPv4 e IPv6) e camada 4 (TCP, UDP, ICMP e ICMPv6)

O filtro das regras é avaliado na ordem sequencial, da primeira para a última. Até que o pacote encontre a regra contendo a palavra "quick" o pacote deve ser avaliado contra as regras de filtro "all" antes que a ação seja finalizada.

As regras de filtragem são avaliadas em ordem sequencial, da primeira para a última. A menos que o pacote corresponda a uma regra que contenha a palavra-chave "quick", o pacote será avaliado em relação a todas as regras de filtragem antes que a ação final seja executada.

A última regra a ser correspondida é a "vencedora" e determinará qual ação tomar no pacote.

Há um passo implícito no início de um conjunto de regras de filtragem, o que significa que, se um pacote não corresponder a nenhuma regra de filtro, a ação resultante será aprovada (pass).

A ação a ser tomada para correspondência de pacotes, seja passar (pass) ou bloquear (block). A ação pass passará o pacote de volta ao kernel para processamento adicional, enquanto a ação de block reagirá com base na configuração da opção block-policy. A reação padrão pode ser substituída especificando ou o block drop ou o block return.

Default Deny

A prática recomendada é para se usar por padrão a aproximação "default deny", que irá negar qualquer coisa e então seletivamente permitir certos tráfegos através do firewall.

Para criar uma política que filtre usando "default deny" a primeira regra pode ser:

```
block in all
block out all
```

ou

```
block all
```

ou

```
block
```

Isto irá bloquear todo o tráfego em todas as interfaces em todas as direções de (from) todo lugar (any) para (to) todo lugar (any).

Outro exemplo que resume

```
block in on r10 all
pass in quick log on r10 proto tcp from any to any port 22
```

Pode ficar assim:

```
block in on r10
pass in quick log on r10 proto tcp to port 22
```

Simplificação do return

```
block in all
block return-rst in proto tcp all
block return-icmp in proto udp all
block out all
block return-rst out proto tcp all
block return-icmp out proto udp all
```

Pode ficar assim:

```
block return
```

Quando o PF vê a palavra-chave return, ele é inteligente o suficiente para enviar a resposta apropriada, ou nenhuma resposta, dependendo do protocolo do pacote que está sendo bloqueado.

Palavra-chave quick

Como indicado anteriormente, cada pacote é avaliado em relação ao conjunto de regras de filtragem de cima para baixo, sequencialmente. Por padrão, o pacote é marcado para passagem, que pode ser alterado por qualquer regra, e pode ser alterado várias vezes antes do término das regras de filtragem. A última regra correspondente ganha. Há uma exceção: a opção quick em uma regra de filtragem tem o efeito de cancelar qualquer processamento de regra adicional e faz com que a ação especificada seja executada. Vamos dar uma olhada em alguns exemplos:

Erro

```
block in on egress proto tcp to port ssh
pass in all
```

Melhor

```
block in quick on egress proto tcp to port ssh
pass in all
```

Preservando o estado

A inspeção com estado refere-se à capacidade do PF de rastrear o estado ou o progresso de uma conexão de rede. Armazenando (estado) informações sobre cada conexão em uma tabela de estados.

Manter o estado tem muitas vantagens, incluindo conjuntos de regras mais simples e melhor desempenho de filtragem de pacotes.

Quando uma regra cria um estado, o primeiro pacote que corresponde à regra cria um "estado" entre o emissor e o receptor.

Todas as regras pass criam automaticamente uma entrada de estado quando um pacote corresponde à regra. Isso pode ser explicitamente desativado usando a opção sem estado (no state).

```
pass out on egress proto tcp from any to any
```

A opção de estado de modulação (modulate state) funciona justamente como manter estado, exceto que isso se aplica somente a pacotes TCP. Com o estado modular (modulate state), o Número de Sequência Inicial (ISN) das conexões de saída é randomizado.

```
pass out on egress proto { tcp, udp, icmp } from any to any modulate state
```

Outra vantagem de manter o estado é que o tráfego ICMP correspondente será passado pelo firewall.

Bloqueando pacotes spoofed

O endereço "spoofing" é quando um usuário mal-intencionado falsifica o endereço IP de origem em pacotes que eles transmitem para ocultar seu endereço real ou para representar outro nó na rede. Depois que o usuário falsificar seu endereço, ele poderá iniciar um ataque à rede sem revelar a verdadeira origem do ataque ou tentar obter acesso a serviços de rede restritos a determinados endereços IP.

O PF oferece alguma proteção contra spoofing de endereços por meio da palavra-chave antispoof:

```
antispoof [log] [quick] for interface [af]
```

Exemplo:

```
antispoof for fxp0 inet
```

Quando um conjunto de regras é carregado, todas as ocorrências da palavra-chave antispoof são expandidas em duas regras de filtragem. Supondo que a interface de saída tenha o endereço IP 10.0.0.1 e uma máscara de sub-rede de 255.255.255.0 (ou seja, a / 24), a regra antispoof acima se expandirá para:

```
block in on ! fxp0 inet from 10.0.0.0/24 to any
```

```
block in inet from 10.0.0.1 to any
```

Mostrar sistema operacional passivo

```
pfctl -s ospf
```

IP Options

Por padrão, o PF bloqueia pacotes com opções de IP (IP options) definidas. Isso pode tornar o trabalho mais difícil para os utilitários de impressão digital do sistema operacional, como o nmap. Se você tem um aplicativo que requer a passagem desses pacotes, como multicast ou IGMP, você pode usar a diretiva allow-opts:

```
pass in quick on fxp0 all allow-opts
```

Exemplo de configuração para o PF

```
nano /etc/pf.conf
```

```
int_if = "dc0"
```

```
lan_net = "192.168.0.0/24"
```

```
# table containing all IP addresses assigned to the firewall
table <firewall> const { self }
```

```
# don't filter on the loopback interface
set skip on lo0
```

```
# scrub incoming packets
match in all scrub (no-df)
```

```
# set up a default deny policy
block all
```

```
# activate spoofing protection for all interfaces
block in quick from urpf-failed
```

```
# only allow ssh connections from the local network if it's from the
# trusted computer, 192.168.0.15. use "block return" so that a TCP RST is
# sent to close blocked connections right away. use "quick" so that this
# rule is not overridden by the "pass" rules below.
block return in quick on $int_if proto tcp from ! 192.168.0.15 to $int_if port ssh
```

```
# pass all traffic to and from the local network.
# these rules will create state entries due to the default
# "keep state" option which will automatically be applied.
pass in on $int_if from $lan_net
pass out on $int_if to $lan_net
```

```
# pass tcp, udp, and icmp out on the external (Internet) interface.
# tcp connections will be modulated, udp/icmp will be tracked statefully.
pass out on egress proto { tcp udp icmp } all modulate state
```

```
# allow ssh connections in on the external interface as long as they're
# NOT destined for the firewall (i.e., they're destined for a machine on
# the local network). log the initial packet so that we can later tell
# who is trying to connect.
# Uncomment last part to use the tcp syn proxy to proxy the connection.
pass in log on egress proto tcp to ! <firewall> port ssh # synproxy state
```

```
#/etc/pf.conf
# $OpenBSD: pf.conf,v 1.54 2014/08/23 05:49:42 deraadt Exp $
#
# See pf.conf(5) and /etc/examples/pf.conf
```

```
## Início ##
me="vio0"
table <bruteforcers> persist
table <trusted> persist file "/etc/trusted"
icmp_types = "echoreq"
junk_ports="{ 135,137,138,139,445,68,67,3222 }"
junk_ip="224.0.0.0/4"
```

```
set skip on lo
```

```
block return # block stateless traffic
pass # establish keep-state
```

```
# By default, do not permit remote connections to X11
block return in on ! lo0 proto tcp to port 6000:6010
```

```
# ---- Tables ----
```

```
table <bruteforce> persist
block in quick from <bruteforce>
```

```
table <rfc1918> const { 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 }
table <spammers> persist
block in on fxp0 from { <rfc1918>, <spammers> } to any
```

```
set loginterface vio0
```

```
# ---- First rule obligatory "Pass all on loopback"
pass quick on lo0 all
```

```
# ---- Block junk logs
block quick proto { tcp, udp } from any to $junk_ip
block quick proto { tcp, udp } from any to any port $junk_ports
```

```
# ---- Second rule "Block all in and pass all out"
block in log all
pass out all keep state
```

```
##### FIREWALL #####
```

```
# ---- Allow all traffic from my Home
pass quick proto {tcp, udp} from 45.77.195.154 to $me keep state
```

```
# ---- block SMTP out
block quick proto tcp from $me to any port 25
```

```
# ---- Allow incoming Web traffic
pass quick proto tcp from any to $me port { 80, 443 } flags S/SA keep state
```

```
# ---- Allow my team member SSH access
pass quick proto tcp from 45.77.195.154 to $me port 65522 flags S/SA keep state
```

```
# ---- Block bruteforcers
block log quick from <bruteforcers>
```

```
# ---- Allow SSH from trusted sources, but block bruteforcers
pass quick proto tcp from <trusted> to $me port 65522 \
flags S/SA keep state \
(max-src-conn 10, max-src-conn-rate 20/60, \
overload <bruteforcers> flush global)
```

```
# ---- Allow ICMP
pass in inet proto icmp all icmp-type $icmp_types keep state
pass out inet proto icmp all icmp-type $icmp_types keep state
## Final ##
```

