

**Administração de Servidores Linux,
Passo-a-passo para pequenas
empresas**
(Usando Debian, Ubuntu Server e Zentyal)

Ribamar FS - 2012

Ficha Catalográfica

S725c

Administração de Servidores Linux, Passo-a-passos / Ribamar
Ferreira de Sousa. - Fortaleza: Clube de Autores, 2012

128p.

1. Servidores Linux. 2. Administração. I.
Título.

Normalização Bibliográfica

Lúcia Maria Piancó Chaves – DNOCS-CGE/MD
Margarida Lídia de Abreu Vieira – DNOCS-CGE/MD

RIBAMAR FERREIRA DE SOUSA



Ribamar Ferreira de Sousa é funcionário público lotado no DNOCS – Departamento Nacional de Obras Contra as Secas, em Fortaleza no Ceará. Onde trabalhou como desenvolvedor web para a intranet, em PHP com PostgreSQL. Já tendo participado de diversas atividades no órgão:

suporte, treinamento, administração do SGBD PostgreSQL, etc. Trabalha atualmente (04/2012) na administração dos servidores Linux.

Concluiu o curso de engenharia civil;

Concluiu o de especialização em irrigação e drenagem;

Também tendo iniciado e quase concluído o curso de especialização em Java;

Apenas iniciou (primeiro ano) o curso de psicologia na UFC.

Concluiu diversos cursos na área de desenvolvimento web através do CDTC (<http://cursos.cdtc.org.br>) e em outros (online e presenciais).

Curso de Administração de Servidores Linux na 4Linux em São Paulo.

Ministrou treinamento em desenvolvimento web na UNIFOR.

Ministrou curso de Joomla na SIGMA para os servidores das secretarias do governo do Estado do Ceará.

Ministrou curso de PostgreSQL na Evolução Informática.

Ministrou curso de Joomla na Faculdade CDL em 2010.

Ministrou curso de PHP na UFC de férias em 2011.

Instalação e Configuração de Servidor Linux no SINDIFORT.

Autor dos livros Curso de Joomla e Componentes Comerciais para Joomla, publicados pela editora Clube de Autores

(<http://clubedeautores.com.br>), além dos livros PostgreSQL Prático e Aplicativos em PHP, ambos em colaboração no Wikibooks.

Site pessoal com sub-domínios sobre servidores e sobre virtualização – <http://ribafs.org>

Fortaleza, Ceará, Brasil, 06 de abril de 2012.

Agradecimentos

Gostaria de agradecer aqui a todos que direta ou indiretamente trabalham para a criação e manutenção do Sistema Operacional Linux, do Linus Torvalds, de toda a equipe que colabora diretamente, e da grande comunidade que colabora através de livros, treinamentos, tutoriais, participação em listas, forums ou de outra forma.

Muito obrigado a todos.

Margarida e Lúcia

Também aproveito para agradecer outra generosa colaboração, das também colegas de trabalho no DNOCS, Lúcia Maria Piancó Chaves e Margarida Lídia de Abreu Vieira, que cuidaram da normalização deste livro e me ensinaram como fazer isso de hoje em diante. Embora eu não tenha cumprido a risca as recomendações das colegas mas estou muito agradecido.

Sumário

Introdução.....	8
1 - Vantagens do Linux	11
2 - Dicas para o Projeto da Instalação de Servidor Linux	13
3 - Instalação.....	17
3.1 - Instalação do Debian 6.0.4 de 64 BITS	17
3.2 - Instalação do Ubuntu Server 11.10 de 64 BIT	22
4 - Servidor de Firewall compartilhando Internet com o Zentyal (Modem ADSL).....	28
5 - Servidor de Firewall compartilhando Internet com o Zentyal (IP Fixo).....	46
6 - Projeto de Servidor de Arquivos	70
6.1 - AntiVirus no Samba.....	80
7 - Projeto de Servidor de Backup	84
8 - Projeto do Servidor de Testes	88
9 - Projeto de Instalação de Servidor SGBD	89
9.1 - Instalação do MySQL	89
9.2 - Instalação do PostgreSQL	92
10 - Projeto de Servidor Web	98
10.1 - Permissões ideais para docRoot	100
10.2 - Instalação e Configurações do Tomcat	103
11 - Scripts Úteis.....	105
12 - Apêndicas.....	107
12.1 - Documentação e Ajuda	107
12.2 - Acesso Remoto	111
12.3 - Configurações do Apache	112
12.4 - Compactar na Linha de Comando	113
12.5 - Compilar fontes	114
12.6 - Criação de Pacote .deb Simples	115
12.7 - Usando o crontab no Linux	116
12.8 - Distribuições Linux	117
12.9 - Sistemas de Arquivos	118

12.10 - Configurando o GRUB	123
12.11 - Configurando o Hardware via Terminal	125
12.12 - Usando o Modem ADSL	127
12.13 - Montando Dispositivos no Linux pela Linha de Comando	131
12.14 - Gerenciamento de Pacotes	132
12.15 - Particionamento e Formatação	134
12.16 - Permissões	136
12.17 - Gerenciamento de Processos	145
12.18 - Regras que o sysadmin não pode quebrar.....	146
12.19 - Configurações da Rede	147
12.20 - Scripts de Configuração do Debian/Ubuntu e similares	151
12.21 - Operações com serviços	161
12.22 - Gerenciamento de Usuários e Grupos	162
12.23 - Dicas sobre Servidores Windows	163
12.24 - Política de Segurança	164
12.26 – Usando Dois Links nos Servidores.....	169
12.27 - Alguns Comandos Linux.....	170
12.28 – Quebrando a senha do root.....	176
12.29 – Dicas para o Desktop.....	177
12.29 – Infraestrutura de Redes	180
12.30 – Material extra por download.....	182

Introdução

Procurarei mostrar de forma bem prática e ágil a administração de servidores Linux.

Geralmente serão mostrados os passos de forma simplificada, deixando de lado a parte teórica. Para acesso à parte teórica precisará recorrer a outros documentos, como os Howtos citados e outros livros.

Um recurso importante do Linux que ajuda o administrador, reduzindo as tarefas repetitivas e tornando mais eficiente a administração são os scripts shell. Podemos com eles reduzir muito o tempo de administração dos servidores.

Apresentaremos alguns exemplos.

Datacenter

É um ambiente construído exclusivamente para hospedar servidores.

Servidores de hospedagem, que abrigam sites e outros servidores são hospedados em grandes datacenters.

Servidor

É uma máquina que fica ligada o tempo todo oferecendo um ou vários serviços aos clientes de uma rede.

Serviço

É uma aplicação como o MySQL ou Apache, que fica escutando pedidos de clientes de uma rede.

Qualquer distribuição Linux pode ser usada como servidor. A sua escolha da distribuição a ser usada no servidor da empresa deve levar em conta

- suas características;
- conhecimento da distribuição pela equipe de administradores
- ferramentas da distribuição que atendem às necessidades da empresa
- tamanho da comunidade e facilidade de encontrar documentação/ajuda
- estabilidade e robustez
- facilidade de instalação de pacotes e de atualização da distribuição
- recursos e facilidades de administração

Alerta

Gostaria de deixar a minha avaliação pessoal sobre a administração de servidores Linux. A meu ver é uma atividade que requer uma boa dose de jeito para a coisa (para não dizer vocação) muito empenho e força de vontade. Isso por não ser uma atividade simples, trivial. Seguir os roteiros deste livro ou de outro não é algo complicado, mas quando o roteiro por algum motivo não funcionar e você não conseguir nem formular o problema corretamente para pedir ajuda na internet, aí sim é que precisará de algumas características importantes em você. Primeiro não pode se desesperar, depois ajuda muito se tiver um caso semelhante, um outro servidor que possa ver os scripts de configuração. Caso não tenha precisará rastrear o problema, como se fosse um grande detetive, que investiga criteriosamente, eliminando organizadamente, uma-a-uma as pistas até que, se não desistir antes, descubra o vilão. Por conta disso é muito importante sempre guardar um backup dos scripts de servidores que estão funcionando corretamente. Administrar servidores requer um perfil de pessoa, que a meu ver, é alguém intelectualmente e psicologicamente superior ao normal.

1 - Vantagens do Linux

Inicialmente o primeiro fator que deve ser considerado ao se escolher entre Windows e Linux para um servidor é a experiência do(s) administradores com os sistemas. Caso tenham maior experiência em um deles deve ser ele que devem escolher.

Caso tenham boa experiência em ambos, então realmente devem pesar as características dos dois sistemas para decidir qual usar. Geralmente o Linux ganha em desempenho, segurança e robustez.

O Linux é um sistema operacional estável, robusto, acessível, flexível e seguro.

Estável – suporta serviços pesados sem falha e pode permanecer em funcionamento por meses ou anos sem precisar reiniciar uma só vez. Podemos, se necessário, encerrar processos sem afetar os demais.

Acessível – podemos instalar o linux em quantos computador quisermos sem pagar por licença.

Flexível – como tem código-fonte aberto torna-se bem mais flexível que os sistemas comerciais.

Seguro – o Linux foi concebido pensando em segurança e é mais resistência à várias ameaças que afetam o Windows, por exemplo.

Inclusive na fase atual o Linux também já é uma opção viável para uso em desktops. Temos aí a distribuição Ubuntu e outras que podem perfeitamente substituir os sistemas comerciais.

Alguns servidores livres já há alguns anos que são mais usados que os comerciais, como é o caso do Apache. Se você for escolher um servidor de hospedagem que precise de PHP, como para usar o CMS Joomla, o Wordpress, o Drupal, o MediaWiki ou outro, neste caso é indicado um servidor Linux, que tenha o Apache e que tenha habilitado o mod_rewrite.

Atualmente grandes corporações usam Linux em seus servidores.

Dois bons artigos:

Servidores Linux – A Escolha Certa Para Seu Web Site

<http://www.artigonal.com/advertising-artigos/conheca-todas-as-vantagens-dos-servidores-linux-1835419.html>

Servidores Windows X Servidores Linux

<http://www.artigonal.com/hospedagem-artigos/saiba-escolher-entre-servidores-windows-e-servidores-linux-1677330.html>

2 - Dicas para o Projeto da Instalação de Servidor Linux

Algumas recomendações

Planejar as características do hardware de acordo com as necessidade para este servidor:

CPU (clock, núcleos, suporte a virtualização, etc)

RAM

HDs, velocidade e Controladora RAID

Placas de Rede, quantidade e marcas

Switchs

Cabos

Instrumentos para criação de conectores, testes de cabos, crimpagem, etc

Muito Importante: ter certeza da compatibilidade de todo o hardware com o Linux a ser usado

Planejar e ter anotadas as Configurações da Rede:

Hostname

IP

Máscara

Rede

Broadcast

GateWay

DNS

Outros detalhes:

- Detalhamento das partições: tipo, tamanho, quantas, etc
- Uso de no mínimo duas placas de rede no servidor de firewall: uma para a WAN (eth0) e outra para a LAN (eth1). Para os demais também usar duas se for adotar dois links.
- Definição da faixa de IPs para a LAN: 192.168.0.0 (192.168.0.100 - server)
- Configuração da rede no novo servidor: eth0 dhcp (se modem) e eth1 static
- Configuração do Modem ADSL
- Instalação do Sistema Operacional Linux (Debian ou Ubuntu Server LTS para 64 BIT)
- Copiar script de firewall com compartilhamento de internet e redirecionamento do Squid
- Instalar e configurar o servidor de SSH
- Corrigir problema do IPV6 no Firefox:
 - about:config e digitar ipv6. Mudar para false
- Instalação do dyndns (ddclient) para o caso de acesso remoto via SSH, quando não tiver IP fixo
- Configurações diversas no Servidor para otimizar seu uso e desempenho
 - /etc/network/interfaces
 - eth1 para rede local com IP estático 192.68.0.100
 - eth0 para modem com IP dinâmico
 - /etc/squid3/squid.conf
 - /etc/dhcp3/dhcpd.conf
 - /etc/resolv.conf
 - /etc/hosts
- Testes básicos:
 - ping ou arping e ssh
- Servidor de Proxy (Squid) com controle de banda e antivírus no download

-Servidor de impressão e de arquivos com Samba, clamav e amavis

-Definir serviços a serem configurados e remover não necessários e seus pacotes

Obs.: Caso existam dois links que possam ser usados, devemos ter sempre duas placas de rede para usar os dois links em cada servidor.

Instalar sob um firewall ou desconectado da internet, por conta da segurança

Seleção da Distribuição Linux

- Uma estável e com recursos que atendem às necessidades
- Com bons recursos de atualização
- Que a equipe de administradores tenha bom conhecimento sobre a mesma
- Instalar sempre a última versão estável, em sendo Ubuntu Server usar uma LTS

Efetue o download sempre do site oficial e de preferência cheque a autenticidade

Documentar todos os procedimentos de instalação e configuração dos serviços e de preferência criar scripts shell que os automatize e torne mais fácil a administração.

Serviços

Planejar serviços e pacotes a serem instalados no servidor

Instalação

Instalar rigorosamente o sistema mínimo

Após a instalação, então instalar os pacotes dos serviços que farão parte do servidor.

Criar Diagramas/desenhos com o projeto completo de hardware e software e manter anotações para servirem de guia para a instalação e configurações e de documentação. E/ou então listar os passos a serem seguidos e sair ticando cada etapa concluída.

3 - Instalação

Infra-estrutura

Antes da instalação propriamente dita do sistema operacional, devemos ter pronta toda a estrutura de rede: servidores, placas de rede, switch, roteador com o Link, cabos, etc.

Os servidores aqui abordados usarão as distribuições Debian ou Ubuntu Server.

LTS

No caso do Ubuntu é recomendável sempre usar as versões LTS em servidores, que duram 5 anos entre cada versão LTS, com suporte por todo este período.

Agora vou listar os procedimentos para a instalação do Debian e do Ubuntu Server e para os servidores a serem instalados usaremos um destes três.

Usaremos o Zentyal para o Servidor de Firewall e o Ubuntu Server ou Debian para os demais servidores.

3.1 - Instalação do Debian 6.0.4 de 64 BITS

Download - <http://debian.pop-sc.rnp.br/debian-cd/>

Baixar apenas o CD1 da última versão (32 ou 64 dependendo do hardware)

Gravar o CD com a imagem baixada

No modo Expert

(Usaremos apenas o DVD1 (para uma instalação mais enxuta usar o CD Netinstall))

Instalar em todos os servidores: mc, htop, ncd, ssh, gpm
(exceto nos virtualizados)

Dar boot pelo DVD

Advanced Options

Expert install

Choose language

Portuguese (Brazil)

Brasil

Brasil - pt_BR.UTF-8

Continuar

Selecione um layout de teclado

Teclado Estilo PC

Português Brasileiro (layout ABNT2) ou Selecionar o seu se diferente

Dica

Configurar Teclado após a Instalação

`dpkg-reconfigure console-setup`

Detectar e montar o CD-ROM

Módulos - desmarcar apenas se tiver certeza, caso contrário

Continuar

Carregar componentes do instalador a partir do CD-ROM
Não selecionar e Continuar

Detectar hardware de rede

Inserir o Pendrive com os drivers (no caso dos Dell Power Edge R710, onde o Debian não traz os drivers das placas de rede)

Configurar a rede

Apenas tecle enter para detectar DHCP ou escolha Não para entrar com os dados para Static

eth0

IP - 10.40.100.101

M - 255.0.0.0

GW - 10.0.0.2

DNS - 10.0.0.2

Noma da máquina (hostname) - dnocs101

Domínio - dnocs.gov.br

Configurar usuário e senha

Habilitar sombra de senha (shadow) - Sim

Permitir login como root - Não, para maior segurança

Nome completo para o novo usuário

Login

Senha

Configurar o relógio

Ajustar o relógio usando NTP - Sim

a.ntp.br b.ntp.br c.ntp.br

Fuso horário - Fortaleza

Detectar discos

Particionar discos

Manual, caso queira definir cada partição

Partições todas com EXT4

(ver sugestão no referido servidor, pois cada tipo de servidor requer esquema de partições diferentes)

Instalar o sistema básico

Kernel a ser instalado (apenas enter ou selecione)

linux_image_2.6.32-5-686

Drivers a serem incluídos

Genérico é para montados

Direcionano (para micros de marca)

Configurar o gerenciador de pacotes

Outro DVD? - Não

Espelho de Rede? - Sim, se estiver conectado e configurado

http

Brasil

debian.pop-sc.rnp.br

Usar programas não livres? Sim (ou o que achar mais adequado)

Serviços a serem usados - manter e Continuar

Selecionar e instalar software

Participar do concurso - Não

Man - Não

Seleção de software

Ambiente gráfico (caso queira instalar)

Marcar somente SSH (após instalar faremos a instalação dos pacotes deste servidor)

Continuar e aguardar a instalação

Instalar o Grub em um disco rígido

Instalar o carregador ... - Sim

Finalizar a Instalação.

O relógio do sistema está configurado para UTC? - Sim

Instalação Completa - Continuar

Instalar modo gráfico do Debian após a instalação

```
apt-get update
```

```
apt-get install xserver-xorg gdm gnome-desktop-environment
```

3.2 - Instalação do Ubuntu Server 11.10 de 64 BIT

Download

<http://mirror.pop-sc.rnp.br/mirror/ubuntu/>

Baixar o último LTS (32 ou 64 de acordo com o hardware)

Gravar o CD/DVD com a imagem baixada

Instalação

Efetuar o boot com o CD no drive

Selecione o Idioma

Continue the installation in selected language? - Yes

Pais de origem para o teclado?

English (US)

Layouto do teclado

English (US) - International (...AltGr...)

Dica:

Configurar Teclado após a Instalação

`dpkg-reconfigure console-setup`

Configurar a rede

Nome de máquina:

`dnocs102`

Caso vá usar IP estático:

IP - 10.40.0.110

Máscara - 255.255.255.0

Gateway - 10.40.0.1

DNS - 10.40.0.1

Configurar o Relógio - Sim (Caso esteja errado selecione Não e corrija)

Particionar discos

Vamos selecionar Manual para ver como criar as partições

Selecionar o disco onde criaremos as partições e Enter

Criar uma nova partição vazia neste dispositivo? - Sim

Selecionar ESPAÇO LIVRE E Enter

Criar uma nova partição

Novo tamanho da partição - apague tudo e digite "3gb" e Enter

Primária

Início

Usar como: ... ext4

Ponto de montagem: /

...