Extensões do PHP 7.0.23

```
pkg_add php-bz2-7.0.23 php-cgi-7.0.23 php-curl-7.0.23 php-dba-7.0.23 php-gd-7.0.23
php-gmp-7.0.23 php-imap-7.0.23 php-intl-7.0.23 php-ldap-7.0.23 php-7.0.23 php-mcrypt-
7.0.23 php-mysqli-7.0.23 php-odbc-7.0.23 php-pcntl-7.0.23 php-pdo_dblib-7.0.23 php-
pdo_mysql-7.0.23 php-pdo_pgsql-7.0.23 php-pgsql-7.0.23 php-pspell-7.0.23 php-shmop-
7.0.23 php-snmp-7.0.23 php-soap-7.0.23 php-tidy-7.0.23 php-xmlrpc-7.0.23 php-xsl-7.0.23
php-zip-7.0.23
```

rc.conf

```
# $OpenBSD: rc.conf,v 1.216 2017/05/30 12:04:26 tb Exp $
#/etc/rc.conf
# DO NOT EDIT THIS FILE!!
#
# This file defines the default service selection as shipped in a
# release. Upgrades of your system will modify this file.
#
# To select the service options you desire, please override these
# options in the file /etc/rc.conf.local
#
# DO NOT EDIT THIS FILE!!

# Set these variables to "NO" to turn the respective service off.
# Set them to "" to run them with the default flags.
# Otherwise, these variables override the default flags.
apmd_flags=NO
bgpd_flags=NO
bootparamd_flags=NO
cron_flags=
dhcpcd_flags=NO
dhcrelay_flags=NO      # for normal use: "-i interface [server]"
dvmrpd_flags=NO
eigrpd_flags=NO
ftpd_flags=NO         # set to NO if ftpd is running out of inetd
ftpproxy_flags=NO
ftpproxy6_flags=NO
hostapd_flags=NO
hotplugd_flags=NO
httpd_flags=""
identd_flags=NO
ifstated_flags=NO
iked_flags=NO
inetd_flags=NO
isakmpd_flags=NO
iscsid_flags=NO
ldapd_flags=NO
ldattach_flags=NO     # for normal use: "[options] linedisc cua-device"
ldomd_flags=NO
ldpd_flags=NO
lpd_flags=NO         # for normal use: "" (or "-l" for debugging)
mopd_flags=NO
mrouted_flags=NO     # be sure to enable multicast below
npppd_flags=NO
nsd_flags=NO
ntpd_flags=
ospfd_flags=NO
ospf6d_flags=NO
pflogd_flags=        # add more flags, e.g. "-s 256"
```

```
radiusd_flags=NO
rarpd_flags=NO
rbootd_flags=NO
relayd_flags=NO
rebound_flags=NO
ripd_flags=NO
route6d_flags=NO      # be sure to set net.inet6.ip6.forwarding=1
rtadvd_flags=NO      # for normal use: list of interfaces
                    # be sure to set net.inet6.ip6.forwarding=1
sasyncd_flags=NO
sensorsd_flags=NO
slaacd_flags=
slowcgi_flags=NO
smtpd_flags=
sndiod_flags=
snmpd_flags=NO
spamd_flags=NO      # also see spamd_black below
spamlogd_flags=    # use eg. "-i interface" and see spamlogd(8)
sshd_flags=
switchd_flags=NO
syslogd_flags=    # add more flags, e.g. "-u -a /chroot/dev/log"
tftpd_flags=NO
tftpproxy_flags=NO
unbound_flags=NO
vmd_flags=NO
watchdogd_flags=NO
wsmoused_flags=NO  # for enabling console mouse support (i386 alpha amd64)
                    # for ps/2 or usb mice: "", serial: "-p /dev/cua00"
xenodm_flags=NO    # on some architectures, you must also
                    # disable console getty in /etc/ttys

# services related to RPC, NFS, and YP
amd_flags=NO      # also see amd_master below
lockd_flags=NO
mountd_flags=NO
nfsd_flags=NO
portmap_flags=NO  # note: inetd(8) rpc services need portmap too
statd_flags=NO
ypbind_flags=NO
ypldap_flags=NO
ypserv_flags=NO

# set the following to "YES" to turn them on
pf=YES          # Packet filter / NAT
ipsec=NO       # IPsec
check_quotas=YES  # NO may be desirable in some YP environments
accounting=NO    # process accounting (using /var/account/acct)

# Multicast routing configuration
# Please look at netstart(8) for a detailed description if you change these
```

```

multicast=NO          # Reject IPv4 multicast packets by default

# miscellaneous other flags
amd_master=/etc/amd/master  # AMD 'master' map
library_aslr=YES          # set to NO to disable library randomization
savecore_flags=          # "-z" to compress
spamd_black=NO           # set to YES to run spamd without greylisting
shlib_dirs=              # extra directories for ldconfig, separated
                          # by space

sshd_enable=YES
ntpd_enable=YES
pf_enable=YES
pf_rules=/etc/firewall
pf_rules=/etc/firewall
pf_flags=
pflog_enable=YES
pflog_logfile="/var/log/pflog"
pflog_flags=
sendmail_enable="NONE"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
mysqld_flags=""

mysql_server_enable=YES

# rc.d(8) packages scripts
# started in the specified order and stopped in reverse order
pkg_scripts="mysqld"

```

Redes no OpenBSD

As interfaces são nomeadas pelo tipo de placa e não pela conexão.

Exemplos: fxp0, enc0

ifconfig

netstat

/etc/hostname

/etc/hosts

Logs das interfaces

pflog

Defaults hostname e gateway

```
/etc/myname
```

```
/etc/mygate
```

Ambos usam apenas uma única linha

```
cat /etc/resolv.conf
```

```
search example.com  
nameserver 125.2.2.4  
nameserver 125.2.2.5  
lookup file bind
```

Para efetuar as mudanças efetue um reboot ou execute

```
sh /etc/netstart
```

Sempre que efetuar alterações em placas de rede no OpenBSD efetue um reboot

Testando

```
netstat -rn
```

```
route show
```

```
cat /etc/hostname.dc0
```

9.6 – Ubuntu com LAMP

Servidor Criado com o Ubuntu 16.04 na DO Limpo

Tamanho - US\$ 5,00/mês

Data - 08/03/2018

Londres

ubuntu-llamp

159.65.91.82

O objetivo deste servidor é de instalar o LAMP para abrigar um site com Joomla.

Conectar pelo desktop com ssh

Após trocar a senha na console (poderia ter feito no terminal do desktop) conectei pelo desktop

```
ssh root@159.65.91.82
```

UFW está inativo

```
ufw status
```

Configurando o UFW

Como o ufw está limpo

```
ufw enable
```

```
ufw allow 65522
```

```
ufw logging on
```

```
ufw allow http
```

```
ufw allow https
```

```
ufw status verbose
```

Criar diretório para backup dos scripts

```
mkdir /root/backup
```

Adicionar usuário

```
adduser ribafs
```

Adicionar usuário ao SUDO

```
cp /etc/sudoers /root/backup
```

```
nano /etc/sudoers
```

Adicione

```
ribafs ALL=(ALL) NOPASSWD:ALL
```

Adicionar usuário ao ssh e reforçar a segurança do mesmo

```
cp /etc/ssh/sshd_config /root/backup
```

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

Alterar/descomentar:

```
Port 5522  
LoginGraceTime 30  
PermitRootLogin no
```

Adicionar ao final
AllowUsers ribafs

```
service ssh restart
```

Atualizar Ubuntu

```
apt update -y  
apt upgrade -y  
reboot
```

Conectar via desktop com ribafs

```
ssh -p 5522 ribafs@159.65.91.82
```

Passar para root
sudo su

Instalar pacotes básicos

```
apt install unzip mc aptitude
```

Adicionar partição de swap com 2GB

```
dd if=/dev/zero of=/swapfile bs=1M count=2048
mkswap /swapfile
chmod 600 /swapfile
swapon /swapfile
```

```
nano /etc/fstab
Adicionar ao final
```

```
/swapfile  swap  swap  defaults  0  0
```

```
Testar
free -m
```

Exportar a chave do ssh do desktop para o servidor

Acessar o servidor como ribafs e execute:

```
su - ribafs
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_ribafs -t dsa (Enter 2 vezes)
cat ../.ssh/id_ribafs*.pub > ../.ssh/authorized_keys
chmod 600 ../.ssh/*
exit
```

Acessar o desktop

```
ssh-copy-id ribafs@159.65.91.82 -p 55522
```

Entrar a senha do servidor

Agora pode fazer login sem senha usando

```
ssh -p 55522 ribafs@159.65.91.82
```

Criar script para limpar o cache da RAM

```
nano /usr/local/bin/m
```

```
sysctl -w vm.drop_caches=3
swapoff -a
swapon -a
```

```
chmod +x /usr/local/bin/m
```

Executar com root

Observe os valores

```
free -m
```

Execute

```
m
```

Execute novamente e compare com os valores anteriores

```
free -m
```

Criar um script para configurar as permissões do /var/www/html

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

```
#!/bin/sh
clear;
echo "Aguarde enquanto configuro as permissões do /var/www/html/$1";
echo "";
chown -R www-data:www-data /var/www/html/$1;
find /var/www/html/$1 -type d -exec chmod 755 {} \;
find /var/www/html/$1 -type f -exec chmod 654 {} \;
echo "";
echo "Concluído!";
```

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

Executar somente após instalar o Apache

Executando no diretório /var/www/html/portal

```
perms portal
```

Executando no diretório /var/www/html

```
perms
```

Executo sempre que faço alguma alteração como root no /var/www/html

Agora vou instalar os componentes do LAMP, aliás, do AMP, pois o L já se foi, que é o Ubuntu

Usarei o arquivo 2lamp

Agora irei instalar os componentes do AMP

Apache, MySQL e PHP

O Ubuntu 16.04 vem por padrão com o PHP 7.0, o MySQL 5.7 e o Apache 2.4

Instalar o LAMP com um script

Usarei um shell script para realizar a instalação destes componentes e efetuar algumas configurações

```
ub1604_lamp.sh
```

Basta enviar para o servidor usando o scp

- Copiar para a pasta /home/ribafs no desktop
- Acessar o terminal e executar:
 `scp -P 55522 ub1604_lamp.sh ribafs@159.65.91.82:/tmp`

Agora basta executar o mesmo

Instalar o LAMP

Acessar o servidor

```
sh /tmp/ub1604_lamp.sh
```

Logo ao executar ele abre um menu usando a biblioteca dialog

```
1 Atualizar Repositórios
2 Instalar Servidor Web e Cia
3 Efetuar o Upgrade da Distribuição
0 Sair
```

= Mantenha o item 1 selecionado e tecle Enter para atualizar a distribuição. Ele voltará para o menu

= Selecione com a seta para baixo o item 2 e tecle Enter. Aguarde...

= Na primeira interação ele pede a senha do MySQL. Digite e tecle Enter. Repita e tecle Enter

= A próxima interação ele mostra na tela a mensagem

Configurar .htaccess no Apache 2.4 trocando None por All
Aperte ENTER para configurar o Apache.

Tecla Enter apenas
Altere as linhas para configurar o .htaccess e mod_rewrite

Role a tela até as ocorrências de <Directory >

Antes da primeira ocorrência de <Directory > digite:
ServerName localhost

Logo mais abaixo mude de None para All deixando assim:

```
<Directory />
  Options FollowSymLinks
  AllowOverride All
  Require all denied
</Directory>

<Directory /usr/share>
  AllowOverride All
  Require all granted
</Directory>

<Directory /var/www/>
  Options Indexes FollowSymLinks
  AllowOverride All
  Require all granted
</Directory>
```

Salve e feche com Ctrl+O e Ctrl+X

= Selecione o item 3 e tecle Enter para que seja feito o upgrade da distribuição

= Agora selecione o 0 para Sair

Verificações

```
php -v
apache2 -v
mysql -V
```

Reforçar a segurança do mysql

```
mysql_secure_installation
```

Change the password for root ? ((Press y|Y for Yes, any other key for No) : n

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
All done!

Agora implementar o SSL para ser usado no administrador do site em Joomla

Usando o arquivo 3ssl
Aplicando SSL ao Apache

```
a2enmod ssl
```

```
service apache2 restart
```

```
mkdir /etc/apache2/ssl
```

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
```

Responda às perguntas:

Country Name (2 letter code) [XX]:BR
State or Province Name (full name) []:Ceará
Locality Name (eg, city) [Default City]:Fortaleza
Organization Name (eg, company) [Default Company Ltd]:FreeLancer
Organizational Unit Name (eg, section) []:Free
Common Name (eg, your name or your server's hostname) []:ribafs.org
Email Address []:ribafs@gmail.com

```
nano /etc/apache2/sites-available/default-ssl.conf
```

Remover todo o conteúdo e deixar somente:

```
<IfModule mod_ssl.c>  
  <VirtualHost _default_:443>  
    ServerAdmin ribafs@gmail.com  
    ServerName 159.65.91.82  
    #ServerAlias www.ribafs.org  
    DocumentRoot /var/www/html  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
    SSLEngine on  
    SSLCertificateFile /etc/apache2/ssl/apache.crt  
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key  
    <FilesMatch "\.(cgi|shtml|phtml|php)$">  
      SSLOptions +StdEnvVars  
    </FilesMatch>  
    <Directory /usr/lib/cgi-bin>  
      SSLOptions +StdEnvVars  
    </Directory>  
    BrowserMatch "MSIE [2-6]" \  
      nokeepalive ssl-unclean-shutdown \  
      downgrade-1.0 force-response-1.0
```

```
    BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
  </VirtualHost>
</IfModule>
```

```
a2ensite default-ssl.conf
```

```
service apache2 restart
```

Testar

```
http://159.65.91.82
```

```
https://159.65.91.82
```

```
OK
```

Agora Instalar o site com Joomla

Usando o arquivo 4joomla

Referências

<https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-ubuntu-14-04>

Enviar o site para o Servidor

Acessar o desktop

- Copiar o arquivo zip para o /home/ribafs

- Enviar o arquivo de backup criado com o Akeeba Backup para o servidor executando no terminal

```
scp -P 55522 portal.zip ribafs@159.65.91.82:/tmp
```

Criar o banco de dados para o site e o usuário para o mesmo

Acessar o servidor

```
mysql -uroot -p
```

```
create database portal;
```

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'  
WITH GRANT OPTION;  
\q
```

Descompactar o arquivo

```
cd /tmp  
unzip portal.zip -d /var/www/html/portal  
Ajustar as permissões executando  
perms portal
```

Ajustes no php.ini

```
nano /etc/php/7.0/apache2/php.ini  
Altere os dois abaixo  
date.timezone = America/Fortaleza  
output_buffering = Off  
service apache2 restart
```

Restaurando o backup do site, ou seja, instalando o site

Como é o restore de um backup feito com o Akeeba Backup precisamos configurar toda a instalação em alguns passos

Abrir o site em

<http://159.65.91.82/portal>

Pre-installation check and Recommended

Na primeira tela ele mostra uma checagem dos requisitos e se todos foram ou não satisfeitos. Caso tenha algum que não tenha sido satisfeito faça a alteração do php.ini e reinicie o apache então volte para a página e clique em Check again. Agora, que tá tudo verde, apenas clique em Next

Restoration

Database server host name - localhost
User name - portal
Password - senhaforte

Database name - portal

Clique em Next

Se aparecer um popup dizendo que a senha do banco contém caracteres especiais e que isso pode dar problema. Leia as recomendações. Apenas clique no OK do popup.

Database Restoration

Quando esta etapa finalizar clique no botão Next step do popup

Finished

Apenas entre com a senha do Super User em

Super User settings

Super User - ribafs

E-mail - ribafs@gmail.com

Password - senhaforte

Password (repeat) - senhaforte

Remover diretório Installation

Clique no botão

Remove the Installation directory

Ready to start

Clique no botão

Visit your site's front-end

Com isso o site aparece

<http://159.65.91.82/portal>

<https://159.65.91.82/portal/administrator>

Backup

Agora faça um backup completo com o componente Akeeba e quando terminar restaure por exemplo para a pasta
`/var/www/html/portal2`

Crie o banco portal2, pode ser o mesmo user e senha

Restaure pela web:

http://159.65.91.82/portal2

Agora implementar a autenticação do Apache para proteger o diretório administrator do site com senha

Usando o arquivo 5auth

Proteger diretório administrator com senha pelo Apache

```
htpasswd -c /etc/apache2/.htpasswd ribafs
```

Visualizando user e senha

```
cat /etc/apache2/.htpasswd
```

Editar o arquivo do site default e alterar assim deixando como abaixo:

```
nano /etc/apache2/sites-available/000-default.conf
```

Adicione ao final do arquivo, antes de </VirtualHost>

```
<Directory "/var/www/html/administrator">
  AuthType Basic
  AuthName "Acesso Restrito"
  AuthUserFile /etc/apache2/.htpasswd
  Require valid-user
</Directory>
```

Para que fique assim

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined

  <Directory "/var/www/html/portal/administrator">
    AuthType Basic
    AuthName "Acesso Restritot"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
  </Directory>
</VirtualHost>
```

Testar sintaxe

```
apache2ctl configtest
```

Agora para o default-ssl.conf

```
nano /etc/apache2/sites-available/default-ssl.conf
```

Adicione ao final do arquivo, antes de </VirtualHost>

```
<Directory "/var/www/html/portal/administrator">
  AuthType Basic
  AuthName "Acesso Restrita"
  AuthUserFile /etc/apache2/.htpasswd
  Require valid-user
</Directory>
```

Para que fique assim

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin ribafs@gmail.com
    ServerName 159.65.91.82
    #ServerAlias www.ribafs.org
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
    <FilesMatch "\.(cgi|shtml|phtml|php)$">
      SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
      SSLOptions +StdEnvVars
    </Directory>
    BrowserMatch "MSIE [2-6]" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
    BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
  <Directory "/var/www/html/portal/administrator">
    AuthType Basic
    AuthName "Acesso Restritot"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
  </Directory>
</VirtualHost>
</IfModule>
```

Reiniciar o Apache
service apache2 restart

Testar

<https://159.65.91.82/portal/administrator>

Funcionou.