...

...

...

Flag inicializável: ligado

Finalizar a configuração da Partição

Selecione ESPAÇO LIVRE novamente e tecle Enter
Criar uma nova partição
Novo tamanho da partição - apague tudo e digite "1gb" e Enter
Lógica
Início

Usar como:
Área de troca (swap)
Finalizar a configuração da Partição

Selecione ESPAÇO LIVRE novamente e tecle Enter
Assim crie todas as partições desejadas e com os respectivos tamanhos e tipos.

Veja no respectivo servidor que partições e tamanhos.

Escrever as mudanças no disco? - Sim

Aguardar formatação e instalação

Nome completo para o novo usuário

Nome de usuário para sua conta

Entre com a senha para o novo usuário

Repita

Encriptar sua pasta pessoal? - Não (sim, se preferir)

Proxy

Enter e aguarde

Atualização

Sem atualizações automáticas (recomendado)

Seleção de Software

Selecione OpenSSH Server e Continuar

Caso ache que instalar algum dos grupos de pacotes pode facilitar para você, que o faça.

Um dos que gosto e me ajuda é quando vou instalar o Tomcat (instalando aqui já facilita muito)

Aguarde a instalação...

Configurar Grub - Sim

Instalação Completa - Continuar

Remover CD e teclar Enter

Após a instalação os ajustes

```
sudo passwd root
```

Instalar Ambiente Gráfico no Ubuntu Server

```
apt-get update
```

```
apt-get install ubuntu-desktop
```

```
apt-get upgrade
```

```
reboot
```

```
su
```

```
nano /etc/apt/sources.list
```

Descomentar partners

```
apt-get update
aptitude safe-upgrade
```

Instalar:

```
apt-get install openssh-server gpm mc htop
```

Configurar a rede com IP estático

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

```
# The loopback network interface
auto lo
iface lo inet loopback
# Interface primária em servidor de firewall
auto eth0
iface eth0 inet static
    address 10.40.0.110
    netmask 255.255.255.0
    network 10.40.0.0
    broadcast 10.40.0.255
    gateway 10.40.0.1
    dns-nameservers 10.40.0.1
```

```
/etc/init.d/networking restart
```

```
nano /etc/hosts
```

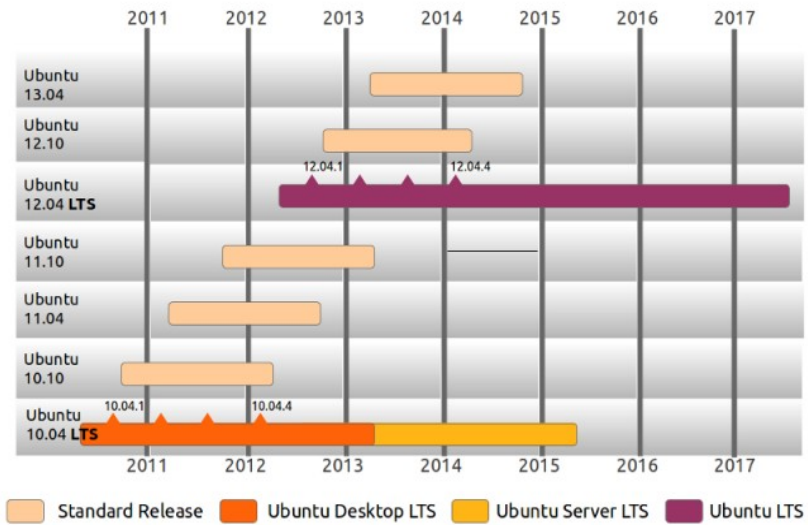
```
127.0.0.1 localhost.localdomain localhost
10.40.0.110 dnocs02.dnocs.gov.br dnocs02
```

```
echo dnocs02.dnocs.gov.br > /etc/hostname  
/etc/init.d/hostname restart
```

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

```
hostname  
hostname -f
```

Versões LTS do Ubuntu



4 - Servidor de Firewall compartilhando Internet com o Zentyal (Modem ADSL)

Ambiente

Usaremos a distribuição Zentyal, que é vontade para gateway de firewall entre outras funções.

Tomaremos a versão 2.2.1, que pode ser baixada do site, em versões de 32 e 64 bit:

<http://www.zentyal.org/downloads/>

Hardware exigido para algumas funções:

Zentyal task	Users	CPU	Memory	Disk	NI
Gateway	<100	P4 equivalent	2G	80G	2+
	100+	Xeon Dual core equivalent	4G	160G	2+
UTM	<100	P4 equivalent	2G	80G	1
	100+	Xeon Dual core equivalent	4G	160G	1
Infrastructure	<100	P4 equivalent	1G	80G	1
	100+	P4 equivalent	2G	160G	1
Office	<100	P4 equivalent	1G	250G	1
	100+	Xeon Dual core equivalent	2G	500G	1
Communications	<100	Xeon Dual core equivalent	4G	250G	1
	100+	Xeon Quad core equivalent	8G	500G	1

O servidor será ligado ao modem ADSL através de uma placa de rede

eth0 – dhcp

e de um swtch para servir a rede interna
eth1 – 192.168.0.1 – 255.255.255.0

Configuração do Modem

Configurando o modem como bridge precisaremos configurar a eth0 do Zentyal como PPPoE, com os dados para autenticação:

VELOX

login – prefixotelefoneusado@telemar.com.br

senha - prefixotelefoneusado (exemplo: 8532234592)

GVT

login - turbonet@turbonet

senha – gvt25

Firewall

Software que fica entre os computadores da rede interna e o modem/roteador da Internet, com a finalidade de proteger os computadores da LAN de ataques vindos da Internet.

Compartilhamento de Internet

Como os computadores da rede interna não têm um IP válido que os possibilite acessar diretamente a internet, então o firewall desempenha também a função de compartilhar a internet com os micros da LAN.

Instalação do Linux Zentyal 2.2.2 - 64

Download - <http://www.zentyal.org/downloads/>

Gravar o CD com a imagem baixada

Ambiente:

- servidor com Linux Zentyal instalado
- modem ADSL
- switch (para a rede interna)
- eth0 - dhcp (ligada ao modem)
- eth1 - static (192.168.0.1, 255.255.255.0) ligada ao switch, que será ligado à LAN

Efetuar boot pelo CD

Languages (selecione)

Instalar

- delete all disk (apagará todas as partições do disk principal)
- expert mode (poderá customizar o particionamento)

Teclado (selecionar). Caso seu teclado não seja identificado pode selecionar

- Generic 105 teclas
- E tentar a autodeteção

Ou então selecionar Do not configure keyboard ...(e usar o do kernel)

Origem

Layout

Configurar Teclado após a Instalação
dpkg-reconfigure console-setup

Detectando Hardware
Lendo CD-ROM
Carregando componentes adicionais

Configurando a rede
(Caso o DHCP esteja habilitado será detectado e configurada a rede da eth0)
Caso queira usar IP estático escolha Manual e entre com os dados

Instalando o sistema básico

Cadastre um usuário para administrar o sistema

Configurando o apt

Selecionar e instalar software
Instalando o GRUB - Sim
Finalizará e reiniciará o computador

Configuração do ddclient

```
nano /etc/default/ddclient  
run_daemon true
```

Configuração da interface web dos modems

Modem Huawei – SmartAX MT880a (GVT)

```
192.168.1.1  
login – admin  
senha – gvt12345
```

Roteador LinkSys WRT54G2 – Ligado após o modem acima, que está como bridge

```
login – admin  
senha – admin
```

Serviços a serem configurados

- rede
- firewall
- DHCP
- squid (proxy)

O Zentyal vem com uma bem maior quantidade de módulos/serviços, mas na primeira etapa usaremos apenas estes.

Lembrando que já traz configurados:

Apache 2
PHP 5.3.2
PostgreSQL 8.4 e muito mais.

Também precisaremos instalar e configurar (por default o Zentyal traz somente o PostgreSQL):

MySQL cliente e servidor
php5-mysql
phpmyadmin

```
apt-get install mysql-server mysql-client php5-mysql  
phpmyadmin
```

Instalerei o xvidcap para gravar um vídeo da instalação atual.

Após a instalação, após o primeiro boot iremos efetuar as configurações básicas.

A tela de login da administração web é aberta automaticamente.

Efetuar login.

Grupos de Pacotes/Módulos

Selecionar os dois Grupos de pacotes abaixo para instalar:

Gateway
Infraestrutura

Então clique em Instalar e OK

Configurando Interfaces de Rede

eth0 – external

eth1 – internal

Próximo

eth0 – dhcp

eth1 – static (192.168.1.1 e 255.255.255.0)

Próximo

Tipo de Servidor

SeleServidor Standalone

Próximo

Zend Cloud Subscription

Salvar configurações

[Click here to return to the Dashboard](#)

Estado dos Módulos

Habilitar o Módulo DHCP e Salvar

Observação – Apenas mostrarei algumas configurações onde requer intervenção, tendo em vista que as demais o Zentyal já fez por nós.

Configuração da Rede

A configuração da rede já foi feita na etapa anterior, mas vou mostrar aqui apenas caso queira alterar.

Core

Rede

Interfaces

eth0

Interfaces de Rede [\(mostrar ajuda\)](#)

eth0 eth1

Nome:

Método:

Externa (WAN):

Verifique se você está usando o Zentyal como um gateway e esta interface está conectada ao seu roteador de Internet.

Os métodos disponíveis são:

Estático

DHCP

PPPoE

Trunk

Bridge

Não definido

Estático

IP – 201.30.148.254

Máscara – 255.255.255.248

PPPoE

Usuário - turbonet@turbonet

Senha – gvt25

eth1

Interfaces de Rede [\(mostrar ajuda\)](#)

eth0 eth1

Nome:

Método: ↕

Externa (WAN):
Verifique se você está usando Internet.

Endereço IP:

Máscara de rede: ↕

Que servirá à LAN (rede interna)

Gateway e DNS já foram feitos pelo Zentyal.

Core - Rede

Objetos

Clique em Adicionar Novo e preencha de forma semelhante a este:

Objetos ▶ **bloqueados** [\(mostrar ajuda\)](#)

Editando membro

Nome:

Endereço IP: /

Endereço MAC:
Opcional

Que será usado por outros serviços, como o Proxy, por exemplo.

Configuração do DHCP

Infraestrutura

DHCP

Service Configuration

DHCP [\(mostrar ajuda\)](#)

Service configuration

Choose a static interface to configure:



<u>Opcões comuns</u>	<u>Opcões para DNS Dinâmico</u>	<u>Opcões avançadas</u>
Gateway padrão:	<input type="text" value="Zentyal"/>	
	Configurando "Zentyal" como gateway padrão gateway	
Procurar domínio:	<input type="text" value="Nenhum"/>	
	O domínio selecionado completará os cliente qualificadas (FQDN)	
Servidor de nomes primário:	<input type="text" value="DNS local Zentyal"/>	
	Se "Zentyal DNS" está presente e selecionad DNS	
Servidor de nomes secundário:	<input type="text"/>	
	<i>Opcional</i>	
Servidor NTP:	<input type="text" value="Nenhum"/>	
	Se "Zentyal NTP" está presente e selecionad clientes DHCP	
Servidor WINS:	<input type="text" value="Nenhum"/>	
	Se "Zentyal Samba" está presente e selecion para os clientes DHCP	
	<input type="button" value="Alterar"/>	

Aceite as configurações default e clique abaixo em Alterar

Adicionar Faixa de Ips

Faixas

[+ Adicionar novo](#)

Nome	De	Para	Ação
rede	192.168.0.2	192.168.0.10	 

Clique em Adicionar novo e entre com a faixa de IPs

Adicionando uma nova faixa

Nome:

De:

Para:

Clique em Adicionar – Depois clique acima em Salvar alterações acima.

Após estas configurações as estações já estão na rede interna e até já podem acessar internet.

Configuração do Proxy com Squid

Gateway

Proxy HTTP

Geral

Proxy HTTP [\(mostrar ajuda\)](#)



Get Ad blocking updates to keep your HTTP proxy aware of the latest ad Ad-blocking updates are integrated in the [Advanced Security Updates](#) a Detection System and Content Filtering System installed on your Zentyal provided by the most trusted IT experts.

Configurações Gerais

Proxy transparente:

Note que você não pode fazer proxy de firewall para habilitar este modo.

Bloqueio de anúncios:

Remover anúncios de todo o tráfego

Porta:

Tamanho dos arquivos de Cache (MB):

Política padrão:

Filtrar significa que as requisições H ser rejeitadas caso o conteúdo não :

Preencha assim.

Clicar em Alterar e Salvar Alterações acima


HTTPS – lembrando que se preferir proxy transparente não poderá bloquear os sites com HTTPS.

Gateway

Proxy HTTP

Perfis de Filtro

Entrada do filtro de conteúdo

Limite: 

Isso especifica o rigor do filtro de conteúdo.

Marque Média e clique em Alterar

Vamos Adicionar uma Regra para Bloquear Domínios

Regras de Domínios e URL

 [Adicionar novo](#)

Clique em Adicionar novo e preencha assim:

Adicionando uma nova domínio da internet ou URL

Domínio ou URL:

Política: ↕

Clicar em Adicionar e em Salvar alterações para testar o novo bloqueio.

Para ter o proxy bloqueando corretamente

Filtrar o fluxo da Rede Interna para o Zentyal

UTM

Firewall

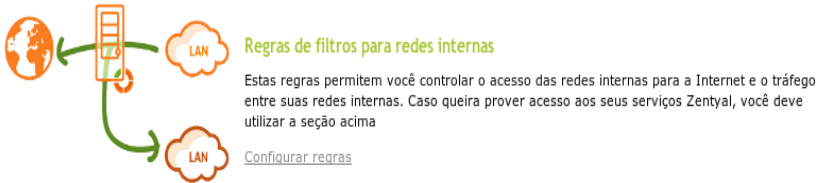
Filtro de Pacotes

Filtro para Redes Internas

UTM

Firewall

Filtro de Pacotes



Clique em Configurar regras em Regras de filtros para redes internas

Então edite a segunda regra a do Serviço qualquer para negar como no exemplo abaixo:

Configure Rules

[+ Adicionar novo](#)

<input type="text"/> <input type="button" value="Pesquisar"/>					
Decisão	Origem	Destino	Serviço	Descrição	Ação
↑	Qualquer	Qualquer	POP3	--	
×	Qualquer	Qualquer	qualquer	--	

10 Página 1

Agora vamos Redirecionar todo tráfego da porta 80 para a 3128:

Firewall – Redirecionamento de Porta
Adicionar novo

Redirecionamentos de porta

Adicionando uma nova encaminhamento

Interface:

Destino original:

Protocolo:

Porta de destino original:

Origem:

IP de destino:

Porta:

Substituir o endereço de origem:

Substitui o endereço de origem da conexão quando o destino não tem uma rota de retorno

Log:

Log novas conexões enviado

Descrição:

Opcional

Clique em Adicionar e Salvar alterações acima.
Agora somente as estações que tiverem seus navegadores configurados com o proxy poderão acessar a internet:

Proxy – 192.168.1.1

Porta – 3128

Redirecionar de forma semelhante também a porta 443 para a 3128.

Redirecionar de forma semelhante também a porta 21 para a 3128 (para o apt-get) e para outras que necessite abrir.

Listas Negras

Também podemos bloquear listas inteiras de sites proibidos. Para isso precisamos de arquivos compactados com as listas e adicionar em

Arquivos de Lista de Domínios

5 - Servidor de Firewall compartilhando Internet com o Zentyal (IP Fixo)

Servidor Dell Power Edge R710

Com 32GB de RAM, 5 discos de 450GB originalmente numa placa com RAID5.

6 placas de rede

Configurar a placa com RAID6

Instalar desconectado da Internet

eth0 para o roteador e eth1 para o switch – LAN

eth0

201.30.148.22

255.255.255.192

Network – 201.30.148.0

Broadcast – 201.30.148.63

Gateway – 201.30.148..1

DNS

200.255.255.66

200.255.255.70

dns-search dnocs.gov.br

eth1

10.0.0.2

255.0.0.0

Network 10.0.0.0

Broadcast 255.255.255.0

Serviços/Portas
/etc/services

Firewall

Deixar rede interna permitir
Desnecessário redirecionar portas

Teclado – Dell – Brasil - Brasil

DNS

webmail.dnocs.gov.br – 10.40.100.7
njord.dnocs.gov.br – 10.40.100.7
www.dnocs.gov.br – 10.40.100.11
apoena.dnocs.gov.br – 10.40.100.11
frigg.dnocs.gov.br – 10.40.100.10
freyja.dnocs.gov.br – 10.40.100.13

O Zentyal envia alertas de desligamento por e-mail

Core

Estado dos módulos

Módulo	Depende	Estado
Rede		<input checked="" type="checkbox"/>
Firewall	Rede	<input checked="" type="checkbox"/>
Antivirus		<input checked="" type="checkbox"/>
DHCP	Rede	<input checked="" type="checkbox"/>
DNS		<input checked="" type="checkbox"/>
Backup		<input checked="" type="checkbox"/>
Eventos		<input checked="" type="checkbox"/>
IDS	Rede	<input checked="" type="checkbox"/>
Logs		<input checked="" type="checkbox"/>
Filtro de Email	Rede, Antivirus, Firewall	<input checked="" type="checkbox"/>
Monitoração		<input checked="" type="checkbox"/>
NTP		<input checked="" type="checkbox"/>
VPN	Rede	<input checked="" type="checkbox"/>
Controle de Banda	Rede, Firewall	<input checked="" type="checkbox"/>
Usuários e Grupos		<input checked="" type="checkbox"/>
Servidor Web		<input checked="" type="checkbox"/>
VoIP	Rede, Usuários e Grupos	<input checked="" type="checkbox"/>
Monitoramento de largura de banda	Rede, Logs	<input checked="" type="checkbox"/>
FTP	Usuários e Grupos	<input checked="" type="checkbox"/>
Jabber	Usuários e Grupos	<input checked="" type="checkbox"/>
Correio	Rede, Usuários e Grupos	<input checked="" type="checkbox"/>
Compartilhamento de Arquivos	Rede, Usuários e Grupos	<input checked="" type="checkbox"/>
Proxy HTTP	Firewall, Usuários e Grupos	<input checked="" type="checkbox"/>
Área do usuário	Usuários e Grupos	<input checked="" type="checkbox"/>
Webmail	Correio, Servidor Web	<input checked="" type="checkbox"/>
Compartilhamento de impressora	Compartilhamento de Arquivos	<input checked="" type="checkbox"/>

Sistema



- Core
 - Dashboard
 - Estado dos módulos
 - Sistema
 - Geral
 - Backup
 - Importar/Exportar Configuração
 - Desligar/Reiniciar
 - Rede
 - Manutenção
 - Gerenciamento de software
 - Subscrição
- Gateway
 - Proxy HTTP
 - Controle de Banda
- UTM
 - Firewall
 - IDS
 - VPN
 - Antivírus
 - Filtro de Email
- Infrastructure

Configuração Geral (mostrar ajuda)

Trocar Senha

Usuário:

Senha Atual:

Nova senha:

Confirmar Senha:

Seleção de linguagem

Português do Brasil

Fuso horário

America Fortaleza

Data e Hora

NTP: **Sincronização habilitada**

Data: / /

Hora: / /

Administração da Interface da Porta TCP

Alterar Hostname

Rede

Interfaces

eth0

Interfases de Rede [\(mostrar ajuda\)](#)

eth0 eth1

Nome: eth0

Método: DHCP

Externa (WAN): Verifique se você está usando o Zentyl internet.