Crédito

<https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/>

Agora vou efetuar o backup

Usando o arquivo 6backup

Efetuando Backup dos scripts e do site

Ao final, após tudo configurado, instalado e o site instalado então efetuar novamente o backup dos scripts mas com prefixo OH

```
cd /root/backup
cp /etc/php/7.0/apache2/php.ini OKphp.ini
cp /etc/apache2/apache2.conf OKapache2.conf
cp /etc/apache2/sites-available/000-default.conf OK000-default.conf
cp /etc/apache2/sites-available/default-ssl.conf OKdefault-ssl.conf
```

```
tar czpvf ub1604lamp.tar.gz *
```

```
cp ub1604lamp.tar.gz /tmp
```

Em caso de algum problema e se perder o controle podemos restaurar o respectivo script.

No desktop

```
scp -P porta ribafs@159.65.91.82:/tmp/ub1604* .
```

Guardar bem estes scripts para em caso de alteração com problema poder restaurar.

Em caso de algum problema e se perder o controle podemos restaurar o respectivo script.

Backup do site

Efetuar backup com o Akeeba

Ajustar as permissões

perms portal

Acessar o administrador

Componentes - Akeeba Backup

Backup Now

Backup Now1

Ele recomenda que não mude para outra página antes que o backup termine

Aguardar...

Backup concluído

Mover o backup para o /tmp

```
cd /tmp
```

```
mv /var/www/html/portal/administrator/components/com_akeeba/backup/portal* .
```

Acessar o desktop e baixar com scp

```
scp -P 55522 ribafs@159.65.91.82:/tmp/ub1604* .
```

Agora guarde com bastante cuidado os script e o backup do site, para quando, se, acontecer algum problema possa restaurar.

A restauração de um script acontece apenas sobrescrevendo o existente com o do backup.

Ja o site precisa descompactar em um diretório dentro de /var/www/html e abrir o site para a restauração.

Boa sorte.

9.7 – Ubuntu com LEMP

Criar um servidor com Ubuntu 16.04 limpo na DigitalOcean

Tamanho de 5 US\$

London

167.99.80.172

Nome - ubuntu-llemp

Conexão via ssh pelo desktop

A criação de servidores Ubuntu limpo, ou seja, que é apenas o servidor, permite conectar via ssh com root pelo desktop.

Já a versão LEMP vem com o firewall habilitado e bloqueia este acesso.

```
ssh root@167.99.80.172
```

Atualizar a distribuição

```
apt update -y  
apt upgrade -y  
reboot
```

Obs.: a cada reboot o Ubuntu remove tudo do /tmp

Usar os script criados na versão LEMP

Enviar os scripts com scp para o servidor

Enviar o script que instala o LEMP no servidor

Enviar por scp

```
Executar  
sh /tmp/ub1604_lemp.sh
```

```
apt autoremove
```

Verificar

```
php -v = 7.0.25  
nginx -v = 1.10.3
```

```
mysql -V = 5.7.21
```

Reforçar a segurança do MySQL

```
mysql_secure_installation
```

Teste

```
http://167.99.80.172
```

Configurar script do site default

Copiar o script do backup ribafs.conf para /etc/nginx/sites-available/

```
service nginx reload
```

Copiar o script www.conf para /etc/php/7.0/fpm/pool.d/

```
nano /etc/php/7.0/fpm/php.ini
```

Mudar

```
cgi.fix_pathinfo=0;  
date.timezone = America/Fortaleza;
```

```
service php7.0-fpm reload
```

```
nano /var/www/html/info.php
```

```
<?php  
phpinfo();
```

```
http://167.99.80.172/info.php
```

Beelza!

```
http://167.99.84.122
```

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

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

```
no location php
```

```
fastcgi_intercept_errors on;
```

```
service nginx restart
```

Adicionar algumas extensões

```
apt install -y php7.0-xm1 php7.0-zip
```

Enviar os arquivos de backup do desktop para a pasta /tmp do servidor

```
portal.zip  
portal.sql
```

Instalar na pasta /var/www/html/portal

```
cd /tmp
```

Criar o banco e o usuário e importar o script para o banco

```
Mostrar senha do mysql  
cat /root/.digitalocean_password
```

```
Reforçar segurança  
mysql_secure_installation
```

```
mysql -uroot -p
```

```
create database portal;  
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'  
WITH GRANT OPTION;
```

```
apt install -y unzip mc
```

```
unzip portal.zip -d /var/www/html/portal
```

Mudar as permissões do portal. Criar o script

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

```
#!/bin/sh  
clear;  
echo "Aguarde enquanto configuro as permissões do /var/www/html/$1";  
echo "";  
chown -R www-data:www-data /var/www/html/$1;  
find /var/www/html/$1 -type d -exec chmod 2755 {} \;  
find /var/www/html/$1 -type f -exec chmod 2644 {} \;  
echo "";  
echo "Concluído!";
```

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

Aplicando SSL ao Nginx

```
mkdir /etc/nginx/ssl/
```

```
openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout
/etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt
```

Responda às perguntas:

```
Country Name (2 letter code) [XX]:BR
State or Province Name (full name) []:Ceará
Locality Name (eg, city) [Default City]:Fortaleza
Organization Name (eg, company) [Default Company Ltd]:FreeLancer
Organizational Unit Name (eg, section) []:Free
Common Name (eg, your name or your server's hostname) []:ribafs.org
Email Address []:ribafs@gmail.com
```

```
ls /etc/nginx/ssl/nginx.crt
```

```
openssl dhparam -out /etc/nginx/ssl/dhparam.pem 4096
```

This is going to take a long time
Aguarde um bom tempo...

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

Adicione para o bloco server inicial

```
server {
    ...
    server_name IP; # ou ribafs.org www.ribafs.org

    ### SSL Config
    listen 443 ssl;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/nginx/ssl/dhparam.pem;
    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;

    if ($request_method !~ ^(GET|HEAD|POST)$ )
    {
        return 405;
    }
}
```

Adicionar ao location /

```
location / {
```

```
    autoindex on;
    try_files $uri $uri/ =404;
}
```

...

Proteção contra ataques Clickjacking
nano /etc/nginx/nginx.conf

Adicionar ao bloco http
add_header X-Frame-Options "SAMEORIGIN";

Descomente a linha
server_tokens off;

service nginx restart
service php7.0-fpm restart

Testar

<https://167.99.80.172>

Logs

Em caso de problema ver logs

```
tail -f /var/log/nginx/error.log
```

Agora proteger diretório administrator com senha usando o arquivo

4senha_diretorio

Instalar um site em Joomla na pasta /var/www/html/portal

Enviar os arquivos portalxxx.zip e o portalxxx.sql do desktop para a pasta /tmp do servidor

Este site será instalado no raiz /var/www/html

No desktop copiar os dois arquivos para a pasta /home/ribafs
scp -P porta portal* ribafs@IP:/tmp

No servidor
cd /tmp

Criar o banco e um usuário dono dele

```
mysql -uroot -p
create database portal;
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senhaforte'
WITH GRANT OPTION;
\q

mysql -uroot -p portal < portalxxx.sql
```

Descompactar o arquivo

```
cd /tmp

unzip portalxxx.zip -d /var/www/html

Ajustar permissões permissões do /var/www/html

perms

Efetuar ajustes no /var/www/html/configuration.php se necessário.
```

Instalar o site em

```
http://167.99.80.172

Ajustar para o Joomla

nano /etc/nginx/sites-available/default

Altere o location / para

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

service nginx restart

nano /etc/php/7.0/fpm/php.ini

Mudar
output_buffering = Off

service php7.0-fpm restart
service nginx restart
```

Redirecionar acesso ao raiz para /portal

Removi index.html e info.php do raiz

```
nano /var/www/html/index.php
```

```
<?php  
header('location: portal');
```

Depois de testado o site e configurado novamente para proteger o administrator com SSL então efetuar um backup full para guardar. Usarei o componente SimpleBackup

Backup e Restore

Agora faça um backup completo com o akeeba e quando terminar restaure por exemplo para a pasta

```
/var/www/html/portal2
```

Crie o banco portal2, pode ser o mesmo user e senha

Restaure pela web:

```
http://167.99.80.172/portal2
```

Agora vou implementar o SSL para usar no administrator usando o arquivo

```
3ssl_nginx
```

Proteger diretório com nhinx

Instalar

```
apt install -y apache2-utils
```

```
htpasswd -c /etc/nginx/.htpasswd ribafs
```

```
cat /etc/nginx/.htpasswd
```

Editar o default.conf e alterar assim deixando assim:

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

```
#/etc/nginx/sites-available/default  
server {  
    listen 80 default_server;  
  
    root /var/www/html;  
    index index.php index.html index.htm;
```

```
auth_basic "Administrator's Area";
auth_basic_user_file /etc/nginx/.htpasswd;

# Make site accessible from http://localhost/
server_name 167.99.80.172;
server_name_in_redirect off;

listen 443 ssl;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/ssl/dhparam.pem;
ssl_certificate /etc/nginx/ssl/nginx.crt;
ssl_certificate_key /etc/nginx/ssl/nginx.key;

if ($request_method !~ ^(GET|HEAD|POST)$ )
{
    return 405;
}

location / {
    auth_basic off;
    autoindex on;
    try_files $uri $uri/ /index.php?$args;
}

error_page 404 /404.html;
error_page 500 502 503 504 /50x.html;
location = /50x.html {
    root /var/www/html;
}

location ~ \.php$ {
    auth_basic off;
    try_files $uri =404;
    include /etc/nginx/fastcgi_params;
    fastcgi_pass unix:/run/php/php7.0-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    fastcgi_intercept_errors on;
}

location /administrator {
    auth_basic "Restrito";
    auth_basic_user_file /etc/nginx/.htpasswd;
}

location ~ /\.ht {
    deny all;
}
```

```

    }
}

```

```

service nginx restart
service php7.0-fpm restart

```

Crédito

<https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/>

Script de instalação do LEMP

```

#!/bin/bash
#
# Criado/adaptado por Ribamar FS - http://ribafs.org
#
apt-get install dialog;
#
while :
do
    clear
    servico=$(dialog --stdout --backtitle 'Instalação de pacotes no Ubuntu Server 16.04 LTS -
64' \
        --menu 'Selecione a opção com a seta ou o número e tecle Enter\n' 0 0 0 \
        1 'Atualizar repositórios' \
        2 'Instalar Servidor Web e cia' \
        3 'Efetuar o Upgrade da distribuição' \
        0 'Sair' )
    case $servico in
        1) apt-get update;;
        2) clear;
echo "Instalar pacotes básicos. Tecla Enter para instalar!";
apt-get install -y aptitude unzip mc git;

clear;
echo "Instalar Apache e módulos. Tecla Enter para instalar!";
apt-get install -y nginx php7.0-fpm;

clear;
# Instalar SGBDs somente para testes locais. Visto que o servidor é outro: 10.0.0.60
apt-get install -y mysql-server;

clear;
echo "Instalar PHP 5 e extensões. Tecla Enter para instalar!";
apt-get install -y php7.0 php7.0-bcmath php7.0 php-mbstring mcrypt mcrypt php7.0-mcrypt
php7.0-mysqlnd php7.0-gd php-pear curl php7.0-curl;
apt-get install -y php7.0-zip php-gettext php-auth php7.0-xml php7.0-xsl;

clear;
echo "Instalar suporte a cache no PHP. Tecla Enter para instalar!";

```

```
# Cache de php
apt-get -y install php-apcu;

wget http://ftp.ussg.iu.edu/linux/ubuntu/pool/main/m/memcached/memcached_1.4.25-
2ubuntu1_amd64.deb;
dpkg -i -y memcached_1.4.25-2ubuntu1_amd64.deb;
apt-get -y install php-memcache;

service nginx restart;

clear;;

    3) clear;
apt-get -y update;
apt-get -y upgrade;;
    0) clear;exit;;
esac
done
```

9.8 – FreeBSD

Após o login aparecem as informações

FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: <https://www.FreeBSD.org/releases/>

Security Advisories: <https://www.FreeBSD.org/security/>

FreeBSD Handbook: <https://www.FreeBSD.org/handbook/>

FreeBSD FAQ: <https://www.FreeBSD.org/faq/>

Questions List: <https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/>

FreeBSD Forums: <https://forums.FreeBSD.org/>

Documents installed with the system are in the `/usr/local/share/doc/freebsd/` directory, or can be installed later with: `pkg install en-freebsd-doc`
For other languages, replace "en" with a language code like `de` or `fr`.

Show the version of FreeBSD installed: `freebsd-version ; uname -a`
Please include that output and any error messages when posting questions.

Introduction to manual pages: `man man`

FreeBSD directory layout: `man hier`

Edit `/etc/motd` to change this login announcement.

Existe um usuário `toor` no sistema por padrão.
Para usá-lo precisa logar como `root` e atribuir uma senha para ele.

Por conta da natureza do FreeBSD administradores do mesmo precisam de um grande nível de experiência e disposição para o trabalho.

Criação de Servidor com FreeBSD 11.1 no DO

Novamente. Citei o DO mas claro que este roteiro de criação de servidor é genérico e não somente para o dO.

Usando uma chave `ssh`

IP - 138.197.169.181

Na criação do servidor associar a uma chave SSH anteriormente criada

`ssh root@138.197.169.181`

Não pedirá senha, mas devemos mudar logo no primeiro acesso:

`passwd root`

pkg install nano

nano /usr/local/etc/sudoers

ribafs ALL=(ALL) NOPASSWD:ALL

Criar novo usuário

adduser ribafs

nano /etc/ssh/sshd_config

Port 5522

LoginGraceTime 30

PermitRootLogin without-password

AllowUsers ribafs root

service sshd restart

Acessar pelo desktop como ribafs

ssh -p 5522 ribafs@138.197.169.181

sudo su

Atualizar

pkg update

pkg upgrade

Pacotes básicos

pkg install -y unzip wget

Para que o shell os encontre

Mudar (se desejar)

setenv EDITOR vi

para

setenv EDITOR nano

Alterando o shell default

pkg install bash

Baixar com fetch

cd ~

fetch <http://wordpress.org/latest.tar.gz>

tar -zxvf latest.tar.gz

Adicionar ao /etc/fstab
sh -c 'echo "fdesc /dev/fd fdescfs rw 0 0" >> /etc/fstab'

mount -a

Execute para atualizar o shell
bash

Para mudar para um usuário

chsh -s /usr/local/bin/bash ribafs

Para que root sem senha no SSH
PermitRootLogin without-password

Mudar o paginador default:

nano ~/.bash_profile

Mudar

export PAGER=less
export EDITOR=nano

Criar uma chave para o ssh

ssh-keygen -b 4096

Ativar o firewall IPFW

nano /etc/rc.conf

Adicione ao final

```
firewall_enable="YES"  
firewall_quiet="YES"
```

Configurar o firewall. Adicionar abaixo das 2 linhas:

```
firewall_type="workstation"  
firewall_myserver="65522 80 443"  
firewall_allowservices="any"  
firewall_logdeny="YES"
```

Pode ser assim:

```
firewall_myserver="ssh http"
```

Edite

nano /etc/rc.firewall

Após este código

```
...
for i in ${firewall_allservices} ; do
  for j in ${firewall_myservices} ; do
    case $j in
      [0-9A-Za-z]*/[Pp][Rr][Oo][Tt][Oo])
        ${fwcmd} add pass ${j%/[Pp][Rr][Oo][Tt][Oo]} from $i to me
        ;;
      [0-9A-Za-z]*/[Tt][Cc][Pp])
        ${fwcmd} add pass tcp from $i to me ${j%/[Tt][Cc][Pp]}
        ;;
      [0-9A-Za-z]*/[Uu][Dd][Pp])
        ${fwcmd} add pass udp from $i to me ${j%/[Uu][Dd][Pp]}
        ;;
      *[0-9A-Za-z])
        echo "Consider using ${j}/tcp in firewall_myservices." \
          > /dev/stderr
        ${fwcmd} add pass tcp from $i to me $j
        ;;
      *)
        echo "Invalid port in firewall_myservices: $j" > /dev/stderr
        ;;
    esac
  done
done
...
```

Adicione a linha

```
${fwcmd} add pass udp from any to me port_num
```

Salve e feche

Inicie o firewall

```
service ipfw start
```

Precisa configurar o ssh para a porta 65522 antes

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

```
service sshd restart
```

Configurar os IPs negados

```
nano /etc/sysctl.conf
```

Limitar a apenas 5 tentativas. Adicionar ao início do arquivo

```
net.inet.ip.fw.verbose_limit=3
```

Isso será efetivado no próximo boot

Para implementar na atual sessão, execute:
sysctl net.inet.ip.fw.verbose_limit=3

Ajustar o fuso horário

```
tzsetup
```

```
America  
Brazil  
Brazil
```

Adicionar swap de 1GB

Ver o swap existente em GB, caso exista
swapinfo -g

```
truncate -s 1G /swapfile  
chmod 0600 /swapfile  
sh -c 'echo "md99 none swap sw,file=/swapfile,late 0 0" >> /etc/fstab'  
swapon -aqL  
swapinfo -g
```

Memória RAM

```
pkg install freecolor
```

```
freecolor
```

```
freecolor -m -o
```

| | total | used | free | shared | buffers | cached |
|-------|-------|------|------|--------|---------|--------|
| Mem: | 962 | 622 | 340 | 0 | 0 | 0 |
| Swap: | 3072 | 84 | 2987 | | | |

```
pkg install htop
```

```
htop
```

```
top d1
```

Procurar atualizações e instalar

```
/usr/sbin/freebsd-update fetch  
freebsd-update fetch install
```