[Alterar](#)

eth1

Interfases de Rede [\(mostrar ajuda\)](#)

eth0 eth1

Nome: eth1

Método: Estático

Externa (WAN): Verifique se você está usando o Zentyl como um Internet.

Endereço IP: 192.168.1.1

Máscara de rede: 255.255.255.0

[Alterar](#)

Interfases virtuais

Nome	Endereço IP
<input type="text"/>	<input type="text"/>

Gateway



- Core
- Dashboard
- Estado dos módulos
- Sistema
- Rede
 - Interfaces
 - Gateways
 - DNS
 - Objetos
 - Serviços
 - Rotas estáticas
 - DNS dinâmico
 - Diagnóstico
 - Monitoramento de largura de banda
- Manutenção
- Gerenciamento de software
- Subscrição
- Gateway

Configuração de Gateways (mostrar ajuda)

Lista de Gateways

 [Adicionar novo](#)

Habilitado	Nome	Endereço IP	Interface
<input checked="" type="checkbox"/>	dhcp-gw-eth0	192.168.0.1	eth0

Proxy

Usuário:
Opcional

Senha:
Opcional

Servidor proxy:
Opcional

Porta do proxy:

DNS



- Core
- Dashboard
- Estado dos módulos
- Sistema
- Rede
 - Interfaces
 - Gateways
 - DNS
 - Objetos
 - Serviços
 - Rotas estáticas
 - DNS dinâmico
 - Diagnóstico
 - Monitoramento de largura de banda

Servidor de Resolução de Nomes de Domínio (mostrar ajuda)

Lista dos Servidores de Resolução de Nomes

 [Adicionar novo](#)

Servidor de Nomes de Domínio	
	200.165.132.155
	200.149.55.140

Domínio de Busca

Domínio:
Opcional

Rede - Objetos

Objetos [\(mostrar ajuda\)](#)

Lista de objetos

[+ Adicionar novo](#)

Nome
bloqueados

Clicando no lápis em Membros

Objetos > bloqueados [\(mostrar ajuda\)](#)

Membros

[+ Adicionar novo](#)

Nome	Endereço IP
aledeval	192.168.1.2/32

Clicando no lápis em Ação

[Objetos > bloqueados](#) [\[mostrar ajuda\]](#)


Editando membro

Nome:

Endereço IP: CIDR /

Endereço MAC:
Opcional

Membros

Nome	Endereço IP	Endereço MAC	Ação
aledeval	192.168.1.2/32	--	

Rede – Serviços

Serviços [\[mostrar ajuda\]](#)

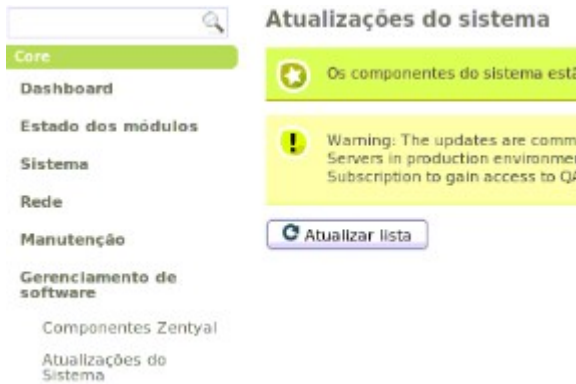
Lista de serviços

[+](#) Adicionar novo

Nome do serviço	Descrição
FTP	Zentyal FTP Server
HTTP	HTTP
Incoming Mail	Protocolos POP, IMAP e SIEVE
Mail Submission	Saída de Correio (protocolo de submissão)
POP Transparent proxy	POP transparent proxy
POP3	POP3 protocol
SMTP	Saída de Correio (protocolo SMTP).
VoIP	Zentyal VoIP system
administração do eBox	Zentyal Administration Web Server
adsync	--

Core

Gerenciamento de Software
Atualizações do sistema



Gerenciamento de Software
Configurações



Gateway

Proxy HTTP

Core

- Dashboard
- Estado dos módulos
- Sistema
- Rede
- Manutenção
- Gerenciamento de software
- Subscrição
- Gateway**
- Proxy HTTP
 - Geral
 - Estrangulamento de Largura de banda
 - Política de objetos
 - Política de grupos
 - Perfis de Filtros
- Controle de Banda

Proxy HTTP [\(mostrar ajuda\)](#)



Get Ad blocking updates to keep your HTTP proxy aware of the latest. Ad-blocking updates are integrated in the [Advanced Security Update Detection System](#) and Content Filtering System installed on your system provided by the most trusted IT experts.

Configurações Gerais

Proxy transparente:

Note que você não pode fazer de firewall para habilitar este

Bloqueio de anúncios:

Remover anúncios de todo o t

Porta:

Tamanho dos arquivos de Cache (MB):

Política padrão:

Filtrar significa que as requisicões ser rejeitadas caso o conteúdo

[Alterar](#)

Inserções de cache

[+ Adicionar novo](#)

Proxy HTTP

Política de objetos

Proxy HTTP

- Core
- Dashboard
- Estado dos módulos
- Sistema
- Rede
- Manutenção
- Gerenciamento de software
- Subscrição
- Gateway
- Proxy HTTP**
 - Geral
 - Estrangulamento de Largura de banda
 - Política de objetos
 - Política de grupos
 - Perfis de Filtros

Perfis de filtro

★

Get Content Filtering updates to keep your HTTP proxy a Filtering updates are integrated in the [Advanced Security Intrusion Detection System](#) and Content Filtering System information provided by the most trusted IT experts.

Lista de perfis

[+ Adicionar novo](#)

Pesquisar

Filtro de grupo
default

Clicar no lápis em Configuração

- Core
- Dashboard
- Estado dos módulos
- Sistema
- Rede
- Manutenção
- Gerenciamento de software
- Subscrição
- Gateway
- Proxy HTTP
- Geral
- Estrangulamento de Largura de banda
- Política de objetos
- Política de grupos
- Perfis de Filtros
- Controle de Banda
- UTM
- Firewall
- IDS
- VPN
- Antivírus
- Filtro de Email
- Infrastructure
- DHCP
- DNS
- Servidor Web
- FTP

Perfis de Filtros ▶ default (mostrar ajuda)

Filtrar vírus

Usar antivírus:

[Alterar](#)

Entrada do filtro de conteúdo

Limite:

Isso especifica o rigor do filtro de conteúdo.

[Alterar](#)

Filtragem de domínios

Filtro de tipos MIME

Filtro de extensões

Opções de filtro de domínios

Bloquear domínios e URL's não listados

Se isto estiver habilitado, qual de domínios e URL's ou em Ar

Bloquear sites especificados apenas por IP

[Alterar](#)

Regras de Domínios e URL

[+ Adicionar novo](#)

[Pesquisar](#)

Domínio ou URL	
facebook.com	
playboy.abril.com.br	

Arquivos de lista de domínios

[+ Adicionar novo](#)

Firewall

Packet Filter



Regras de filtragem das redes internas para o Zent

Estas regras permitem você controlar o acesso de redes externas executados na sua máquina do Zentyal.

[Configurar regras](#)



Regras de filtros para redes internas

Estas regras permitem você controlar o acesso das redes internas entre suas redes internas. Caso queira prover acesso aos seus usuários, utilize a seção acima

[Configurar regras](#)



Regras de filtros de redes externas para o Zent

Estas regras permitem você controlar o acesso de redes externas executados na sua máquina Zentyal.



Esteja avisado de que adicionar regras nesta seção pode comprometer sua rede e você pode garantir acesso à redes inseguras. Por favor, não saiba o que está fazendo.

[Configurar regras](#)

Regras de filtros de redes externas para rede interna

Estas regras permitem você controlar o acesso de redes externas para sua rede interna.



Esteja avisado de que adicionar regras nesta seção pode comprometer sua rede e você pode garantir acesso à redes inseguras. Por favor, não saiba o que está fazendo.

[Configurar regras](#)



Regras de filtros para o tráfego saindo do Zent

Estas regras permitem você controlar o acesso do seu Zentyal para redes externas.

[Configurar regras](#)

Redirecionamento de portas

Impressora

Communications

Correio

Jabber

VoIP

Webmail

Regras adicionais

Essas regras são ativas

! Você pode desativar alguns serviços

[Configurar regras](#)

Firewall

IDS

Interfaces

Sistema de detecção de intrusos (mostrar)

★ Get IDS updates to protect your system against the latest vulnerabilities! The IDS updates are integrated in the Antivirus, Antispam, Intrusion Detection System and Content Filter based on the information provided by the most recent updates.

Interfaces | Regras

Interface
eth0
eth1

Core

Dashboard

Estado dos módulos

Sistema

Rede

Manutenção

Gerenciamento de software

Subscrição

Gateway

Proxy HTTP

Controle de Banda

UTM

Firewall

IDS

Após Habilitar a eth0 aparece um aviso em vermelho acima para Salvar as alterações, veja:

detecção de intrusos [\(mostrar ajuda\)](#)

updates to protect your system against the latest security threats such as hacking attempts and attacks on security lities! The IDS updates are integrated in the [Advanced Security Updates](#) subscription add-on. It guarantees that the Antispam, Intrusion Detection System and Content Filtering System installed on your Zentyal server are updated on daily ed on the information provided by the most trusted IT experts.

[Regras](#)

[Pesquisar](#)

Interface	Habilitado	Ação
eth0	<input type="checkbox"/>	
eth1	<input type="checkbox"/>	

10

Clicar em Salvar alterações acima e à direita então aparece:

Salvar a configuração



Existem configurações não salvas em um ou mais módulos, você pode salvar ou descartar essas mudanças.

Se você fez mudanças nas interfaces de rede ou na porta de administração, você precisa reescrever manualmente a url para acessar essa interface de administração novamente.

[Salvar](#)

[Descartar alterações](#)

Clicar em Salvar e aguarde

IDS

Regras

Sistema de detecção de intrusos [\(mostrar ajuda\)](#)



Get IDS updates to protect your system against the latest security threats such as hacking attempt vulnerabilities! The IDS updates are integrated in the [Advanced Security Updates](#) subscription add-on. Antivirus, Antispam, Intrusion Detection System and Content Filtering System installed on your Zentao basis based on the information provided by the most trusted IT experts.

[Interfaces](#)[Regras](#)

Rule Set	Habilitado
community-virus	<input checked="" type="checkbox"/>
imap	<input checked="" type="checkbox"/>
info	<input type="checkbox"/>
attack-responses	<input checked="" type="checkbox"/>
pop2	<input checked="" type="checkbox"/>
experimental	<input type="checkbox"/>
web-php	<input checked="" type="checkbox"/>
rservices	<input checked="" type="checkbox"/>
community-ldap	<input checked="" type="checkbox"/>
community-web-php	<input checked="" type="checkbox"/>

10

Infraestrutura
DHCP**DHCP** [\(mostrar ajuda\)](#)**Service configuration**Choose a static interface to configure:

Opções comuns

Opções para DNS Dinâmico

Opções avançadas

Gateway padrão:

Configurando "Zentyal" como gateway padrão gateway

Procurar domínio:

O domínio selecionado completará os clientes qualificadas (FQDN)

Servidor de nomes primário:

Se "Zentyal DNS" está presente e selecionado, DNS

Servidor de nomes secundário: *Opcional*Servidor NTP:

Se "Zentyal NTP" está presente e selecionado, clientes DHCP

Servidor WINS:

Se "Zentyal Samba" está presente e seleciona os clientes DHCP

Faixas DHCP

Endereço IP da interface: 192.168.1.1

Subrede: 192.168.1.0/24

Faixa disponível: 192.168.1.1 - 192.168.1.254

Faixas

[+ Adicionar novo](#)

Pesquisar

Nome	De	Para
rede	192.168.1.2	192.168.1.10

10



Somente objetos membros cujo endereço IP é uma máquina (/32), um MAC válido, o endereço IP não é usado e cujo nome é único como endereço fixo serão usados. Membros cujo nome não é um hostname válido serão tomarem um nome de domínio válido.

Endereços fixos

[+ Adicionar novo](#)

Clicando no lápis em Ação

Editando faixa

Nome:

De:

Para:

Faixas

Nome	De	Para	Ação
rede	192.168.1.2	192.168.1.10	

10

Somente objetos membros cujo endereço IP é uma máquina (/32), um MAC válido, o endereço IP não é usado pela faixa disponível e cujo nome é único como endereço fixo serão usados. Membros cujo nome não é um hostname válido serão modificados para se tomarem um nome de domínio válido.

Endereços fixos

[+ Adicionar novo](#)

Infraestrutura DNS

DNS (mostrar ajuda)

Configurações

Ativar cache de DNS transparente:

Encaminhadores

[+ Adicionar novo](#)

Domínios

[+ Adicionar novo](#)

Marcar Ativar cache de DNS transparente e Alterar – Salvar alterações e Salvar

Infraestrutura Servidor Web

Servidor Web (mostrar ajuda)

Opções de configuração geral

Porta em escuta:

Porta SSL em escuta:

Habilitar por usuário public_html:

Permitir usuários para publicar documentos web usando o public_html em seu diretório home.

Hosts virtuais

[+ Adicionar novo](#)

Infraestrutura FTP

Servidor FTP (mostrar ajuda)

Opções de configuração geral

Acesso anônimo:

Permite o acesso FTP anônimo para o diretório /srv/ftp.

Diretórios pessoais:

Permite o acesso FTP autenticado para o diretório home de cada usuário.

Restringe para diretórios pessoais:

Restringe acesso para o diretório home de cada usuário. Leve em consideração que esta restrição pode ser contornada em algumas condições.

Suporte SSL:

Permite suporte FTP SSL para usuários autenticados.

Office Compartilhamento de arquivos

Compartilhamento de Arquivos [\(mostrar ajuda\)](#)

[Configurações gerais](#) | **PDC** | [Compartilhamentos](#) | [Lixeira](#) | [Antivírus](#)

Habilitar PDC:

Nome do domínio:

Nome Netbios:

Descrição:

Habilitar perfis móveis:

Letra da unidade:

Grupos do Samba:

Somente usuários pertencentes a este grupo terão acesso a uma conta samba. A sincronia acontece a cada hora

Office Compartilhamento de arquivos PDC

Compartilhamento de Arquivos [\(mostrar ajuda\)](#)

[Configurações gerais](#) | **PDC** | [Compartilhamentos](#) | [Lixeira](#) | [Antivírus](#)

Comprimento mínimo de senha: caracteres

Idade máxima de senha:

Forçar histórico de senha:

Office

Compartilhamento de arquivos

Compartilhamentos

Compartilhamento de Arquivos [\(mostrar ajuda\)](#)

Configurações gerais

PDC

Compartilhamentos

Lixeira

Antivírus

Adicionando uma nova compartilhamento

Habilitado:

Nome do compartilhamento:

Caminho do compartilhamento:

Diretório no Zentyal vai criar automaticamente o compartilhamento. Diretório em /home/samba /shares

Caminho do sistema de arquivos vai permitir a você compartilhar um diretório existente com o seu sistema de arquivos.

Comentário:

Acesso para convidados:

Este compartilhamento não requer autenticação.

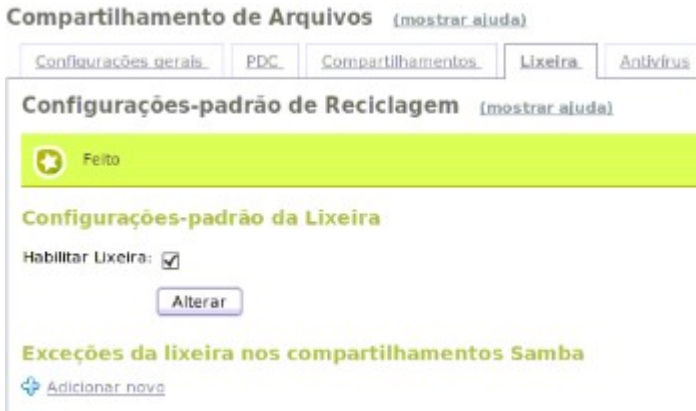
Adicionar

Cancelar

Office

Compartilhamento de arquivos

Lixeira



Office

Compartilhamento de arquivos

Antivírus



6 - Projeto de Servidor de Arquivos

Para este servidor podemos usar o **Debian** ou o **Ubuntu Server**. No caso de usar servidores que contenham hardware com drivers proprietários, como é o caso dos Dell Power Edge R710, acho indicado usar o Ubuntu Server, pois o Debian exige um driver por fora para as placas de rede.

Ambiente

Dell Power Edge R710

32GB de RAM

5 discos SCSI de 450GB cada numa placa RAID configurada por default para RAID5 e alterada para RAID6

6 placas de Rede

Partições (todas com ext4, exceto swap)

Sugestões de Particionamento para um conjunto de discos com 1.2 TB em RAID6 32GB de RAM

Caso seu disco tenha tamanho diferente faça as devidas adaptações.

/ - 100 GB - Setar Flag para ON

/home - 700 GB

/tmp - 3 GB

swap - 5 GB

/backup - com o restante

Para servidores como o de e-mail que usam muito a /var, criar uma partição /var com 500 GB.

Ao final melhorar a segurança da /tmp no /etc/fstab

Instalar

```
apt-get install samba samba-common-bin
```

nmbd é carregado e fica residente.

Quando um compartilhamento é acessado o smbd é carregado e lê o smb.conf a cada acesso do cliente a um compartilhamento.

Reiniciar o serviço nmbd

```
killall -HUP nmbd
```

Criar Compartilhamento no Samba

Alternativas: pela linha de comando (terminal), modo gráfico (system-config-samba) e via Web com webmin

Criar Compartilhamento Pela Linha de Comando

Abrir o terminal

- Criar usuário no Linux
adduser --disabled-login --no-create-home teste
- Atribuir senha no samba
smbpasswd -a teste
- Criar diretório do compartilhamento
mkdir /home/teste
- Mudar permissões e dono
chmod -R 775 /home/teste
chown -R teste:teste /home/teste
- Criar o compartilhamento
nano /etc/samba/smb.conf

[TESTE]

comment = Teste de Compartilhamento

path = /home/teste

valid users = teste

admin users = root

force group = teste

read only = No

create mask = 0771

directory mask = 0771

force create mask = 0771

force directory mask = 0771

hosts allow = 10.40.4.109,10.40.4.108,10.40.4.107

- Restartar Samba
/etc/init.d/smbd restart

Administração Gráfica

Instalando

- apt-get install python-glade2
- apt-get install system-config-samba

Criando o Compartilhamento

- Criar usuário do sistema operacional no servidor
- Criar grupo do sistema operacional com os usuários desejados
- Criar usuário no samba (deve ser um dos usuários do sistema operacional)
- Criar o compartilhamento adicionando os usuários a ele
- Cuidas das permissões do sistema de arquivos

Criar Usuários no Sistema Operacional (SO)

Antes de criar usuários do samba precisamos criar usuários do sistema operacional (UNIX). Idealmente criar usuários sem acesso ao terminal.

- Sistema - Administração - Usuários e Grupos
- Adicionar
- Nome - Usuário1
- Nome de usuário - usuario1 e OK
- Senha (5 ou mais caracteres) - *****
- Confirmação - ***** OK

Avançado (não obrigatório, mas por segurança)

Shell - /bin/false e OK

Criar Grupos no Sistema Operacional (opcional)

-Sistema – Administração – Usuários e Grupos

-Gerenciar Grupos – Adicionar

Entre com sua senha

Nome do Grupo – digite “civil” (por exemplo)

Marque em Membros do Grupo quais usuários farão parte deste grupo

E clique em OK

Cadastrar Usuário do Sistema Operacional no Samba

- No Ubuntu 11.10 e similares clicar no Painel Inicial e digitar "sa" na caixa de Pesquisa

- Clicar em Samba

- Preferências - Usuários Samba

- Adicionar Usuário

- Nome de usuário UNIX (Selecione o usuário criado anteriormente)

- Nome de Usuário Windows - digite o nome (sugestão: pode ser o mesmo nome do usuário do SO)

- Senha do Samba (crie uma senha, que também pode ser a mesma do usuário do SO)

- Confirme Ok e Ok.

Criar um Compartilhamento

Vamos criar um compartilhamento chamado civil.

- No Ubuntu 11.10 clicar no Painel Inicial e digitar "sa" na caixa de Pesquisa
- Antes de continuar crie o diretório em /home/backup/civil
- Clique no botão com uma cruz verde
- Diretório: /home/ribafs/civil
- Nome do compartilhamento (ele já joga civil)
- Marque Permitir escrita e Visível e OK
- Ao aparecer a mensagem "Por favor permita o acesso a pelo menos um usuário" clique em OK
- Selecione o usuário e clique em OK

Ajustando as Permissões do Compartilhamento

- Acesse o terminal
- Execute os comandos abaixo:
sudo find /home/backup/civil -type d -exec chmod 2775 {} \;
sudo find /home/backup/civil -type f -exec chmod 0664 {} \;

Administração Web com webmin

Baixar de <http://webmin.net>

Clicar em Debian Package e aguardar o download

Instalar com:

Acessar o diretório do download

```
dpkg -i webmin_1.580_all.deb
```

```
apt-get -f install
```

Outras Ferramentas

- Criar script com dialog e com yad
- Aplicativo com PHP
- Swat
- Webmin

/etc/samba/smb.conf de Exemplo

```
# Samba config file created using SWAT
# from 0.0.0.0 (0.0.0.0)
# Date: 2012/03/22 18:58:00

# Global parameters
[global]
    workgroup = DNOCS
    server string = Samba Server
    netbios name = FRIGG
    update encrypted = Yes
    pam password change = Yes
    passwd program = /usr/bin/passwd %u
    passwd chat debug = Yes
    username map = /etc/samba/smbusers
    log level = 1
    log file = /var/log/samba/%m.log
    max log size = 100
    socket options = TCP_NODELAY SO_RCVBUF=8192
SO_SNDBUF=8192
    logon path =
    os level = 100
    preferred master = Yes
    domain master = Yes      #Servidor terá vantagem em
disputa local
```

```
wins proxy = Yes
wins support = Yes
ldap ssl = no
idmap uid = 16777216-33554431
idmap gid = 16777216-33554431
winbind use default domain = Yes
admin users = ribafs
guest ok = Yes
#invalid users = usuario1, usuario2, usuario3
#valid users = usuario4, usuario5
security = user # Usuários precisam ser cadastrados no
linux e no samba
```

```
# Define quais extensoes vao ser vetadas, ou seja nao
poderao ser gravadas
veto files =
/*.flv/* .mp4/* .mp3/* .wav/* .tif/* .pif/* .mpg/* .mpeg/* .jpg/* .b
mp/* .avi/* .bat/* .bin/* .com/* .exe/* .cab/* .cdr/* .dat/* .dll/* .dwg/* .l
h
z/* .mid/* .zip/* .rar/* .mov/* .msi/* .pps/* .src/* .tar/* .gz/* .torrent/
*.wmv
delete veto files = yes
# Lock
lock directory = /var/lock/samba
strict locking = no
locking = no
level2 oplocks = no
#kernel oplocks = yes
#oplocks = yes
```

```
[homes]
comment = Home Directories
browseable = No
```

[printers]

comment = All Printers
path = /var/spool/samba
printer admin = @adm
create mask = 00
security mask = 00
directory mask = 00
directory security mask = 00
printable = Yes
browseable = No

[CORREIOS]

comment = CORREIOS
path = /home/correios
valid users = correios,ribafs
admin users = root
read only = No
create mask = 0771
directory mask = 0771

[PESSOAL]

comment = Arquivos do PESSOAL
path = /home/pessoal
valid users = pessoal, ribafs
admin users = root
force group = pessoal
read only = No
create mask = 0771
directory mask = 0771
hosts allow =
10.40.0.61,10.40.4.130,10.40.0.133,10.40.4.67

[MATERIAL]

comment = Material

```
path = /home/material  
valid users = material, ribafs  
admin users = root  
force group = material  
read only = No  
create mask = 0771  
directory mask = 0771
```

[APTRIMONIO]

```
comment = Arquivos do Patrimonio  
path = /home/patrimonio  
valid users = patrimonio, ribafs  
admin users = root  
force group = patrimonio  
read only = No  
create mask = 0771  
directory mask = 0771
```

[documentacao]

```
comment = Documentacao CGE  
path = /home/documentacao  
valid users = documentacao, ribafs  
admin users = root  
force group = documentacao  
read only = No  
create mask = 0751  
guest ok = No
```

Neste caso, foi criado um usuário para cada compartilhamento. Depois adicionados ao samba. Finalmente alteradas devidamente as permissões e os donos dos arquivos e pastas.

6.1 - AntiVirus no Samba

Instalação do antivírus Clamav e Amavis para proteção dos arquivos no servidor.

Instalação

```
apt-get update
apt-get install clamav clamav-daemon clamav-docs amavis
spamassassin amavisd-new clamav-testfiles
```

Atualização do Banco de Dados

```
freshclam -v
```

No Ubuntu a atualização funciona assim, mas o Debian pode não encontrar os mais recentes, então adicione o repositório abaixo:

Adicionar:

```
deb http://ppa.launchpad.net/ubuntu-clamav/ppa/ubuntu lucid
main
```

Executar

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-
keys 5ADC2037
sudo apt-get update
sudo apt-get upgrade
```

Proxy

Caso seu computador/servidor utilize proxy, devemos adicionar as linhas abaixo no arquivo `/etc/clamav/freshclam.conf`:

```
HTTPProxyServer ip_do_servidor_proxy
HTTPProxyPort porta_do_proxy
```



```
HTTPProxyUsername usuário_do_proxy  
HTTPProxyPassword senha_do_usuario_do_proxy
```

Teste do Antivirus

```
clamscan -r /usr/share/clamav-testfiles
```

Removendo o pacote de testes (que não é mais necessário)
aptitude remove clamav-testfiles

Varrendo Partições NTFS Windows

```
mkdir /mnt/windows
```

Verificar onde se encontra o hd a ser montado.

```
dmesg | grep hd
```

Montando o hd:

```
mount -t ntfs /dev/hdc1 /mnt/windos
```

Agendar Atualização Diária do Antivirus

```
crontab -e
```

Adicione a linha abaixo (atualizar todos os dias a 1 hora da manhã):

```
0 1 * * * /usr/bin/freshclam
```

Fonte: <http://www.vivaolinux.com.br/dica/Instalacao-e-integracao-do-CLAMAV-com-o-SAMBA>

Adicionando Quotas ao Samba

A quota será adicionada por usuário, para controlar cada compartilhamento.

Os compartilhamentos usarão a partição home e os usuários terão seu login desabilitado e sem home já na criação.

Instalação

```
apt-get install quota quotatool
```

A quota será aplicada ao diretório /home.

Alterar a linha da /home no fstab, que originalmente estava assim:

```
/dev/sda3 /home ext4 defaults 0 2
```

Para:

```
/dev/sda3 /home ext4 defaults,usrquota,grpquota 0 2
```

Habilitar as cotas

```
touch /home/quota.user /home/quota.group
```

```
chmod 600 /home/quota.*
```

```
mount -o remount /home
```

```
quotaoff -avug /home
```

```
quotacheck -avugm
```

```
quotaon -avug /home
```

Desabilitando as Quotas

```
quotaoff -avug /home
```

Parâmetros das Quotas

soft limit – 180MB (valor mínimo da quota em disco)
hard limit - 200MB (valor máximo da quota em disco)
grace period - tempo que o usuário pode ficar com mais que soft limit.

Configurar grace periodo

edquota -t

Ver valores para o usuário ribafs
quota ribafs

ou apenas
quota

Relatório geral das quotas de todos os usuários
repquota /home

Para facilitar a criação dos usuários, criei este pequeno script:

```
#!/bin/bash
echo "Digite o login do usuário"
read LOGIN
echo "Digite a senha do usuário"
read SENHA
useradd --no-create-home --password $SENHA $LOGIN
smbpasswd -a $LOGIN
mkdir /home/$LOGIN
chmod -R 775 /home/$LOGIN
chown -R $LOGIN:$LOGIN /home/$LOGIN
```

7 - Projeto de Servidor de Backup

Usando rsync com backup full inicialmente e incremental para os demais diariamente no cron.

Instalar o sistema operacional (Ubuntu Server ou Debian)

Instalar os serviços:

```
apt-get update
```

```
# No Ubuntu o rsync já vem instalado por padrão
```

```
apt-get install ssh rsync
```

```
apt-get install clamav clamav-daemon clamav-docs amavis
```

```
spamassassin amavisd-new clamav-testfiles
```

Criar script com rsync em cada servidor que enviará seu backup para o servidor.

Este script ficará no crontab para backup automático usando o scp.

Criar a chave SSH em cada servidor:

Backup remoto com rsync

Entre dois computadores com IPs 10.0.0.4 (servidor de backup) e 10.40.100.13 (servidor web) que estão em uma mesma rede

O usuário do backup será o root

Os pacotes ssh e rsync devem estar instalados em ambos

Estando em 10.40.100.13 acessar o servidor de backup via ssh
ssh root@10.0.0.4
exit

cd e enter
Gerar a chave com
ssh-keygen -t rsa

Enter duas vezes
Tecle Enter duas vezes quando perguntado
Copiar a chave de backup para o servidor web

```
ssh-copy-id -i .ssh/id_rsa.pub root@10.0.0.4
```

Acessar o servidor web por ssh:
ssh root@10.40.100.13

Para testar que não pedirá senha

Efetuar logoff
exit

Obs: caso o ssh-copy não funcione como é o caso do
OpenBSD, então use o scp para copiar o arquivo
scp /root/.ssh/id_rsa.pub root@10.0.0.4:/root
ssh 10.0.0.4
cd
cat /root/id_rsa.pub >> /root/.ssh/redefined_keys

Copiar um pequeno arquivo com rsync para o servidor de
backup para testar:
rsync -tP backupfull root@10.0.0.4:/backup/

Efetuar o backup do diretório ou do arquivo final
rsync -t /directory/to/backup/* root@10.0.0.4:/backup/www/

- p - preserva permissões
- r - recursivo
- z - compacta arquivos não compactados

Adicionando ao crontab

Este script poderia ser executado uma vez por dia usando o cron, de forma que você tivesse sempre um backup do dia anterior à mão, pronto para recuperar qualquer arquivo deletado acidentalmente.

No cron para todos os dias as zero horas, exceto sábados e domingos

Execute como root:

crontab -e

Adicione a linha abaixo para executar o script backup.sh:

```
0 0 * * 1-5 /backup/backup.sh
```

=====SCRIPT=====

```
#!/bin/sh
```

```
# Script de backup incremental para o SINDIFORT
```

```
#http://www.hardware.com.br/tutoriais/backup2/
```

```
#tar --newer-mtime=`date +%Y%m%d%H%M` -cf  
/home/ribafs/guardar/backup_`date +%Y%m%d_%H  
%M`.tar /home/ribafs/backup
```

"-a" (archive) faz com que todas as permissões e atributos dos arquivos sejam mantidos,
da mesma forma que ao criar os arquivos com o tar, e o
"v" (verbose) mostra o progresso na tela.

origem - destino

```
rsync -av /home/backup/ /home2/backup/
```

Se algum desastre acontecer e você precisar recuperar os dados, basta inverter a
ordem das pastas no comando, fazendo com que a pasta com o
backup seja a origem e a pasta original seja o destino, como em:

destino - origem

```
rsync -av --delete /home2/backup/ /home/backup/
```

O "--delete" faz com que arquivos apagados na pasta original sejam apagados também na
pasta do backup, fazendo com que ela se mantenha como uma cópia
fiel. Naturalmente, a opção pode ser removida do comando se o objetivo é fazer com
que o backup mantenha arquivos antigos, de forma que você
possa recuperá-los posteriormente, caso necessário.

8 - Projeto do Servidor de Testes

Uma providência muito importante é a criação de um servidor de testes, aquele onde testamos sempre antes de colocar em produção.

Este servidor pode conter o servidor de SGBD, o servidor Web e outros que se achar necessário, como uma nova instalação do servidor de Arquivos.

9 - Projeto de Instalação de Servidor SGBD

Aqui instalaremos os SGBDs MySQL e PostgreSQL.

9.1 - Instalação do MySQL

```
apt-get update
apt-get upgrade
aptitude install mysql-server mysql-client
```

Permitir acesso de host externo (não recomendado)

```
nano /etc/mysql/my.cnf
```

```
#bind-address          = 127.0.0.1
```

Descomentado aceita somente conexão local

Checar se rede está habilitada:

```
netstat -tap | grep mysql
```

Hardening e Tuning do MySQL

Execute o seguinte comando e siga os passos recomendados:

```
/usr/bin/mysql_secure_installation
```

Resumo de comandos para Administração do MySQL

E criar um usuário para acesso remoto e plenos poderes, já que o root deve estar restrito aos acessos locais (pelo `mysql_secure_installation`)

EVITAR A CRIAÇÃO DESTE USUÁRIO

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

```
GRANT ALL PRIVILEGES ON *.* TO admin@""  
IDENTIFIED BY 'senha' WITH GRANT OPTION;
```

Criar usuário para o site em Joomla com poderes apenas no localhost

banco - portal

usuário - portal

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

```
create database portal;
```

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

Liberando apenas para 192.168.0.102 (web)

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

```
create database portal;
```

```
GRANT ALL PRIVILEGES ON portal.* TO  
portal@192.168.0.102 IDENTIFIED BY 'senha' WITH  
GRANT OPTION;
```

```
\q
```

```
/etc/init.d/mysql restart
```

Privilégios:

. - Privilégio global. Todos os bancos (*) e todas as tabelas de todos os bancos (.*)

db.* - Todas as tabelas do banco db

db.tb - Somente a tabela tb do banco db

Acesso com o uso do coringa (%):

Exemplos:

... TO remoto@"%.mysqlbrasil.com.br"

... TO remoto@"200.236.13.%"

... TO " "@%.mysqlbrasil.com.br"

/etc/init.d/mysql restart

Para administração pela linha de comando use:

mysql -h localhost -u root -p (o super usuário default é root)

mysql -u root (quando estiver sem senha)

Para Resetar a senha de root

dpkg-reconfigure mysql-server-5.1

Mostrar Usuários

show full processlist;

Mostrar bancos

show databases;

Mostrar tabelas

use banco

show tables;

Mostrar estrutura de tabela

```
use banco
describe tabela;
Mostrar privilégios
use banco
show privileges;
```

Mostrar privilégios de um usuário
SHOW GRANTS FOR teste@localhost;

Remover usuário
DELETE FROM mysql.user WHERE user="teste" AND
host="localhost";
FLUSH PRIVILEGES;
Alterar o password de determinado usuário:
set password for 'root'@'localhost'=password('novopassword');

9.2 - Instalação do PostgreSQL

```
apt-get update
apt-get upgrade
apt-get install postgresql postgresql-doc postgresql-8.4-slony1
postgresql-8.4-postgis
```

EVITAR TROCAR A SENHA, DEIXANDO O ACESSO
SOMENTE ATRAVÉS DO ROOT MESMO
passwd postgres (Alterar a senha no Sistema Operacional)

Permitir Acesso somente Local
Para permitir que aplicativos e sites criados com o PHP tenham
acesso através de uma conexão onde usam 'host=localhost', ou

seja, local, devemos executar como root.

CRIAR MAIS DOIS USUÁRIOS

Criar usuários que não podem criar usuários, bancos nem roles

```
su - postgres
createuser apoena
createuser _postgresql
```

Alterar a senha dentro do SGBD

```
psql
ALTER USER postgres WITH PASSWORD 'senha';
\q      para sair
```

```
cp /etc/postgresql/8.4/main/postgresql.conf
/etc/postgresql/8.4/main/postgresql.confCOP
nano /etc/postgresql/8.4/main/postgresql.conf
```

listen_addresses = '*' (Escutar todas os IPs. Controlar no pg_hba.conf)

Neste arquivo (pg_hba.conf) você consegue restringir o acesso ao seu banco de dados por IP, por usuário, por tipo de senha, etc.