Reiniciar agora
shutdown -r now

Desabilitando soft-updates

Verificar atualizações automáticas
nano /etc/crontab

Adicione non início do arquivo
@daily root freebsd-update -t freebsd cron

Checar vulnerabilidades em softwares
pkg audit -F

Atualizar todos os softwares opcionais instalados:

Serviços

pkg search apache24

pkg install apache24

sysrc apache24_enable=yes

service apache24 start

http://159.65.50.168
OK

MySQL

pkg search mysql57

pkg install mysql57-server

sysrc mysql_enable=yes

service mysql-server start

mysql_secure_installation

PHP

pkg search php72

```
pkg install mod_php72 php72-gd php72-pdo php72-mbstring php72-xml php72-zip php72-
bcmath php72-memcache php72-pdo_mysql php72-json php72-simplexml php72-curl
php72-opcache php72-simplexml php72-mysqli
```

Adicionar ao conf do Apache

```
nano /usr/local/etc/apache24/httpd.conf
```

```
ServerName localhost
```

```
<FilesMatch "\.php$" >
    SetHandler application/x-httpd-php
</FilesMatch >
<FilesMatch "\.phps$" >
    SetHandler application/x-httpd-php-source
</FilesMatch >
```

```
<IfModule dir_module >
    DirectoryIndex index.php index.html
</IfModule >
```

```
# Descomentar a linha abaixo
```

```
LoadModule rewrite_module libexec/apache24/mod_rewrite.so
```

```
RewriteEngine On
RewriteOptions Inherit
```

```
sysrc apache24_enable=yes
```

```
service apache24 restart
```

Para instalar o Joomla no subdiretório portal fiz assim:

```
nano /usr/local/etc/apache24/httpd.conf
```

```
<Directory /usr/local/www/apache22/data/portal >
    Options Indexes FollowSymLinks
    AllowOverride All
</Directory >
```

```
service apache24 restart
```

Da documentação

```
<VirtualHost * >
    ServerName www.domain.tld
    DocumentRoot /www/domain.tld
</VirtualHost >
```

```
<VirtualHost * >
    ServerName www.someotherdomain.tld
    DocumentRoot /www/someotherdomain.tld
```

```
</VirtualHost>
```

```
Diretório web  
/usr/local/www/apache24/data
```

```
group - www  
user - www
```

```
cp /usr/local/etc/php.ini-production /usr/local/etc/php.ini
```

```
nano /usr/local/etc/php.ini
```

```
date.timezone = America/Fortaleza  
output_buffering = Off  
allow_url_fopen = On
```

```
service apache24 restart
```

```
nano /usr/local/www/apache24/data/info.php
```

```
<?php  
phpinfo();
```

```
http://138.197.169.181/info.php
```

```
rm /usr/local/www/apache24/data/info.php
```

Informações sobre pacotes

```
pkg info package_name
```

Excluindo pacote

```
pkg delete package_name
```

Remover dependências usadas

```
pkg autoremove
```

Busca

```
pkg search package_name
```

Para busca com detalhes

```
pkg search -f package_name
```

Com descrição

```
pkg search -D pattern
```

```
pkg help subcommand
```

Ativar o daemon do rsysc
rsyncd_enable="YES"

```
sudo sh -c "echo 'rsyncd_enable="YES"' >> /etc/rc.conf"
```

```
sudo service rsyncd start
```

Segurança

```
/usr/bin/netstat plunt
```

Observação

As operações em disco geralmente demoram mais no FreeBSD que nos linux.

<https://www.digitalocean.com/community/tutorials/how-to-install-an-apache-mysql-and-php-famp-stack-on-freebsd-10-1>

Vantagens dos BSD sobre os Linux

- Mais robustos
- Organização mais limpa
- Estabilidade
- Segurança
- Sistema de arquivos conservador e seguro
- Facilidade de administração do sistema
- Facilidade de instalação
- Excelente performance para execução de aplicativos web e de bancos de dados

Várias instituições educacionais e grandes corporações estão migrando para os BSD: Yahoo, Microsoft, McAfee, etc

Uma pesquisa da Netcraft mostrou que os 5 sites mais confiáveis do planeta rodam FreeBSD.

Consultoria sobre o FreeBSD

https://www.freebsd.org/commercial/consult_bycat.html

Patrocinadores

<https://gist.github.com/SaveTheRbtz/1742025>

Alguns: DARPA, Google, Nokia, Apple,

Doações

<https://www.freebsdoundation.org/donors/>

Atualizar o sistema

```
sudo freebsd-update fetch
sudo freebsd-update install
sudo pkg update
sudo pkg upgrade -y
reboot
```

Servidor

ribafs.org

1 GB Memory
25 GB Disk
LON1
FreeBSD 11.1 x64

46.101.50.99

```
pkg install nano wget mc
```

```
nano /usr/local/etc/sudoers
```

```
ribafs  ALL=(ALL) NOPASSWD:ALL
```

Criar novo usuário

```
adduser ribafs
```

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

```
Port 5522
LoginGraceTime 30
PermitRootLogin without-password
AllowUsers ribafs root
```

```
service sshd restart
```

Acessar pelo desktop como ribafs

```
ssh -p 5522 ribafs@138.197.169.181
```

Após o login aparece

```
Last login: Sat Mar 31 22:35:53 2018 from 177.130.216.50
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017
```

Welcome to FreeBSD!

Release Notes, Errata: <https://www.FreeBSD.org/releases/>
 Security Advisories: <https://www.FreeBSD.org/security/>
 FreeBSD Handbook: <https://www.FreeBSD.org/handbook/>
 FreeBSD FAQ: <https://www.FreeBSD.org/faq/>
 Questions List: <https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/>
 FreeBSD Forums: <https://forums.FreeBSD.org/>

Documents installed with the system are in the `/usr/local/share/doc/freebsd/` directory, or can be installed later with: `pkg install en-freebsd-doc`
 For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: `freebsd-version ; uname -a`
 Please include that output and any error messages when posting questions.
 Introduction to manual pages: `man man`
 FreeBSD directory layout: `man hier`

Edit `/etc/motd` to change this login announcement.
 To see how much disk space is left on your partitions, use

```
df -h
-- Dru <genesis@istar.ca>
=====
```

Veja que podemos mudar a mensagem de pós login editando:

```
nano /etc/motd
```

Esta é uma ótima característica do FreeBSD, após a instalação de cada software aparece mensagem contendo informações importantes.

```
sudo su
```

```
Para que root sem senha no SSH
PermitRootLogin without-password
```

Criar uma chave para o ssh no desktop

```
ssh-keygen -b 4096
```

Configurar o PF como firewall

Checar vulnerabilidades em softwares/auditoria

```
pkg audit -F
```

```
nano /etc/rc.conf
```

```
pf_enable="YES"
```

```
pf_rules="/etc/pf.conf"
pf_flags=""
pflog_enable="YES"
pflog_logfile="/var/log/pflog"
pflog_flags=""
```

Criar
nano /etc/pf.conf

```
interface="vtnet0"
scrub in all
block in on $interface
#allow SSH traffic from our network
pass in on $interface proto tcp from 177.130.216.50/32 to $interface port 65522
#allow HTTP (80), and HTTPS (443) to the world
pass in on $interface proto tcp from any to $interface port 80
pass in on $interface proto tcp from any to $interface port 443
# Comabte aos ataques de bruteforce
# ---- Allow SSH from trusted sources, but block bruteforcers
pass quick proto tcp from <trusted> to $interface port 65522 \
flags S/SA keep state \
(max-src-conn 10, max-src-conn-rate 20/60, \
overload <bruteforcers> flush global)
#allow outgoing traffic
pass out on $interface proto { tcp, udp } all
```

Ativando as regras

```
pfctl -nf /etc/pf.conf
```

Caso apareçam erros, corrija e execute novamente removendo o flag -n

```
pfctl -f /etc/pf.conf
```

reboot

Apenas visualizar as regras

```
pfctl -sr
```

Para Remover todas as regras do arquivo pf.conf

```
pfctl -Fa
```

```
/etc/rc.d/pf reload
```

ou
service pf reload

Veja quem está tentando se conectar ao servidor em tempo real

```
tcpdump -n -e -ttt -i pflog0
```

Mostrar logs

```
tcpdump -n -e -ttt -r /var/log/pflog
```

Ver se tem algo na tabela bruteforce

```
pfctl -t bruteforcercs -T show
```

Criar WhiteList

```
nano /etc/trusted
```

Adicionar alguns IPs

```
# Casa  
177.130.216.50
```

```
# DNOCS  
187.120.206.60
```

Implementar atualizações automáticas

```
nano /etc/crontab
```

Adicione após a linha

```
*/5 * * * * root /usr/libexec/atrun
```

```
#Esta linha  
@daily root freebsd-update -t freebsd cron
```

FAMP

Apache

```
sudo pkg search apache24
```

```
sudo pkg install -y apache24
```

```
user - www  
group - www
```

```
sudo sysrc apache24_enable=yes
```

```
sudo service apache24 start
```

Testar

```
http://46.101.50.99
```

Configurações

```
sudo nano /usr/local/etc/apache24/httpd.conf
```

```
ServerAdmin ribafs@gmail.com
```

```
ServerName www.ribafs.org
```

```
Rotação de logs, a cada 10.000 requisições gerar em torno de 1MB de log  
ErrorLog "|/usr/local/sbin/rotatelog /var/log/httpd-mysite-error-log 86400"
```

```
mod_rewrite, descomentar a linha  
LoadModule rewrite_module libexec/apache24/mod_rewrite.so
```

Mudar none para All

```
Checar  
DocumentRoot "/usr/local/www/apache24/data"
```

Checar sintaxe

```
apachectl configtest
```

```
sudo service apache24 restart
```

```
ou  
sudo apachectl restart
```

```
Logs  
/var/log/httpd-error.log  
/var/log/httpd-access.log
```

Instalar php7.1

```
sudo pkg install -y php71 mod_php71 php71-gd php71-mbstring php71-mysqli php71-xml  
php71-curl php71-tidy php71-ctype php71-tokenizer php71-simplexml php71-dom php71-  
session php71-iconv php71-hash php71-json php71-fileinfo php71-bcmath php71-zip  
php71-zlib
```

Após a instalação aparece

The 2.7.x series now uses the new subpixel hinting mode (V40 port's option) as the default, emulating a modern version of ClearType. This change inevitably leads to different rendering results, and you might change port's options to adapt it to your taste (or use the new "FREETYPE_PROPERTIES" environment variable).