```
cp /etc/postgresql/8.4/main/pg_hba.conf
/etc/postgresql/8.4/main/pg_hba.confCOP
```

```
nano /etc/postgresql/8.4/main/pg_hba.conf
```

Liberar o IP do servidor WEB (10.10.0.102) e do servidor de Email (10.10.0.103)

```
# Database administrative login by UNIX sockets
local all postgres ident (Usuário
postgres usa a mesma senha do SO)
```

```
# TYPE DATABASE USER CIDR-ADDRESS
METHOD
```

```
# "local" is for Unix domain socket connections only
```

```
local all all ident
```

```
# IPv4 local connections:
```

```
host all all 127.0.0.1/32 md5
```

```
host all all 10.10.0.102/32 md5
```

```
#host all all 10.10.0.103/32 md5
```

Toda uma rede:

```
host all all 10.0.0.0/24 md5
```

```
exit
```

```
/etc/init.d/postgresql restart
```

Para não atribuir senha para o postgres, usando somente através do root podemos usar:

```
su postgres -c psql postgres
```

Alguns scripts em

```
/usr/share/postgresql/8.4/
```

Uso Remoto do PostgreSQL

Acesso remoto do IP 192.168.1.67

No postgresql.conf listen_addresses deve estar com '*'

Alterar o pg_hba.conf na linha do IP para trust

```
host all all 192.168.1.67/32 md5
```

Para toda a rede:

```
host all all 192.168.1.0/24 md5
```

Restartar

```
/etc/init.d/postgresql restart
```

Acessar com:

```
psql -h IP -U usuario -d banco
```

ou

```
psql -h IP -U usuario
```

Listar bancos remotamente

```
psql -l -h 192.168.1.12 -U postgres
```

Ajuda

```
psql --help
```

Backup local e restore remoto

```
pg_dump banco | psql -h hostname banco -U postgres
```

```
pg_restore apoena -f
```

Usando o pg_hba.conf

Liberar um IP

```
host all 192.168.1.10 255.255.255.255 md5
```

Rejeitando

```
host all 192.168.1.10 255.255.255.255 reject
```

Liberar toda uma rede

```
host all all 192.168.0.0/32 md5
```

```
host booktown 192.168.1.0 255.255.255.240 trust
```

Liberar toda a Web

```
host all all 0.0.0.0/0 md5
```

Certo usuário

```
host all usuariodobanco 192.168.0.0/32 md5
```

Certo banco

```
host bancodedados usuariodobanco 192.168.0.0/32 md5
```

Dicas

Acessar um banco

```
psql banco
```


Toda operação agora fica restrita apenas ao esquema atual, que é o public

Listar tabelas do esquema public

```
\d
```

Conectar a outro banco

```
\c banco
```

Mostrar search_path atual

```
SHOW search_path;
```

Listar esquemas do banco atual

```
\dn
```

Adicionar esquema no search_path

```
SET search_path TO apoena,public;
```

Ou

```
SET search_path TO apoena;
```

Listar tabelas do esquema public e do apoena

Todas as operações agora enxergam o esquema apoena

```
\d
```

10 - Projeto de Servidor Web

Evitar os arquivos de desenvolvimento sempre que possível, para não instalar bibliotecas e compiladores. Caso instale por alguma necessidade, desinstale logo em seguida.

Após instalar o servidor, efetuar a instalação dos pacotes manualmente como a seguir:

Apache

```
apt-get update
```

```
apt-get upgrade
```

```
apt-get install -f apache2 # Instalar com dependências
```

PHP e extensões com suporte ao MySQL e ao PostgreSQL

```
apt-get install php5 libapache2-mod-php5 php5-gd php5-mysql  
php5-pgsql php5-imap php-pear php-auth php5-ming php5-  
snmp php5-xmlrpc php5-xsl php5-suhosin
```

Criar um usuário no MySQL que acesse o SGBD somente da estação do DBA e o mesmo para o PostgreSQL

Habilitar o mod_rewrite no Apache (Joomla e outros softwares)
a2enmod rewrite

Caso queira Desabilitar o módulo
a2dismod rewrite

Habilitar site
a2ensite nomesite

Se necessário remover o link do site, exemplo:

```
rm /etc/apache2/sites-enabled/nomesite
```

Comentar SetHandler

```
nano /etc/apache2/mods-enabled/php5.conf
```

```
<IfModule mod_php5.c>
  <FilesMatch "\.ph(p3?|tml)$">
    #SetHandler application/x-httpd-php
  </FilesMatch>
  <FilesMatch "\.phps$">
    #SetHandler application/x-httpd-php-source
  </FilesMatch>
  # To re-enable php in user directories comment the following
  lines
  # (from <IfModule ...> to </IfModule>.) Do NOT set it to
  On as it
  # prevents .htaccess files from disabling it.
  <IfModule mod_userdir.c>
    <Directory /home/*/public_html>
      php_admin_value engine Off
    </Directory>
  </IfModule>
</IfModule>
```

Habilitar a porta 443 (Habiiltada por default):

```
Editar /etc/apache2/ports.conf
```

```
Listen 80
```

```
Listen 443
```

Instalar Webalizer (somente no web)

```
apt-get install webalizer
```

nano /etc/webalizer/webalizer.conf

Mudar

LogFile /var/log/apache2/access.log.1

para

LogFile /var/log/apache2/access.log

Executar

webalizer

Restartar apache:

/etc/init.d/apache2 restart

Editar

nano /var/www/webalizer/index.html

Adicionar na seção

<HEADER>

<meta http-equiv="Content-Type"

content="text/html; charset=utf-8" />

10.1 - Permissões ideais para docRoot

Este recurso é muito importante, especialmente para servidores de hospedagem de sites.

Criando um grupo de administradores para o documentroot que terão plenos poderes no mesmo, além de permitir que outros do grupo também o façam sem impedimentos

addgroup webdevel

```
adduser ribafs webdevel
adduser www-data webdevel
chown -R root:webdevel /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
```

```
nano /etc/skel/.bashrc
umask u=rwx,g=rwx,o=rx
```

Agora qualquer usuário do grupo webdevel pode alterar os arquivos existentes, remover e criar novos sem que outros do grupo estejam impedidos de fazê-lo com os mesmos arquivos.

- Testar Apache com PHP

```
nano /var/www/tt.php
```

```
<?php
phpinfo();
?>
```

- Pequeno teste para ver se o PHP está com suporte ao PostgreSQL

```
nano /var/www/pg.php
```

```
<?php
$conn = pg_connect("host=localhost user=postgres
password=postgres dbname=template1");

if($conn){
    print 'PHP com suporte a PostgreSQL habilitado!';
```

```
}else{  
    print 'PHP sem suporte a PostgreSQL!';  
}  
?>
```

Obs.: Lembrar que para fazer este teste a VM sgbd deve estar ligada.

Codificação de Caracteres

A ser adicionada no início do referido arquivo

HTML

```
<meta http-equiv="Content-Type"  
content="text/html;charset=utf-8" />
```

XML ou JavaScript ou AJAX

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

ASP:

```
<% Response.Charset="ISO-8859-1" %>
```

PHP:

```
<?php header("Content-Type: text/html; charset=UTF-  
8",true) ?>
```

JSP:

```
<%@ page contentType="text/html; charset=ISO-8859-1" %>
```

10.2 - Instalação e Configurações do Tomcat

```
apt-get update  
apt-get upgrade  
apt-get install sun-java6-jdk
```

```
apt-get install tomcat6  
apt-get install tomcat6-docs tomcat6-admin tomcat6-examples  
tomcat6-user
```

```
/etc/init.d/tomcat6 restart
```

```
/etc/init.d/tomcat6 stop
```

```
nano /var/lib/tomcat6/conf/tomcat-users.xml  
<?xml version='1.0' encoding='utf-8'?>  
<tomcat-users>  
<role rolename="admin"/>  
<role rolename="manager"/>  
<role rolename="tomcat"/>  
<user username="tomcat" password="senha"  
roles="tomcat,admin,manager"/>  
</tomcat-users>
```

```
/etc/init.d/tomcat6 start
```

```
nano /etc/default/tomcat6
```

```
AUTHBIND=yes
```

Porta

```
nano /etc/tomcat6/server.xml
```

```
<Connector port="8080" protocol="HTTP/1.1"...
```

```
/etc/init.d/tomcat6 restart
```

Testar com:

```
http://localhost:8080/manager/html
```

Detalhes: <http://www.debianadmin.com/how-to-setup-apache-tomcat-55-on-debian-etch.html>

11 - Scripts Úteis

Listar os 6 maiores arquivos do diretório atual

```
du -k * | sort -nr | cut -f2 | xargs -d "\n" -x du -sh | head  
ou  
du -h | sort -nr | head -6
```

Listar os arquivos modificados há mais de 4 dias.

Procurará em /var/log e gravará a lista no arquivo /tmp/lista4dias

```
find /var/log -mtime +4 > /tmp/lista4dias
```

Script para renomear vários arquivos de uma vez.

```
#Por José Henrique  
#!/bin/sh  
for f in *.php  
do  
    #Troca o sufixo .php pelo .html  
    newname=$(basename $f php)html  
  
    #Renomeia  
    mv $f $newname  
done
```

Script com menus que executam ações usando dialog

```
#!/bin/sh
#
# Script com menus que executam ações usando dialog
# menu item
#
while :
do
    clear
    servico=$(dialog --stdout --backtitle 'DNOCS - Administração
do Firewall Interno' \
        --menu '    Selecione o Serviço e tecle Enter' 0 0 0 \
        1 'DHCP - Cadastrar Computador' \
        2 'Squid - Liberar IP' \
        3 'Squidguard - Liberar Site' \
        4 'Squidguard - Bloquear Site' \
        5 'Shorewall - Liberar ou Bloquear Porta' \
        0 'Sair' )
    case $servico in
        1) nano /root/dhcp.txt;nano
/etc/dhcp/dhcpd.conf;/etc/init.d/isc-dhcp3-server restart;;
        2) nano /etc/squid/acls/ips_liberados;squid -k reconfigure;;
        3) nano /var/lib/squidguard/db/white/domains;squidGuard
-C /var/lib/squidguard/db/white/domains;squid -k reconfigure;;
        4) nano
/var/lib/squidguard/db/blocked/domains;squidGuard -C
/var/lib/squidguard/db/blocked/domains;squid -k reconfigure;;
        5) nano /etc/shorewall/rules;/etc/init.d/shorewall restart;;
        0) clear;exit;;
    esac
done
```

12 - Apêndicas

12.1 - Documentação e Ajuda

Ubuntu Server

<https://help.ubuntu.com/10.04/index.html>

<https://help.ubuntu.com/11.10/index.html>

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

Debian

http://www.debian.org/doc/index_pt.html

<http://www.debian.org/releases/stable/amd64/>

<http://www.debian.org/doc/manuals/debian-faq/>

<http://www.debian.org/doc/manuals/debian-reference/>

<http://www.debian.org/releases/stable/amd64/release-notes/>

<http://wiki.debian.org/>

<http://www.debian.org/doc/manuals/refcard/refcard>

<http://www.debian.org/doc/user-manuals#securing>

Zentyal

<http://doc.zentyal.org/en/>

Howtos

<http://tldp.org/HOWTO/pdf/>

http://tldp.org/HOWTO/html_single/

<http://www.linuxhowtos.org/>

FocaLinux

Site - <http://www.guiafoca.org/>

Online - http://www.guiafoca.org/?page_id=14

Redes

<http://tldp.org/HOWTO/NET3-4-HOWTO.html>

<http://www.aboutdebian.com/network.htm>

Shell

<http://tldp.org/LDP/abs/html/>

<http://www.gnu.org/software/bash/manual/bashref.html>

<http://steve-parker.org/sh/bourne.shtml>

RSync

<http://linux.die.net/man/1/rsync>

<http://www.thegeekstuff.com/2010/09/rsync-command-examples/>

<http://ss64.com/bash/rsync.html>

Samba

<http://www.samba.org/samba/docs/>

<http://www.samba.org/~samba-bugs/docs/>

http://www.samba.org/samba/docs/using_samba/toc.html

<http://www.samba.org/samba/docs/man/Samba-Guide/>

http://wiki.samba.org/index.php/Main_Page

Quota

<http://tldp.org/HOWTO/Quota.html>

Clamav

<http://www.clamav.net/lang/en/doc/>

Spamassassin

<http://spamassassin.apache.org/doc.html>

Squid

<http://www.squid-cache.org/Doc/>

IPTables

<http://netfilter.org/documentation/>

Shorewall

<http://www.shorewall.net/Documentation.html>

SquidGuard

<http://www.squidguard.org/Doc/>

DansGuardian

<http://dansguardian.org/?page=documentation>

DHCP

<http://www.isc.org/software/dhcp/documentation>

DNS

<http://tldp.org/HOWTO/DNS-HOWTO.html>

<http://technet.microsoft.com/en-us/library/cc772774%28v=ws.10%29.aspx>

Postfix

<http://www.postfix.org/documentation.html>

MySQL

<http://dev.mysql.com/doc/>

PostgreSQL

<http://www.postgresql.org/docs/>

SQLite

<http://www.sqlite.org/docs.html>

Apache

<http://httpd.apache.org/docs/>

PHP

http://www.php.net/manual/pt_BR/

http://www.php.net/get/php_manual_pt_BR.chm/from/a/mirror

http://www.php.net/get/php_enhanced_pt_BR.chm/from/a/mirror

Tomcat

<http://tomcat.apache.org/>

Vídeos sobre hospedagem

<http://www.hostgator.com.br/tutoriais/>

Bons sites

<http://br-linux.org/faq-linux/>

<http://www.howtoforge.com/>

<http://www.vivaolinux.com.br/>

<http://www.vivaolinux.com.br/perguntas/>

<http://www.hardware.com.br/tutoriais/>

http://www.uniriotec.br/~morganna/guia/introd_guia.html

<http://www.ufpa.br/dicas/linux/li-libib.htm>

Bons Forums

<http://ubuntuforums.org/>

<https://lists.ubuntu.com/mailman/listinfo/ubuntu-pt>

<http://ubuntuforum-br.org/>

<http://under-linux.org/forums/>

<http://www.forumdebian.com.br/>

12.2 - Acesso Remoto

Teamviewer

Este é o software mais popular atualmente para acesso remoto.

Tem versões para Windows, Linux, MAC e Mobile:

<http://www.teamviewer.com/pt/download/index.aspx>

cliente terminal server

VNC

Acesso Remoto com SSH

É um acesso via terminal do Linux

Acessar

```
ssh ribafs@10.40.0.23 -p 622
```

Copia remota

De lá para cá:

```
scp ribafsne@74.220.207.123:/home/ribafs/joomla.tar.bz2  
backup/
```

Daqui para lá:

```
scp arquivo usuario@host:/diretorio/
```

Para acessar um servidor remoto com rdesktop:

```
rdesktop -a8 -u usuario -p senha endereço.do.servidor
```

Nota: o -a é para quantidade de cores, 8 bits, 15 bits, 16 bits, 24 bits, etc...

Para permitir acesso remoto a um servidor:

Instalar o `tightvncserver`

12.3 - Configurações do Apache

Verificar que módulos estão ativos

`apache2ctl -M`

Ativar módulo

`a2enmod nomemodulo`

Desativar módulo

`a2dismod nomemodulo`

Ativar site

`a2ensite dominiosite`

Desativar site

Remover o arquivo do site da pasta:

`/etc/apache2/sites-enabled/nomesite`

Restart

`/etc/init.d/apache2 restart`

Reload

`/etc/init.d/apache2 reload`

Habilitar site

`a2ensite gnuteca`

Se necessário remover o link do site, exemplo:
rm /etc/apache2/sites-enabled/gnuteca

Desativar site
a2disite gnuteca

12.4 - Compactar na Linha de Comando

Compactar zip recursivamente
zip -r nome.zip /home/teste

Descompactar zip
unzip nome.zip
unzip nome.zip -x joao.txt (Extrair tudo de nome.zip exceto joao.txt)

Compactar rar
sudo apt-get install rar

rar a nome.rar /home/teste

Descompactar rar
unrar x nome.rar

Compactar tar.gz
tar czpvf nome.tar.gz /home/teste

Descompactar tar.gz
tar xpvf nome.tar.gz -C /home/teste2

```
Descompactar bzip2  
bunzip2 nome.bz2
```

12.5 - Compilar fontes

Idealmente devemos instalar os pacotes que já vêm prontos dos repositórios.

Tem a vantagem de atualizar na próxima vez que houver uma versão nova.

Se compilar algo sempre precisará compilar novamente para ter a nova versão.

Passos básicos:

Geralmente para compilar um fonte:

- Descompactamos o arquivo
- Acessamos o diretório
- E executamos os 3 passos seguintes:

```
./configure  
make  
make install
```

Caso estes não sejam os passos para a compilação leia um dos arquivos com instrução, que geralmente é um readme.txt ou algo do gênero.

12.6 - Criação de Pacote .deb Simples

Criar um pacote chamado linuxadmin

Criar estrutura de arquivos abaixo:

```
/home/ribafs/linuxadmin  
/home/ribafs/linuxadmin/DEBIAN  
/home/ribafs/linuxadmin/DEBIAN/control
```

Conteúdo do arquivo control:

```
Package: linuxadmin  
Priority: Optional  
Section: system  
Version: 1.0  
Architecture: all  
Maintainer: Ribamar FS - ribafs@gmail.com  
Installed-Size: 35  
Depends: apache2, php5  
Description: Administração de servidores Linux (obrigatório)  
  Detalhes no site: http://ribafs.org
```

```
Package: linuxadmin (obrigatório)  
Priority: Optional  
Section: system (obrigatório)  
Version: 1.0 (obrigatório)  
Architecture: all  
Maintainer: Ribamar FS - ribafs@gmail.com (obrigatório)  
Installed-Size: 35 (em KB)  
Depends: (pacotes separados por vírgula)  
Description: Administração de servidores Linux (obrigatório)
```

Detalhes no site: <http://ribafs.org>

Gerar o pacote:

```
dpkg -b /root/linuxadmin linuxadmin-1.0.deb
```

Arquiteturas:

all

i386

amd64

12.7 - Usando o crontab no Linux

```
crontab -e
```

```
0 4 * * * who
```

a linha é dividida em 6 campos separados por tabs ou espaço:

Campo	Função
-------	--------

1o. Minuto

2o. Hora

3o. Dia do mês

4o. Mês

5o. Dia da semana

6o. Programa para execução

Todos estes campos, sem contar com o 6o., são especificados por números. Veja a tabela abaixo para os valores destes campos:

Campo	Valores
Minuto	0-59
Hora	0-23
Dia do mês	1-31
Mês	1-12
Dia da semana	0-6 (o "0" é domingo), 1 é segunda, etc.

Também podemos usar Mon para 1 e Fri para 6
Dom-Sat

Exemplo:

Executar o comando 'backup' todo dia 1 e 15 às 2:45

```
45 2 1,15 * * /usr/local/bin/backup
```

Executar o comando 'backup' às 2:45 somente de segunda a sexta

```
45 2 1,15 * Mon-Fri /usr/local/bin/backup
```

12.8 - Distribuições Linux

O sistema operacional Linux é entregue ao usuário por distribuições, que podem ser empresas, grupos de usuários e até por um único usuário.

Quando escolher uma distribuição deve pensar nos requisitos necessários para seu projeto e ver se a distribuição contempla os mesmos, como arquitetura, quantidade de memória, processadores, estabilidade, suporte da comunidade, suporte comercial, etc.

Existe uma grande quantidade de distribuições atualmente. As mais populares hoje são:

LinuxMint
Ubuntu
Fedora
openSuse
Debian
CentOS
PCLinuxOS
Mageia

Também temos
RedHat
SuSE
Slackware
Gentoo

12.9 - Sistemas de Arquivos

Alguns sistemas de arquivos suportados pelo Linux

vfat
ext2
ext3
ext4
reiserfs
swap

Corrigindo Discos

fdisk -l

psck.ext4 /dev/sda1

Linux File Systems: Ext2 vs Ext3 vs Ext4

by Ramesh Natarajan on May 16, 2011

ext2, ext3 and ext4 are all filesystems created for Linux. This article explains the following:

- * High level difference between these filesystems.
- * How to create these filesystems.
- * How to convert from one filesystem type to another.

Ext2

- * Ext2 stands for second extended file system.
- * It was introduced in 1993. Developed by Rémy Card.
- * This was developed to overcome the limitation of the original ext file system.
- * Ext2 does not have journaling feature.
- * On flash drives, usb drives, ext2 is recommended, as it doesn't need to do the over head of journaling.
- * Maximum individual file size can be from 16 GB to 2 TB
- * Overall ext2 file system size can be from 2 TB to 32 TB

Ext3

- * Ext3 stands for third extended file system.
- * It was introduced in 2001. Developed by Stephen Tweedie.
- * Starting from Linux Kernel 2.4.15 ext3 was available.

- * The main benefit of ext3 is that it allows journaling.
- * Journaling has a dedicated area in the file system, where all the changes are tracked. When the system crashes, the possibility of file system corruption is less because of journaling.
- * Maximum individual file size can be from 16 GB to 2 TB
- * Overall ext3 file system size can be from 2 TB to 32 TB
- * There are three types of journaling available in ext3 file system.
 - o Journal – Metadata and content are saved in the journal.
 - o Ordered – Only metadata is saved in the journal. Metadata are journaled only after writing the content to disk. This is the default.
 - o Writeback – Only metadata is saved in the journal. Metadata might be journaled either before or after the content is written to the disk.
- * You can convert a ext2 file system to ext3 file system directly (without backup/restore).

Ext4

- * Ext4 stands for fourth extended file system.
- * It was introduced in 2008.
- * Starting from Linux Kernel 2.6.19 ext4 was available.
- * Supports huge individual file size and overall file system size.
- * Maximum individual file size can be from 16 GB to 16 TB
- * Overall maximum ext3 file system size is 1 EB (exabyte).
1 EB = 1024 PB (petabyte). 1 PB = 1024 TB (terabyte).
- * Directory can contain a maximum of 64,000 subdirectories (as opposed to 32,000 in ext3)

* You can also mount an existing ext3 fs as ext4 fs (without having to upgrade it).

* Several other new features are introduced in ext4: multiblock allocation, delayed allocation, journal checksum, fast fsck, etc. All you need to know is that these new features have improved the performance and reliability of the filesystem when compared to ext3.

* In ext4, you also have the option of turning the journaling feature “off”.

Use the method we discussed earlier to identify whether you have ext2 or ext3 or ext4 file system.

Warning: Don't execute any of the commands given below, if you don't know what you are doing. You will lose your data!

Creating an ext2, or ext3, or ext4 filesystem

Once you've partitioned your hard disk using fdisk command, use mke2fs to create either ext2, ext3, or ext4 file system.

Create an ext2 file system:

```
mke2fs /dev/sda1
```

Create an ext3 file system:

```
mkfs.ext3 /dev/sda1
```

(or)

```
mke2fs -j /dev/sda1
```

Create an ext4 file system:

```
mkfs.ext4 /dev/sda1
```

(or)

```
mke2fs -t ext4 /dev/sda1
```

Converting ext2 to ext3

For example, if you are upgrading /dev/sda2 that is mounted as /home, from ext2 to ext3, do the following.

```
umount /dev/sda2  
tune2fs -j /dev/sda2
```

```
mount /dev/sda2 /home
```

Note: You really don't need to unmount and mount it, as ext2 to ext3 conversion can happen on a live file system. But, I feel better doing the conversion offline.

Converting ext3 to ext4

If you are upgrading /dev/sda2 that is mounted as /home, from ext3 to ext4, do the following.

```
umount /dev/sda2
```

```
tune2fs -O extents,uninit_bg,dir_index /dev/sda2
```

```
e2fsck -pf /dev/sda2
```

```
mount /dev/sda2 /home
```

Bom arquivo:

<http://www.vivaolinux.com.br/artigo/Fundamentos-do-sistema-Linux-discos-e-particoes>

12.10 - Configurando o GRUB

Sistema gerenciador de Boot mais usado atualmente no Linux

Mudar a ordem do menu

No boot veja qual o número da distribuição/sistema para o qual deseja alterar

```
nano /etc/default/grub
```

```
GRUB_DEFAULT=0      - mudar de 0 para o número  
desejado
```

Adicionar entrada para o Grub2

```
sudo nano /boot/grub/grub.cfg
```

```
menuentry "Windows " {  
set root=(hd0,1)  
chainloader +1  
}
```

Execute agora:

```
sudo update-grub
```

E reinicie o computador.

Reinstalar

```
grub-install /dev/sda
```

```
grub-install --root-directory=/media/sda2 /dev/sda
```

Atualizar

```
update-grub2
```

Recuperar MBR

```
sudo apt-get install lilo
```

```
sudo lilo -M /dev/sda mbr
```

Adicionar entrada para o Grub2

```
sudo nano /boot/grub/grub.cfg
```

```
menuentry "Windows " {  
  set root=(hd0,1)  
  chainloader +1  
}
```

Execute agora:

```
sudo update-grub
```

E reinicie o computador.

Reinstalar

```
grub-install /dev/sda
```

```
grub-install --root-directory=/media/sda2 /dev/sda
```

Atualizar

```
update-grub2
```

Mudar fonte da console

Alterar no

```
nano /etc/default/grub
```

```
GRUB_GFXMODE=1280x1024
```

ou

```
GRUB_GFXMODE=1024x768
```

12.11 - Configurando o Hardware via Terminal

dmesg | less – lista ocorrências do boot

```
dmesg | grep eth0
```

Exibir módulos disponíveis

```
modprobe -l | less
```

Exibir módulos carregados

```
lsmod | less
```

Inserir um novo módulo no kernel
modprobe vmhgfs

lsmod | grep vmhgfs

Carregar o novo módulo com outro nome
modprobe vmhgfs -o vm_hgfs

Remover um módulo
modprobe -r vmhgfs
Informações sobre o Hardware
Modelo do processador:
cat /proc/cpuinfo

Informações sobre o uso da memória:
\$ free -m

Exibe os dispositivos PCI:
lspci -tv

Exibe os dispositivos USB:
lsusb -tv

Hardware
/proc/cpuinfo, devices, partitions ...
lsmod
lsusb
lspci
lspnp
insmod
hdparm

12.12 - Usando o Modem ADSL

Recomenda-se configurar como bridge e usar pppoeconf, pois assim controlará todas as portas de entrada, permitindo acesso remoto ao mesmo via SSH, por exemplo e podendo usar também outros serviços que precisem das portas.

Atualmente as portas são liberadas pelas operadoras

Configuração do Modem pelo navegador

O IP depende do tipo de modem

GVT

IP 192.168.1.1

admin

gvt12345

VELOX (speedstream)

IP 192.168.1.254

login - admin

senha

VELOX (Thonson Speedtouch 510)

GVT DNS

200.175.182.139

200.175.5.139

Instalar:

```
apt-get install pppoeconf
```

pppoeconf

Entrar com os dados da operadora:

Velox

login - telefone@telemar.com.br

senha - telefone

GVT

login - turbonet@turbonet

senha - gvt25

Ver:

[http://forum.if.uff.br/viewtopic.php?](http://forum.if.uff.br/viewtopic.php?t=778&start=0&postdays=0&postorder=asc&highlight=&sid=e1f7dc9cec46996ea00e73e9fb8ef8f6)

[t=778&start=0&postdays=0&postorder=asc&highlight=&sid=e1f7dc9cec46996ea00e73e9fb8ef8f6](http://forum.if.uff.br/viewtopic.php?t=778&start=0&postdays=0&postorder=asc&highlight=&sid=e1f7dc9cec46996ea00e73e9fb8ef8f6)

Para que um Modem ADSL sem IP fixo consiga fornecer serviços para a Internet, como SSH, HTTP e outros, precisará de um DNS Dinâmico.

Crie uma conta em:

www.dyndns.com ou no No-ip

E instale o ddclient ou o no-ip

Detalhes

ddcliente no debian

aptitude install ddclient

Para reconfigurar como serviço e rodar com ppp
dpkg-reconfigure ddclient
nano /etc/ddclient.conf

```
daemon=300
pid=/var/run/ddclient.pid
protocol=dyndns2
#use=if, if=eth0
use=web, web=checkip.dyndns.org/, web-skip='IP Address'
server=members.dyndns.org
login='ribafs'
password='abir1956'
ribafs.dyndns.org
/etc/init.d/ddclient restart
```

Testar

```
ddclient -daemon=0 -query
```

```
ddclient -file /etc/ddclient.conf
```

```
ddclient -file /etc/ddclient.conf -debug -noquiet -verbose
```

Adicionar ao /etc/rc.local:

```
/etc/init.d/ddclient restart
```

Solução para quando o modem conecta, o DHCP funciona, mas o modem não navega porque o NAT não está habilitado. Tirado do seguinte endereço:

http://www.portaladsl.com.br/portala...entid_216.html

- 1- Clique no menu "Iniciar e em seguida EXECUTAR";
 - 2- Digite: telnet 192.168.1.254 (alguns modelos podem vir com 10.0.0.138) e [ENTER], tecle enter.
 - 3- Digite no usuário "User:" Administrator e [ENTER], tecle enter;
 - 4- Na tela do Telnet digite: nat [ENTER], tecle enter;
 - 5- Digite o seguinte comando para habilitar o NAT;
"ifconfig intf=Internet translation=enabled" [ENTER], tecle enter; (sem aspas)
 - 6- Após o anterior, execute o comando seguinte
"tmpladd intf=Internet outside_addr=0.0.0.1" [ENTER], tecle enter; (sem aspas)
 - 7- Como sempre salve as configurações, senão desligando o modem perde-se tudo,
Digite: "saveall" [ENTER], tecle enter; (sem aspas)
 - 8- Pode fechar o telnet, e aguarde entre 15 á 50 segundos.
 - 9- Parabéns!! Abra o navegador e teste a conexão.
- Funciona beleza!

12.13 - Montando Dispositivos no Linux pela Linha de Comando

Montar uma partição /dev/sda1 na pasta /teste
mount /dev/sda1 /teste

Desmontar a partição acima
umount /teste

Montar um pendrive na pasta /usb
Execute e observe a partição do pendrive
fdisk -l
mount /dev/sdc1 /usb

Desmontar
umount /usb

Gerando uma iso de um CD ou DVD
dd if=/dev/cdrom of=imagem.iso

Montar imagem ISO
mount /[caminho ou diretório]/[nome da imagem].iso /
[caminho ou diretório onde será montado a imagem] -o loop
mount /media/dvdrom/imagem.iso imagemdir -o loop

12.14 - Gerenciamento de Pacotes

apt-get
aptitude
dpkg

apt-get

apt-get install pacote
apt-get -f install pacote - reforçando as dependências
apt-get remove pacote
apt-get --purge remove pacote - remover também seus scripts de configuração
apt-get update - atualizar repositórios
apt-get upgrade - atualizar pacotes
apt-get dist-upgrade - atualizar para a nova versão da distribuição
apt-get install --reinstall pacote - reinstalar pacote, especialmente após apagar algum arquivo de configuração
apt-get -f install - corrigir problemas de dependência
apt-get autoclean - remover pacotes antigos e duplicados
apt-get update
apt-get upgrade -s - atualizar somente pacotes de segurança
apt-cache search nomeopartepacote

aptitude

Instalar
aptitude install pacote

Remover

`aptitude remove pacote`

Procurar pacotes existentes instalados ou não

`aptitude search nomeoupartepacote`

Os que aparecem com "i" à esquerda estão instalados.

`dpkg` - Também pode ser instalado com duplo clique no Nautilus

Instalar

`dpkg -i pacote.deb`

Remover

`dpkg -r pacote`

Reconfigurar

`dpkg-reconfigure nomecomando`

`dpkg-reconfigure phpmyadmin`

`dpkg-reconfigure keyboard-configuration` (Dell: Dell - USA - Sem tecla ALTGR e sem Compose - reiniciar)

`dpkg-reconfigure php5-mysql`

Instalação de Pacotes

Antes de instalar qualquer novo pacote, para atualizar os repositórios com os novos pacotes do servidor, execute:

`apt-get update`

Para atualizar todos os pacotes do sistema

apt-get update
apt-get upgrade

Após usar dpkg -i pacote.dep, usar:
apt-get -f install

Para instalar as dependências.

Listar tarefas
tasksel --list-tasks

Listar pacotes instalados de um serviço
tasksel --task-packages dns-server

Atualizar para uma nova versão
do-release-upgrade

12.15 - Particionamento e Formatação

Modo gráfico
gparted

Modo texto
fdisk

Visualizar todas as partições existentes
fdisk -l

Criar partição
fdisk /dev/sda

p - lista partições
n - criar nova partição
t - mudar o tipo de partição
l - lista os tipos suportados
m - ajuda

Formatando

```
mkfs.ext3 /dev/sda1  
mkfs.ext4 /dev/sda2  
mkfs.vfat /dev/sdb1
```

Para copiar a MBR execute o seguinte comando:
`dd if=/dev/sda of=sda.mbr count bs=512`

Para copiar a tabela de partição execute o seguinte comando:
`sfdisk -d /dev/sda > sda.sf`

Uma boa opção gráfica é o Gparted, que pode ser instalado pelo apt-get.

Swap

No Linux é uma partição que tem a finalidade de garantir que o servidor não trave por falta de memória RAM. Na falta de RAM a swap será usada. É importante ficar monitorando, pois caso o servidor comece a usar swap com frequência é hora de adicionar mais memória RAM ao servidor.

12.16 - Permissões

rwX
st

rwX - [r]ead, [w]rite e e[x]ecute
s - permite executar o arquivo com as permissões do dono ou do grupo do dono.
t - impede que usuários apaguem ou sobrescrevam arquivos dos outros.

Donos

u - user
g - grupo
o - outros

```
chmod -R 775 /home/backup  
chown -R joao:joao /home/backup/joao
```

```
chown -R joao:joao /home/joao/*;  
find /home/joao -type d -exec chmod 2775 {} \;  
find /home/joao -type f -exec chmod 0664 {} \;
```

Identificar arquivos com permissão de escrita para outros

```
for SIST in $(grep -v '^#' /etc/fstab | awk '($6 != "0") { print $2 }');  
do  
    find $$SIST -xdev -type f \( -perm -0002 -a ! -perm -1000 \)  
done;
```


Os arquivos que retornarem devem ser avaliados e para remover a permissão dos outros:

```
chmod o-w arquivo
```

Identificar arquivos ou grupos com proprietário inexistente

```
for SIST in $(grep -v '^#' /etc/fstab | awk '($6 != "0") { print $2 }');  
do  
    find $$SIST -xdev \( -nouser -o -nogroup \)  
done;
```

Corrigir permissões do /home

```
for DIR in `awk -F: '($3 >= 500) {print $6}' /etc/passwd`;  
do  
    chmod 700 $DIR  
done;
```

Bloquear Contas de Sistema

```
for USR in bin daemon games gdm lp mail nobody squid sync  
uucp;  
do  
    usermod -s /dev/null -L $USR  
done;
```

Para ativar conta bloqueada remover o ! antes do hash da senha

em /etc/shadow

Identificar Contas sem Senha

```
awk -F: '($2 == "") { print $1 }' /etc/shadow
```

Identificar Contas com privilégio do grupo ou do usuário root:

```
awk -F: '($3 == 0) { print $1 }' /etc/passwd
```

```
awk -F: '($4 == 0) { print $1 }' /etc/passwd
```

Somente a conta root deve ser retornada na primeira linha e o grupo root na segunda.

Impedir que arquivos sejam modificados

```
chattr +i ...
```

Desabilite programas SUID/SGID não utilizados

Primeiro Passo

Para localizar todos os arquivos com o bit 's' de arquivos que tenham o root como dono, utilize o comando:

```
find / -type f ( -perm -04000 -o -perm -02000 ) -exec ls lg {} ;
```

Para desabilitar os bits suid dos programas selecionados acima, digite o seguinte comando:

```
chmod a-s [programa]
```

Utilize o seguinte comando para procurar diretórios e arquivos

com permissão de leitura e escrita para todos:

```
find / -path /proc -prune -o -perm -2 ! -type l -ls
```

```
ls -ld /tmp
```

Remover donos

```
find / -path /proc -prune -o -nouser -o -nogroup
```

Procurar arquivos cujo dono é o usuario

```
find / -path /proc -prune -o -user usuario -ls
```

Listar todas as contas válidas

```
egrep -v '.*:.*|:!' /etc/shadow | awk -F: '{print $1}'
```

Listar contas que não têm um 'x' no campo password

```
grep -v ':x:' /etc/passwd
```

Apagar a conta

```
userdel -r <conta>
```

Forma eficiente de configurar os usuários, grupos e permissões do Apache

Permissões de arquivos para /var/www

Todos os usuários do grupo devel terão privilégios no diretório /var/www de criar arquivos e pastas.

Os arquivos e pastas criadas por cada usuário terão o próprio como dono.

Também terão privilégio de alterar os arquivos existentes, que

têm como dono www-data e grupo devel.

Quando qualquer usuário do grupo devel altera um arquivo o mesmo continua tendo como dono o www-data e assim permitindo aos demais usuários trabalhar no mesmo arquivo.