The environment variable "FREETYPE_PROPERTIES" can be used to control the driver properties. Example:

```
FREETYPE_PROPERTIES=truetype:interpreter-version=35 \
  cff:no-stem-darkening=1 \
  autofitter:warping=1
```

This allows to select, say, the subpixel hinting mode at runtime for a given application.

The controllable properties are listed in the section "Controlling FreeType Modules" in the reference's table of contents (</usr/local/share/doc/freetype2/reference/ft2-toc.html>, if documentation was installed).
 Message from mod_php71-7.1.15:

```
*****
```

Make sure index.php is part of your DirectoryIndex.

You should add the following to your Apache configuration file:

```
<FilesMatch "\.php$" >
  SetHandler application/x-httpd-php
</FilesMatch>
<FilesMatch "\.phps$" >
  SetHandler application/x-httpd-php-source
</FilesMatch>
```

```
*****
```

If you are building PHP-based ports in `poudriere(8)` with ZTS enabled, add `WITH_MPM=event` to `/etc/make.conf` to prevent build failures.

Copiar

```
sudo cp /usr/local/etc/php.ini-production /usr/local/etc/php.ini-production.bakup
```

Criar link simbólico

```
sudo ln -s /usr/local/etc/php.ini-production /usr/local/etc/php.ini
```

Configurar

```
sudo nano /usr/local/etc/php.ini
```

```
date.timezone = America/Fortaleza
```

```
service apache24 restart
```

Então ele mostrou

Make sure index.php is part of your DirectoryIndex.

You should add the following to your Apache configuration file:

```
<FilesMatch "\.php$" >
```

```
    SetHandler application/x-httpd-php
</FilesMatch>
<FilesMatch "\.phps$">
    SetHandler application/x-httpd-php-source
</FilesMatch>
```

```
sudo nano /usr/local/etc/apache24/httpd.conf
```

Adicionar

```
<IfModule dir_module>
    DirectoryIndex index.php index.html
</IfModule>
```

Criar

```
sudo nano /usr/local/etc/apache24/Includes/php.conf
```

```
<IfModule dir_module>
    DirectoryIndex index.php index.html
    <FilesMatch "\.php$" >
        SetHandler application/x-httpd-php
    </FilesMatch>
    <FilesMatch "\.phps$" >
        SetHandler application/x-httpd-php-source
    </FilesMatch>
</IfModule>
```

```
sudo service apache24 restart
```

Testar

```
nano /usr/local/www/apache24/data/info.php
```

```
<?php
phpinfo();
```

```
http://167.99.175.44/info.php
```

Instalar MariaDB

```
sudo pkg search mariadb
```

```
sudo pkg install -y mariadb102-server mariadb102-client
```

```
user e group - mysql
```

Após a instalação aparece:

MariaDB respects hier(7) and doesn't check /etc and /etc/mysql for my.cnf. Please move existing my.cnf files from those paths to /usr/local/etc and /usr/local/etc/mysql.

Message from unixODBC-2.3.4:

==> NOTICE:

The unixODBC port currently does not have a maintainer. As a result, it is more likely to have unresolved issues, not be up-to-date, or even be removed in the future. To volunteer to maintain this port, please create an issue at:

<https://bugs.freebsd.org/bugzilla>

More information about port maintainership is available at:

<https://www.freebsd.org/doc/en/articles/contributing/ports-contributing.html#maintain-port>

Message from mariadb102-server-10.2.13:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!                                                                    !!
!! The default InnoDB storage engine is no longer XtraDB, check your !!
!! configuration and switch it to InnoDB                               !!
!!                                                                    !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Remember to run `mysql_upgrade` (with the optional `--datadir=<dbdir>` flag) the first time you start the MySQL server after an upgrade from an earlier version.

MariaDB respects hier(7) and doesn't check /etc and /etc/mysql for my.cnf. Please move existing my.cnf files from those paths to /usr/local/etc and /usr/local/etc/mysql.

This port does NOT include the mytop perl script, this is included in the MariaDB tarball but the most recent version can be found in the databases/mytop port

Configurar

```
sudo sysrc mysql_enable="yes"
sudo service mysql-server start
```

Reforçar a segurança

```
sudo mysql_secure_installation
```

```
mysql -u root -p
```

Criar usuário e banco

```
CREATE DATABASE portal CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE USER 'portal'@'localhost' IDENTIFIED BY 'senhaforte';
GRANT ALL PRIVILEGES ON portal.* TO 'portal'@'localhost';
FLUSH PRIVILEGES;
\q
```

Outros privilégios

ALL PRIVILEGES- como vimos anteriormente, isso daria a um usuário do MySQL todo o acesso a uma determinada base de dados (ou se nenhuma base de dados for selecionada, todo o sistema)

CREATE- permite criar novas tabelas ou bases de dados

DROP- permite deletar tabelas ou bases de dados

DELETE- permite deletar linhas das tabelas

INSERT- permite inserir linhas nas tabelas

SELECT- permite utilizar o comando Select para ler bases de dados

UPDATE- permite atualizar linhas das tabelas

GRANT OPTION- permite conceder ou revogar privilégios de outros usuários

Checar vulnerabilidades

```
pkg audit -F
```

Após checar acusou vulnerabilidades no apache24.29

Seguindo o link sugerido vi que foi corrigido no apache24.32 e 33

Então instalei os ports e instalei o apache24.33 via ports:

Usando o arquivo 6ports

Instalação do SSL no Apache 2.4 do FreeBSD 11.1

Criar o certificado:

Criar o script abaixo

```
nano ssl.sh
```

```
#!/bin/sh
mkdir -p /root/mycert
cd /root/mycert
mkdir -p /usr/local/etc/apache24/ssl.key
mkdir -p /usr/local/etc/apache24/ssl.crt
chmod 0400 /usr/local/etc/apache24/ssl.key
chmod 0400 /usr/local/etc/apache24/ssl.crt
openssl genrsa -des3 -out $1.key 1024
```

```

openssl req -new -x509 -nodes -sha256 -days 365 -key $1.key -out $1.crt
cp $1.key $1.key.orig
openssl rsa -in $1.key.orig -out $1.key
cp $1.key /usr/local/etc/apache24/ssl.key/
cp $1.crt /usr/local/etc/apache24/ssl.crt/
chmod 0400 /usr/local/etc/apache24/ssl.key/$1.key
chmod 0400 /usr/local/etc/apache24/ssl.crt/$1.crt
### Final

```

```

/usr/local/etc/apache24/ssl.crt/ribafs
chmod +x ssl.sh

```

Executar:

```
./ssl.sh ribafs
```

```
nano /usr/local/etc/apache24/httpd.conf
```

Descomentar a linha

```
Include etc/apache24/extra/httpd-ssl.conf
```

E esta

```
LoadModule ssl_module libexec/apache24/mod_ssl.so
```

```
rm /usr/local/etc/apache24/extra/httpd-ssl.conf
```

Configurar o httpd-ssl.conf para o domínio principal ribafs.org e para um subdomínio familia.ribafs.org

```
nano /usr/local/etc/apache24/extra/httpd-ssl.conf
```

```

Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
<VirtualHost _default_:443>
  DocumentRoot "/usr/local/www/apache24/data"
  ServerName www.ribafs.org:443
  ServerAdmin ribafs@gmail.com
  ErrorLog "/var/log/httpd-error.log"
  TransferLog "/var/log/httpd-access.log"

```

```
SSLEngine on
```

```

SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:
+SSLv2:+EXP:+eNULL