```
groupadd devel
```

```
usermod -a -G devel usera
```

```
usermod -a -G devel userb
```

```
groups usera ## exibir grupo do usera
```

Adicionar www-data ao grupo devel

```
usermod -a -G www-data devel
```

Tornar /var/www de propriedade do grupo devel :

```
chgrp devel /var/www
```

Tornar www-data o dono e devel o grupo para todo o /var/www

```
chown -R www-data:devel /var/www
```

Mudar as permissões de todos os diretórios

```
chmod 2775 /var/www ## 2=set group id, 7=rwx for owner (www-data), 7=rwx for group (devel), 5=rx for world
```

Set group ID (SETGID) bit (2) causes the group (devel) to be copied to all new files/folders created in that folder. Other options are SETUID (4) to copy the user id, and STICKY (1)

which I think lets only the owner delete files.

There's a `-R` recursive option, but that won't discriminate between files and folders, so you have to use `find`, like so:

```
find /var/www -type d -exec chmod 2775 {} \;
```

Change all the files to 0664

```
find /var/www -type f -exec chmod 0664 {} \;
```

Adaptação de dica encontrada em:

<http://serverfault.com/questions/6895/whats-the-best-way-of-handling-permissions-for-apache2s-user-www-data-in-var-w>

UMASK

Cada vez que um arquivo ou diretório é criado em seu sistema, uma permissão é setada para o mesmo, e essa permissão padrão pode ser alterada usando o comando `umask`.

Caso você digite em um terminal o comando `umask`, serão mostradas as permissões (em notação octal) padrão em seu sistema. Para alterá-las, digite:

```
# umask
```

```
umask u=rwx,g=rwx,o=rx
```

Veja os exemplos do comando `umask` para a criação de arquivos:

Permissão: rwx rwx rwx

umask 022 (equivale A:000 010 000)

Resultado: rw- r-- rw-

Permissão: rwx rwx rwx

umask 133 (equivale A:001 011 011)

Resultado: rw- r-- r--

Ou seja, quando o bit estiver em 0, a permissão será dada, quando 1, a permissão será negada. Mas observe que a permissão de execução (permissão x) não é dada, mesmo tendo o bit 0 ativado. Esta é uma proteção do Linux, que não deixa que nenhum arquivo seja criado com permissão de execução. Para setar a permissão x, utilize o comando `chmod`. A exceção são os diretórios, que podem ser criados com permissão de execução.

`chown`

O comando `chown` permite que se altere o dono e grupos relacionados ao arquivo, ou arquivos, selecionado.

`chown [proprietário:grupo] [arquivos]`

Por exemplo:

`$ chown :grupo02 documento.txt`

Altera o grupo do arquivo `documento.txt` para `grupo02`.

ACLs no Linux

Para um sofisticado compartilhamento de arquivos

Importante para trabalhar com uma grande quantidade de usuários e grupos.

ACL - Access Control List

Usadas para controlar acesso a arquivos e diretórios

Campos

123

1 - ugom (u - user, g - group, o - other, m - mask)

2 - UID

3 - Permissão

Instalando

```
aptitude -r install acl
```

Ativando o Suporte a ACLs no Filesystem

```
nano /etc/fstab
```

Altere a entrada para adicionar o suporte:

```
UUID=1135007b-c11c-44cc-80ca-eb9bcd008fb7 /  
ext3 acl,errors=remount-ro 0 1
```

Remontar

```
mount -o remount,acl /dev/sda1
```

Trabalhando com ACLs na linha de comando

Existem os seguintes utilitários para o gerenciamento de ACLs:

chacl: deixa alterar, examinar ou remover user, group, mask, ou outras ACLs nos arquivos ou diretórios

getfacl: examinar ACLs de arquivos e diretórios

setfacl: deixa configurar arquivos e diretórios das ACLs

Acessar um diretório para verificar

```
ls -la
```

```
getfacl .
```

```
getfacl resume.xml
```

Configurar ACLs pela linha de comando

Exemplos

Para adicionar o user djf como quem pode ler o arquivo resume.xml, podemos usar um comando chacl (change ACL)

assim:

```
$ chacl u::rw-,g::r--,o::---,u:djf:r--,m::rw- resume.xml
```

Veja agora

```
getfacl resume.xml
```

```
ls -la
```

Para adicionar o user djf como quem pode ler e escrever no arquivo resume.xml, podemos usar um comando chacl assim:


```
$ chacl u::rw-,g::r--,o::---,u:djf:rw-,m::rw- resume.xml
```

Veja então

```
getfacl resume.xml
```

Trabalhando com ACLs com uma ferramenta gráfica

Eiciel

GNOME File ACL editor

Interface gráfica para configurar, atualizar e remover ACLs.

Lembre que somente poderá abrir arquivos ou diretórios da partição que adicionou suporte a ACL no fstab.

Veja que tem abaixo um botão Ajuda com um Help em inglês sobre o uso do Eiciel.

12.17 - Gerenciamento de Processos

Para saber o PID

```
ps ax |grep apache
```

Matando o processo com o PID

```
kill -9 PID
```

Alternativa, que restarta o processo

```
killall gdm
```

Listar processos

```
pstree -p
```

Listar processor e várias outras informações como RAM, CPU, etc

top

ntop

apt-get install ntop

12.18 - Regras que o sysadmin não pode quebrar

- Backup sempre e validação do backup regularmente

- Use muito a linha de comando e evite sempre a interface gráfica

Tudo em UNIX/Linux se pode fazer na linha de comando e nem tudo no ambiente gráfico

- Automatize sempre que possível, para ficar com tempo para outras atividades

Toda tarefa que se repete pode e deve ser automatizada

12.19 - Configurações da Rede

Tipos de Redes

PAN - Personal Area Network - Geralmente para uma única pessoa. Exemplo: bluetooth

WPAN - Wireless Personal Area Network - idem mas wireless

LAN - Local Area Network - ou Departamentais - Num prédio ou numa sala. WLAN

MAN - Metropolitan Area Network - Redes metropolitadas. No máximo uma cidade. Exemplo: interligar duas redes LAN.

WMAN.

WAN - Wide Area Network - Grandes redes que ligam países e continentes. WMAN

Conceitos

HUB - Interligar computadores. Não possui gerenciamento. Somente dois computadores podem trocar informações por vez.

Usam topologia de barra.

SWITCH - Interligam computadores e possuem gerenciamento. Dois ou mais computadores podem se comunicar ao mesmo tempo.

Usam topologia de estrela.

Repetidor - Amplificam o sinal da rede. Hubs e Switchs possuem repetidor interno.

Roteador - Possibilita comunicação entre redes diferentes.

Alguns também são switchs. Ex.: ligar uma LAN com a WAN.

Bridge - Interliga duas ou mais redes de protocolos semelhantes ou diferentes, através dos MACs.

```
route -n
route add default gw 10.0.0.2 eth0
ifconfig eth0 10.10.0.8 netmask 255.0.0.0 up
ifconfig
ifconfig -a
ifconfig eth0
ifup eth0
ifdown eth0
```

Servidor com duas Placas de Rede :
modem - eth0 - Servidor - eth1 - switch (LAN)

Servidor com Apenas uma Placa de Rede :
modem - Switch - eth0 - Servidor (eth0:1)

Fixar interfaces no Debian e derivados

```
apt-get install ifrename
nano /etc/iftab
eth0 mac mac0
eth1 mac mac1
```

```
telnet opcoes ip/dns porta
traceroute opcoes host/ip
```

Restartando rede com DHCP

```
killall dhclient
/etc/init.d/networking restart
```

Portas comuns

25

22

80

53 tcp/udp

DNS públicos

8.8.8.8 - Google

2.2.2.2 - Embratel

Após a troca de HDs de um computador

Editar /etc/udev/rules.d/70-persistent-net.rules

Deletar linhas com eth0 e eth1

Sincronizar relógio

`ntpdate -u pool.ntp.br`

`hostname --short`

`hostname --domain`

`hostname --fqdn`

`server.home.lan`

`hostname --ip-address`

`192.168.1.100`

Varrer uma faixa de IPs

`sudo nmap -sP 10.40.0.100-200`

`netstat -lutan`

`netstat -lute`

telnet localhost porta

Máscara Explicada

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

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

- 1) Você 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 cálculo de máscara usando 24 bits, numa comparação XOR bit-a-bit que vai resultar em 189.22.33.0
- 3) Ele vai pegar o resultado do cálculo 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 comparação XOR bit-a-bit e vai ter como resultado 189.0.0.0, com esse resultado ele vai comparar 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

12.20 - Scripts de Configuração do Debian/Ubuntu e similares

/etc/apt/sources.list
/etc/hostname
/etc/hosts
/etc/network/interfaces e alias
/etc/fstab
/etc/resolv.conf
/etc/dhcp/dhcpd.conf
/etc/samba/smb.conf
/etc/squid/squid.conf
/home/user/.bashrc
/etc/skel/
/etc/securetty
/etc/mysql/my.cnf

```
/etc/postgresql/8.4/main/postgresql.conf  
/etc/postgresql/8.4/main/pg_hba.conf
```

Exemplo de alguns scripts

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

```
auto lo eth0 eth1
```

```
iface lo inet loopback
```

```
iface eth0 inet dhcp
```

```
iface eth1 inet static  
    address 192.168.0.1  
    netmask 255.255.255.0  
    broadcast 192.168.0.255
```

```
/etc/dhcp3/dhcpcd.conf
```

```
# DHCP server is authoritative for all networks  
authoritative;
```

```
# extra options
```

```
# RFC3442 routes
```

```
option rfc3442-classless-static-routes code 121 = array of  
integer 8;
```

```
# MS routes
```

```
option ms-classless-static-routes code 249 = array of integer 8;
```

```
pid-file-name "/var/run/dhcp3-server/dhcpcd.pid";
```

```
ddns-update-style none;
```

```
option domain-name-servers 200.175.5.139, 200.175.89.139;
```



```
default-lease-time 1800;
max-lease-time 7200;

shared-network eth1 {
    subnet 192.168.0.0 netmask 255.255.255.0 {
        option routers 192.168.0.1;
        option domain-name-servers 192.168.0.1;
        default-lease-time 1800;
        max-lease-time 7200;

        pool {
            range 192.168.0.2 192.168.0.10;
        }
    }
}

group {
    option routers 192.168.0.1;
    option domain-name-servers 192.168.0.1;
    default-lease-time 1800;
    max-lease-time 7200;
}
}
```

/etc/resolv.conf

```
nameserver 200.175.5.139
nameserver 200.175.89.139
```

squid.conf Básico

/etc/squid/squid.conf

squid.conf básico (squid 2)

http_port 3128

visible_hostname dnocs

acl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255

acl SSL_ports port 443 563

acl Safe_ports port 21 80 443 563 70 210 280 488 59 777 901
1025-65535

acl purge method PURGE

acl CONNECT method CONNECT

http_access allow manager localhost

http_access deny manager

http_access allow purge localhost

http_access deny purge

http_access deny !Safe_ports

http_access deny CONNECT !SSL_ports

acl redelocal src 192.168.1.0/24

http_access allow localhost

http_access allow redelocal

http_access deny all

squid.conf Ampliado (versão 2)

/etc/squid/squid.conf

squid.conf (ampliado)

http_port 3128

visible_hostname dnocs

error_directory /usr/share/squid/errors/Portuguese/

cache_mem 64 MB

maximum_object_size_in_memory 64 KB

maximum_object_size 512 MB

minimum_object_size 0 KB

cache_swap_low 90

cache_swap_high 95

cache_dir ufs /var/spool/squid 2048 16 256

cache_access_log /var/log/squid/access.log

refresh_pattern ^ftp: 15 20% 2280

refresh_pattern ^gopher: 15 0% 2280

refresh_pattern . 15 20% 2280

acl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255

acl SSL_ports port 443 563

acl Safe_ports port 21 80 443 563 70 210 280 488 59 777 901
1025-65535

acl purge method PURGE

acl CONNECT method CONNECT

http_access allow manager localhost

http_access deny manager

```
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
```

```
acl bloqueados url_regex -i "/etc/squid/bloqueados"
http_access deny bloqueados
```

```
acl redelocal src 192.168.1.0/24
http_access allow localhost
http_access allow redelocal
```

```
http_access deny all
```

Criar o arquivo /etc/squid/bloqueados, contendo os sites proibidos, um por linha

Script firewall

```
#!/bin/sh
# Pequeno firewall criado por Ribamar FS para o SINDIFORT
# Com compartilhamento de internet
# Carregar módulos
modprobe ip_tables
modprobe iptable_nat
modprobe ipt_MASQUERADE
WAN=eth0
LAN=eth1
REDE=192.168.0.0/255.255.255.0
FW="/etc/init.d/firewall"
#
case "$1" in
```

```
start)
#
echo "[*] Iniciando o Firewall..."
# Definindo política inicial
iptables -t filter -P INPUT DROP
iptables -t filter -P OUTPUT ACCEPT
iptables -t filter -P FORWARD ACCEPT
#
iptables -A INPUT -m state --state RELATED,ESTABLISHED
-j ACCEPT
#
# Compartilhando a Internet - NAT
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
#
# Aceitar Entrada do SSH e Webmin
iptables -A INPUT -p tcp --dport 60022 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
#
# Aceita todo o trafego vindo do loopback e indo pro loopback
iptables -I INPUT -i lo -j ACCEPT
iptables -I OUTPUT -o lo -j ACCEPT
#
#
# Liberar $REDE local
#iptables -A INPUT -p tcp --syn -s $REDE -j ACCEPT
#
#iptables -A INPUT -p tcp --syn -s $REDE -j ACCEPT
#
# Proteção contra IP Spoofing #####
for i in /proc/sys/net/ipv4/conf/*/rp_filter; do
```

```
echo 1 >$i
done
#
# Proteger contra pacotes mal formados
#iptables -A FORWARD -m unclean -j DROP
#
# Redirecionar todas as requisições da porta 80 para a 3128 do
Squid...
# Abre a porta 3128 tcp udp, para o uso do squid
iptables -A INPUT -p tcp --destination-port 3128 -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
REDIRECT --to-port 3128
#
# Qualquer outro tipo de trafego é aceito
iptables -A INPUT -i $WAN -j ACCEPT
#
#
;;
stop)
echo "[*] Parando o Firewall..."
iptables -F
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -t mangle -F
iptables -t nat -F
iptables -X
iptables -Z
#
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

```
;;
restart)
    $FW stop
    $FW start
;;
*)
    echo "Use: $N {start|stop|restart}"
esac
exit 0
```

interfaces com aliases

```
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
#
```

```
auto eth0
iface eth0 inet static
    address 10.40.100.10
    netmask 255.0.0.0
    network 10.0.0.0
    broadcast 10.255.255.255
    gateway 10.0.0.1
    # dns-* options are implemented by the resolvconf
package, if installed
    dns-nameservers 10.0.0.1
```

```
auto eth0:0
iface eth0:0 inet static
    address 10.40.0.5
    netmask 255.255.255.0
```

```
network 10.40.0.0  
broadcast 10.40.0.255
```

```
auto eth0:1  
iface eth0:1 inet static  
    address 10.40.1.5  
    netmask 255.255.255.0  
    network 10.40.1.0  
    broadcast 10.40.1.255
```

```
auto eth0:2  
iface eth0:2 inet static  
    address 10.40.2.5  
    netmask 255.255.255.0  
    network 10.40.2.0  
    broadcast 10.40.2.255
```

```
auto eth0:3  
iface eth0:3 inet static  
    address 10.40.3.5  
    netmask 255.255.255.0  
    network 10.40.3.0  
    broadcast 10.40.3.255
```


12.21 - Operações com serviços

/etc/init.d/servico ação

Alguns serviços já aceitam a sintaxe:
service serviço ação

ação: restart, stop, start, reload, status, etc

Adicionar ao boot
update-rc.d firewall defaults

Remover
update-rc.d -f firewall remove

Teste Sintaxe

Samba
testparm

Squid
squid -k parse
Vistual Host do Apache - apache2ctl -S
apachectl configtest

Iptables

iptables -n -L (listar regras e políticas)

Limpar regras da memória
iptables -F

iptables -F -t nat

iptables -L

iptables -L | grep 80

Descobrir Função dos Serviços

whatis nomeserviço

whatis squid3

12.22 - Gerenciamento de Usuários e Grupos

Criar usuário

adduser nome

Adicionar usuário sem login nem home

adduser --disabled-login --no-create-home nome

useradd nome

Remover Usuário

userdel user

userdel nome --remove-home

Criar Grupo

addgroup nomegrupo

groupadd nomegrupo

Bloquear login

passwd -l user

Desbloquear

passwd -u user

Bloquear usuário no Samba

smbpasswd -d login

Remover no samba

smbpasswd -x login

Desbloquear no samba

smbpasswd -e login

Adicionar Usuário a Grupo

adduser login grupo

chgrp - mudar grupo

umask - mudar a máscara, que ficará padrão

12.23 - Dicas sobre Servidores Windows

Reiniciar a rede

c:\ipconfig /release

c:\ipconfig /renew

Criar Script .bat para Controlar as horas de ligar e desligar o computador:

```
===ligar.bat===
```

```
REM Desligar computador se ligado antes das 16 horas
```

```
IF %time:~0,5% LEQ 16:00 shutdown -s -f -t 60
```

```
REM Desligar computador se ligado após as 22 horas
```

```
IF %time:~0,5% GEQ 22:00 shutdown -s -f -t 60
```

```
=====
```

Adicionar este script ao Inicializar

Criar um segundo script apenas com:

```
====desligar.bat=====
```

```
REM Desligar computador se ligado após as 22 horas
```

```
IF %time:~0,5% GEQ 22:00 shutdown -s -f -t 60
```

```
=====
```

Criar um Agendamento de Tarefa e adicione este script para ficar atento para desligar as 22.