```

```
SSLCertificateFile "/usr/local/etc/apache24/ssl.crt/ribafs.crt"
```

```
SSLCertificateKeyFile "/usr/local/etc/apache24/ssl.key/ribafs.key"
```

```

<FilesMatch "\.(cgi|shtml|phtml|php)$">
  SSLOptions +StdEnvVars
</FilesMatch>
<Directory "/usr/local/www/apache24/cgi-bin">
  SSLOptions +StdEnvVars
</Directory>

BrowserMatch ".*MSIE.*" \
  nokeepalive ssl-unclean-shutdown \
  downgrade-1.0 force-response-1.0

  CustomLog "/var/log/httpd-ssl_request.log" "%t %h %{SSL_PROTOCOL}x %{
{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>

<VirtualHost _default_:443>
  DocumentRoot "/usr/local/www/apache24/data/familia"
  ServerName familia.ribafs.org:443
  ServerAdmin ribafs@gmail.com
  ErrorLog "/var/log/httpd-error.log"
  TransferLog "/var/log/httpd-access.log"

  SSLEngine on

  SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:
+SSLv2:+EXP:+eNULL

  SSLCertificateFile "/usr/local/etc/apache24/ssl.crt/ribafs.crt"

  SSLCertificateKeyFile "/usr/local/etc/apache24/ssl.key/ribafs.key"

<FilesMatch "\.(cgi|shtml|phtml|php)$">
  SSLOptions +StdEnvVars
</FilesMatch>
<Directory "/usr/local/www/apache24/cgi-bin">
  SSLOptions +StdEnvVars
</Directory>

BrowserMatch ".*MSIE.*" \
  nokeepalive ssl-unclean-shutdown \
  downgrade-1.0 force-response-1.0

  CustomLog "/var/log/httpd-ssl_request.log" "%t %h %{SSL_PROTOCOL}x %{
{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>

```

Dica: Cuidado com caracteres malucos criados com copiar e colar. Se precisar digite tudo.

service apache24 restart

Testar:

<https://www.ribafs.org/info.php>

<https://www.rhyous.com/2009/11/06/installing-an-apache-ssl-on-freebsd-using-the-ports-tree/>

Protegendo diretório com a autenticação do Apache 2.4 no FreeBSD 11.1

```
htpasswd -c /usr/local/etc/apache24/.htpasswd_access ribafs
```

```
cat /usr/local/etc/apache24/.htpasswd_access
```

Criar um directório protegido

Adicionar

```
nano /usr/local/etc/apache24/httpd.conf
```

Abaixo do bloco <Directory> existente

```
<Directory "/usr/local/www/apache24/data/administrator">
  AuthType Basic
  AuthName "Restricted Content"
  IndexIgnore .*
  AuthName protectthis
  AuthUserFile /usr/local/etc/apache24/.htpasswd_access
  AuthGroupFile /usr/local/etc/apache24/.htpasswd_access_group
  AuthType Basic
  <Limit GET>
    # A linha abaixo é para um grupo
    #Require valid-user
    require user ribafs
  </Limit>
</Directory>
```

```
mkdir /usr/local/www/apache24/data/administrator
```

```
service apache24 restart
```

Testando

<https://ribafs.org/administrator/>

Caso o DNS não tenha propagado ainda use o iP.

FreeBSD Ports

Uma grande vantagem de instalar programas via ports é o fato de podermos customizar as opções de instalação.

Caso não haja nenhuma necessidade de customização na instalação a opção é o pkg.

```
portsnap fetch
portsnap extract
portsnap update
portsnap fetch update
```

Instalar apache24 atualizado

```
cd /usr/ports
```

```
make search name=apache24
```

```
Mostrou
apache24-2.4.33
```

Enquanto que o instalado pelo pkg é o apache24-2.4.29, que tem vulnerabilidades

```
cd /usr/ports/www/apache24
```

```
pkg delete apache24
```

```
make install
make clean
```

Reinstalei o mod_php

```
pkg install mod_php71
```

```
service apache24 restart
```

Rodando checagem de vulnerabilidades

```
pkg audit -F
```

Agora mostrou que não existe vulnerabilidade

```
Listar ports
portmaster -l
```

Checar pacotes instalados

```
pkg install portmaster
```

```
cd /usr/ports/ports-mgmt/portmaster
```

```
sudo make install clean
```

```
portmaster -L
```

Removendo ports

```
cd /usr/ports/sysutils/lsof  
make deinstall
```

Atualizar tudo

```
portmaster -a
```

Envio do banco e dos arquivos de backup do site do desktop para o servidor

```
scp -P 55522 portal* ribafs@ribafs.org:/tmp
```

Importação do sql para o banco portal

```
cd /tmp
```

```
mysql -uroot -p portal < portal.sql
```

Descompactação do zip para /usr/share/www/apache24/data

```
unzip portal.zip -d /usr/share/www/apache24/data
```

Reinicie o Apache e o MySQL

```
service apache24 restart
```

```
service mysql-server restart
```

Ajuste de permissões do diretório web

Criar o arquivo

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

```
#!/bin/sh
```

```
clear;
```

```
echo "Aguarde enquanto configuro as permissões do /usr/local/www/apache24/data/$1";
```

```
echo "";
```

```
chown -R www:www /usr/local/www/apache24/data/$1;
```

```
find /usr/local/www/apache24/data/$1 -type d -exec chmod 755 {} \;
```

```
find /usr/local/www/apache24/data/$1 -type f -exec chmod 644 {} \;
```

```
echo "Concluído!";
```

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

Instalar Freecolor para checar espaço e memória livres

```
pkg install freecolor
```

```
freecolor -om
```

Reforçar a segurança do SSH no FreeBSD com SSHGUARD

Após a instalação e configuração com sucesso do PF

```
pkg install sshguard
```

```
2.0.0_1
```

Após a instalação mostra:

```
#####  
##
```

```
Sshguard installed successfully.
```

```
You can start sshguard as a daemon by using the  
rc.d script installed at /usr/local/etc/rc.d/sshguard .
```

```
See sshguard-setup(7) and http://www.sshguard.net/docs/setup for additional info.
```

Please note that a few rc script parameters have been renamed to better reflect the documentation:

```
sshguard_safety_thresh -> sshguard_danger_thresh  
sshguard_pardon_min_interval -> sshguard_release_interval  
sshguard_prescribe_interval -> sshguard_reset_interval
```

```
#####  
##
```

```
nano /etc/rc.conf
```

Adicione

```
# sshguard  
sshguard_enable="YES"  
sshguard_danger_thresh="30"  
sshguard_release_interval="600"  
sshguard_reset_interval="7200"
```

```
nano /etc/pf.conf
```

```
table <sshguard> persist
#...
block in quick on bge0 from <sshguard> label "ssh bruteforce"
```

A ordem das linhas acima é importante, se alterada pode causar erro no pf

```
service sshguard start
```

```
pfctl -f /etc/pf.conf
```

```
service pf start
```

Após o comando acima travou meu terminal e saiu com:
packet_write_wait: Connection to 46.101.50.99 port 65522: Broken pipe

Então fui até a hospedagem e acessei pela console

Ao efetuar o acesso pela console aparece a mensagem de que tenho e-mail

Digito mail e tecla enter
Aparecem 3. Digito 1 para ler o security

Ele me avisa para checar o setuid de arquivos e dispositivos em:
var/log/setuid.today

Também para checar permissões negativas de grupos em:
/var/log/mount.today

Checar os uid 0
root 0
toor 0

Checar contas sem senha:
/etc/login.conf

Depois de ler estes e-mails eu carreguei as regras do pf e o reiniciei

Voltei ao meu desktop e acessei o servidor sem problema

Testando

```
pgrep -lfa ssh
```

```
pfctl -t sshguard -T show
```

```
pfctl -sr
```

Questões

<https://forums.freebsd.org/threads/howto-set-up-and-configure-security-sshguard-pf.39196/>

<https://blog.mwzhang.com/2016/02/20/secure-ssh-using-sshguard-and-pf-in-freebsd/>
<https://gist.github.com/WillSquire/b0546bb8ab901f16555aba2e953767d9>

Monitorando o servidor

Memória RAM e swap
freecolor -om

Atualização dos pacotes

pkg update
pkg upgrade

Logs

/var/log/httpd-access.log
/var/log/httpd-error.log
/var/log/httpd-ssl_request.log
/var/log/messages.log
/var/log/pflog
/var/log/security

```
tcpdump -n -e -ttt -i pflog0  
tcpdump -nettr /var/log/pflog -vv "tcp and port 80"  
tcpdump -n -e -ttt -r /var/log/pflog  
tcpdump -n -e -ttt -i pflog0  
tcpdump -n -e -ttt -r /var/log/pflog port 80  
tcpdump -n -e -ttt -r /var/log/pflog port 80 and host 192.168.1.3  
tcpdump -n -e -ttt -i pflog0 host 192.168.4.2  
tcpdump -n -e -ttt -i pflog0 inbound and action block and on wi0
```

This display the log, in real-time, of inbound packets that were blocked on the wi0 interface.

Adicionar uma partição de swap de 1GB

Adicionar swap de 1GB

Ver o swap existente em GB, caso exista

```
swapinfo -g
```

```
truncate -s 1G /swapfile
```

```
chmod 0600 /swapfile
```

```
sh -c 'echo "md99 none swap sw,file=/swapfile,late 0 0" >> /etc/fstab'
```

```
swapon -aqL
```

```
swapinfo -g
```