12.24 - Política de Segurança

Invasões devem ser comunicadas ao CERT BR:

<http://www.cert.br/contato/>

Fatores da Segurança:

segurança – risco – flexibilidade

Aumentando um reduz os outros.

Segurança Física

É a primeira que deve ser garantida, pois em se permitindo acesso físico não há como garantir segurança dos servidores. Acesso à sala dos servidores somente à equipe, ao pessoal autorizado ou com supervisão.

Ativar senha na BIOS

Otimizar BIOS, removendo recursos sem uso

Após a instalação do SO desativar boot por dispositivos removíveis

Adicionar senha criptografada no GRUB

Segurança das Ações

Devemos ter bons scripts que monitorem todo o sistema e que ajudem a cuidar dos servidores.

Cuidado com Dados dos Servidores

Cuidado tanto dos scripts quanto dos dados armazenados em bancos. As informações existentes sobre os servidores (IPs, serviços, usuários, etc) devem ficar em sigilo.

Backup

Efetuar backup regularmente e guardar sempre várias cópias, pois uma cópia comprometida não deve nunca ser usada para restauração.

Partições

É muito importante que tenhamos sempre pelo menos as partições /, /boot, /usr, /var, /tmp e /home, para não correr o risco da partição /var encher e comprometer todo o sistema por invadir a raiz.

Firewall Seguro

Um bom firewall com iptables é peça importante da segurança. A política ideal é fechar todas as portas e abrir apenas as que são necessárias.

Verificar portas:

```
netstat -tulp  
sudo nmap -sTU 10.40.100.123  
sudo lsof -i -n | egrep 'COMMAND|LISTEN|UDP'
```

Evitar softwares inseguros

FTP, telnet, rlogin e outros similares devem ser evitados, pois são inseguros, trafegando senhas em texto claro.

Instalação dos Servidores

A instalação deve sempre ser a mais enxuta possível. F4 – install Minimal System e somente adicionar o SSH. Os demais pacotes devem ser instalados após a instalação do só. Após a instalação evitar ao máximo a instalação de softwares que não estejam nos repositórios oficiais. E para aqueles que tiverem um repositório próprio e sejam confiáveis adicionar este repositório.

Informações Específicas

Manter-se bem informado, especialmente sobre segurança e seus problemas. Assinar listas e fóruns é uma medida indicada. Assim como a compra de bons livros e cursos.

Atualização do Sistema Operacional

Pelo menos as atualizações de segurança devem ser feitas automaticamente.

Senhas Fortes

Caso nós tenhamos todos os cuidados necessários para uma boa segurança e relaxemos nas senhas, todo o nosso trabalho será perdido. Por isso as senhas são um fator importantíssimo da segurança e devem ser bem fortes. Usemos para as senhas dos servidores senhas conendo letras, números e símbolos e também devemos recomendar fortemente que as senhas das estações e seus usuários devam ser fortes.

Além de forte as senhas devem ser de possível memorização para que não precisem ser anotadas.

Segurança nas Estações

É importante também cuidar da segurança nas estações, pois elas também fazem parte da rede e nelas estão usuários que estão bem próximo aos servidores. É prudente instalar antivírus em estações Windows, assim como instalar também nos servidores para que não sejam repassadores dos vírus que por eles possam trafegar via sistema de arquivos.

Também é importante uma política de segurança e sua divulgação junto aos usuários, como também implantar senhas fortes e obrigar a troca periódica.

12.25 - Dicas de Segurança para Servidores Linux

Configurações iniciais com otimizações

Hardening

- Desinstalar pacotes não usados

- Desabilitar serviços sem uso

- Modo gráfico somente se necessário e útil

/etc/hosts.allow

/etc/hosts.deny

Segurança na partição /tmp

Como a partição tmp oferece acesso com escrita para todos ela é muito visada pelos hackers. Então vamos melhorar sua segurança, editando o /etc/fstab e alterando a linha da /tmp

```
/dev/sda7 /tmp ext3 defaults,noexec,nodev 0 0
```

Instalar Alguns Pacotes

```
apt-get install ssh mc sysv-rc-conf fail2ban rkhunter ncd htop  
resolvconf gpm
```

fail2ban - bloqueia (no iptables) acessos via SSH após algumas tentativas erradas

```
rkhunter --update  
rkhunter -c
```

Exigindo Senhas Fortes

passwdqc - password/passphrase strength checking and enforcement

passwdqc is a password/passphrase strength checking and policy enforcement toolset, including an optional PAM module (pam_passwdqc), command-line programs (pwqcheck and pwqgen), and a library (libpasswdqc).

On systems with PAM, pam_passwdqc is normally invoked on password changes by programs such as passwd(1). It is capable

of checking password or passphrase strength, enforcing a policy, and offering randomly-generated passphrases, with all of these features being optional and easily (re-)configurable.

pwqcheck and pwqgen are standalone password/passphrase strength checking and random passphrase generator programs, respectively, which are usable from scripts.

```
apt-get update  
apt-get upgrade  
apt-get install passwdqc
```

As senhas agora precisarão conter letras maiúsculas, minúsculas, números e símbolos ou conterem uma frase com 3 palavras.

Para melhorar a segurança, evite usar o servidor com usuário root. Usar geralmente uma conta de usuário comum. Usar o root somente quando requerido.

É recomendável não usar outros serviços no servidor de firewall. Que outros serviços como DHCP, squid, DNS e outros fiquem num segundo servidor ou em servidores separados.

12.26 – Usando Dois Links nos Servidores

Existem alguns motivos para se usar dois links em um servidor: balanceamento de carga ou simplesmente uma certa disponibilidade, para o caso de um link cair ter o outro ativo. Dois links acarretam um certo conforto para o administrador,

que pode estar usando por exemplo o segundo link para atualizar o servidor e deixando o primeiro para atender a rede.

No `/etc/network/interfaces` podemos ter algo assim:

```
auto eth0
iface eth0 inet static
    address 192.168.0.100
    netmask 255.255.255.0
    gateway 192.168.0.1
```

```
auto eth1
iface eth1 inet static
    address 10.10.0.100
    netmask 255.255.0.0
```

Não usar duas placas com gateway, devemos usar apenas um gateway por interfaces.

12.27 - Alguns Comandos Linux

Locate

locate - localizar arquivos. Como tem um banco de dados ele localiza rapidamente.

Precisamos atualizar seu banco de dados após a instalação de programas ou a criação de arquivos, usando o comando:

```
updatedb
```

Exemplos

```
locate sysctl.conf
```

Resultado:

```
/etc/sysctl.conf  
/etc/ufw/sysctl.conf  
/usr/share/doc/procps/examples/sysctl.conf  
/usr/share/man/man5/sysctl.conf.5.gz
```

Exibindo toda a saída em uma única linha:

```
locate -0 sysctl.conf
```

Receber apenas a quantidade de ocorrências

```
locate -c sysctl.conf
```

Exibindo apenas os arquivos existentes de fato. Caso algum arquivo seja excluído e o updatedb ainda não tenha sido executado, o arquivo excluído continuará aparecendo no comando:

```
locate sysctl.conf
```

Se executarmos o comando abaixo o excluído não aparecerá, pois aparecerá apenas os existentes

```
locate -e sysctl.conf
```

Ignorar o case na localização

```
locate -i sysctl.conf
```

ou

```
locate -i SYSCTL.conf
```

Restringindo os resultados

```
locate -l 5 passwd
```

```
locate -l 2 passwd
```

Formatar Partição Linux:

Formatando ext4 :

```
umount /dev/sdb1  
mkfs -t ext4 /dev/sdb1
```

Formatando ext3:

```
umount /dev/sdb3  
mkfs -t ext3 /dev/sdb3
```

Converter formatos de áudio e vídeo

FLV para AVI

```
mencoder -ovc lavc -oac mp3lame arquivo.flv -o arquivo.avi
```

AVI para MP4

```
ffmpeg -i vagabundo.avi -f mp4 vagabundo.mp
```

Alterar o Java atual

```
sudo update-alternatives --config java
```

Baixar arquivo com wget e salvar em outra pasta automaticamente:

```
sudo wget  
http://wine.budgetdedicated.com/apt/sources.list.d/hardy.list -O  
/etc/apt/sources.list.d/winehq.list
```

Editores

```
mcedit (apt-get install mc)  
nano (já vem por default)  
vi (já vem por default)
```

ls -la – mostra todos os atributos dos arquivos, inclusive os ocultos

ls -lh - mostra o tamanho dos arquivos

w - quem está conectado e o que faz

lynx - browser texto

w3m - browser texto

uname -a ou -r - mostra detalhes do kernel

du -sh - mostra o tamanho de todos os arquivos de um diretório

du -sh /home - mostra o tamanho de todos os arquivos do diretório /home

df -h - mostra todas as partições montadas com tamanho legível pelo ser humano (-h)

free -m - mostra tamanho da memória e do swap em MB. Para KB usar k e GB usar g

dmesg | grep eth - procurar por mensagem no boot que contenha a substring eth, como eth0

pwd - mostra o diretório atual

cp -ra /origem /destino - copiar todo o diretório /origem para /destino preservando os atributos

cat - mostrar conteúdo de arquivo texto na tela. Ex.: cat /etc/passwd

less - lista conteúdo de arquivo texto paginando e podendo passar e voltar

more - lista conteúdo de arquivo texto paginando mas apenas passando, sem voltar

touch - cria arquivo vazio: touch nome.bat

find - localiza arquivos e mostra na tela os encontrados: find / nomearquivo

grep - localiza string ou substring em arquivos: grep “queue”
/etc/postfix/main.cf

```
teste1.txt  
abcd  
bcde  
cdef  
defg
```

```
teste2.txt  
efgh  
fghi  
ghij  
hijk
```

paste - concatena colunas de artigos texto em novo arquivo:
paste teste1.txt teste2.txt > teste3.txt

```
teste3.txt conterà:  
abcd  efgh  
bcde  fghi  
cdef  ghij  
defg  hijk
```

tail -f /var/log/messages - mostra conteúdo de messages na tela
à medida que ele cresce

```
shutdown -h now - desliga o computador agora (now)  
shutdown -r now - reinicia o computador agora (now)  
shutdown -r +06:00 - reinicia o computador daqui há 6 horas  
shutdown -r +60 - reinicia o computador daqui há 60 minutos
```

halt - desligar computador
reboot - reiniciar

cal – mostrar o calendário no terminal

cut - traz colunas de arquivos texto ou da saída padrão

passwd - trocar senha de usuário no terminal

sort - Escreve de forma ordenada a concatenação do(s)
ARQUIVO(s) na saída padrão.

Exemplo: sort teste1.txt teste2.txt > teste4.txt

teste4.txt conterà:

abcd

bcde

cdef

defg

efgh

fghi

ghij

hijk

sudo - executa um comando como superusuário, mas para isso o usuário precisa estar habilitado.

su - passa para o root. Usado assim: su – nomeusuário passará para um usuário.

whereis - localiza binários

who - mostra usuários conectados e seu terminal

whoami - mostra quem é o usuário atual

12.28 – Quebrando a senha do root

Em casos de perda da senha do root e em outros casos em que precisamos quebrar a senha do root, precisaremos geralmente de um Live CD com um Linux.

Efetuar o boot

Ao final acessar um terminal e executar:

Para visualizar as partições do HD:

```
fdisk -l
```

Criar um diretório temporário (acima anote quem é a partição raiz, por exemplo sda1):

```
mkdir teste
```

Montar a raiz em teste:

```
mount /mnt/sda1 teste
```

Acessar o diretório /etc:

```
cd teste/etc
```

```
nano passwd
```

A primeira linha está mais ou menos assim:

```
root:x:0:0:root:/root:/bin/bash
```

Altere removendo apenas o “x”:

```
root::0:0:root:/root:/bin/bash
```


Salve e saia com CTRL+O e CTRL+X

Agora desmonte a partição:
umount /dev/sda1

Reinicie

Agora poderá acessar o root sem senha. Apenas entre com root para o usuário e quando solicitar a senha apenas tecle Enter.

Não esqueça de adicionar uma senha para o root:

passwd root

12.29 – Dicas para o Desktop

Desktop

Algumas sugestões de customização para uma máquina desktop com Ubuntu 11.10

- Atalhos do teclado

Clique no ícone Configurações de Sistema - Teclado - Atalho

Atalhos Personalizados

Entre com o nome e o comando

Feche e abra novamente

Agora clique no atalho criado e clique novamente para editar e entrar com a tecla de atalho

Assim entre com os demais atalhos

- Configurações no Náutilus

Configurar Náutilus para abrir arquivos e pastas com clique único

Editar - Preferência - Comportamento - Clique único para abrir itens

Criar Marcadores/Favoritos na Lateral do Nautilus

Caso não vá usar, remova os existentes

Abra uma pasta que use com frequência e arraste para à esquerda (abaixo da Lixeira) e solte

Assim proceda com as demais para não precisar ficar procurando suas pastas mais usadas

- Customizar Firefox

Baixar a última versão de <http://mozilla.org> e usar no lugar do Iceweasel

Editar - Preferências - Principal

Ao iniciar o firefox - Abrir página em branco

Fechar ao concluir todos os downloads

Sempre perguntar onde salvar arquivos

Instalar as extensões

xmarks

DownloadHelper

- Configurar LibreOffice

Ferramentas - Opções - Caminhos

Selecionar à direita Meus Documentos - Editar (indicar /backup/transp) - Ok

Ferramentas - Personalizar - Teclado

Configurar a combinação de teclas Ctrl+9 para aumentar fonte de texto selecionado

Categoria - Formatar

Função - Aumentar Fonte

Tecla de Atalho - Ctrl + 9 e Modificar (BrOffice.org)

Configurar a combinação de teclas Ctrl+8 para redizer fonte de texto selecionado

Categoria - Formatar

Função - Reduzir Fonte

Tecla de Atalho - Ctrl + 8 e Modificar (BrOffice.org)

- Atualizar - Sistema - Administração - Gerenciador de Atualizações

- Instalar pacotes adicionais

```
apt-get install flashplugin-nonfree gimp gnucash scribus  
audacity mplayer kino vlc k3b k3b-i18n kompozer sun-java6-  
plugin filezilla
```

12.29 – Infraestrutura de Redes

Devemos cuidar bem de todos os fatores envolvidos com os servidores.

Começar pelos circuitos que alimentam os servidores. Estes circuitos devem ser bem dimensionados, de forma que os disjuntores disparem quando houver algum problema. Para isso precisará de um bom eletricitista ou engenheiro.

Os aparelhos de ar condicionado da sala também precisam ter seus disjuntores bem dimensionados. Nunca deve acontecer de os aparelhos de ar condicionado desligarem e os computadores ficarem funcionando. Para isso é importante que seus disjuntores sejam bem dimensionados.

Outro componente da parte elétrica que também deve ser bem dimensionado de forma a atender de fato toda a potência dos servidores é o no-break.

Não existe complicação para se dimensionar um circuito elétrico. Apenas precisamos conhecer a potência de cada componente, somar e ao final jogar um fator de segurança em cima (em torno de 60%).

Exemplo:

16 servidores Dell (870W cada) = 13.920W

2 storages EMC/Dell (440W cada) = 880W

1 robô Dell = 440W

8 servidores Itautec (760W cada) = 6.080W

2 servidores comuns (400W cada) = 800W

5 Switchs (aproximadamente 30W cada) = 150W

4 Roteadores ou coisa que o valha (EMBRATEL) = 120W

2 Servidores VOIP (400W cada) = 800W

8 equipamentos com antena do VOIP (12W cada) = 96W

4 roteadores ou similares do VOIP = 120W

Totalizando 23.406W

Com 60% fica $23406 * 1,60 = 37449,6W$ ou 37KVA

12.30 – Material extra por download

No site abaixo:

<http://ribafs.org/livros/servidores>

estou oferecendo vários tutoriais de terceiros que tenho acumulado aqui durante algum tempo.

Login – servidores

Senha – z01mx92nser