



# **Recuperação do sistema**

# Sumário

## Capítulo 1

Recuperação do sistema.....	3
1.1. Mãos a obra.....	4

## Capítulo 2

Gerenciando .....	18
2.1. Objetivos.....	18
2.1. Troubleshooting.....	18

## Índice de tabelas

## Índice de Figuras

# Capítulo 1

## Recuperação do sistema

- Habilitar o shell a partir da inicialização;
- Recuperar senha do root;
- Retirar senha do Grub;
- Manutenção do sistema com Live CD;

## 1.1. Mãos a obra

A inicialização do sistema começa quando o kernel é carregado pelo Lilo ou Grub, e daí em diante temos a identificação do hardware e carregamento dos daemons, e em alguns desses estágios você pode encontrar travamentos no sistema.

Quando tudo ocorre bem no boot, ainda existe a perda da senha do root, quando por exemplo o sistema foi configurado por terceiros.



O que posso fazer para recuperar o sistema nessa situação?

Na tela de inicialização do Grub é possível editar parâmetros de inicialização para manutenção ou recuperação do sistema. Vamos a prática:

Ao ligar a máquina você encontra a tela de inicialização do Grub com a lista de sistemas operacionais, e logo abaixo a indicação das teclas “e” para editar e “c” para linha de comando. Escolha o sistema e tecla “e”, no nosso caso a primeira opção de cima para baixo.

```
GNU GRUB  version 0.97  (639K lower / 392128K upper memory)

Debian GNU/Linux, kernel 2.6.26-2-686
Debian GNU/Linux, kernel 2.6.26-2-686 (single-user mode)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
```

A próxima tela você encontra uma lista com informações da partição (root), imagem do kernel (kernel) e imagem do initrd (kernel). Logo abaixo mais indicações de teclas, vamos a descrição:

*b* - Inicia o boot com as alterações;

*e* - Edita a configuração da linha selecionada;

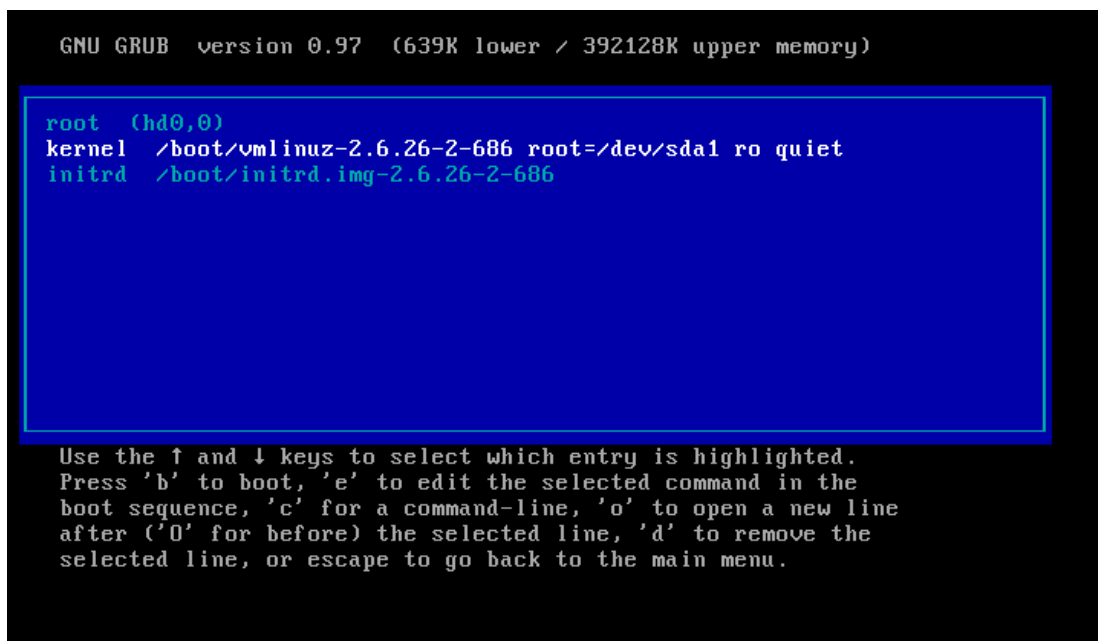
*c* - Abre um prompt do Grub para digitar comandos;

*o* - Abre uma linha vazia após a linha selecionada;

*O* - Abre uma linha vazia antes da linha selecionada;

*d* - Apaga a linha selecionada;

*ESC* - Retorna a tela anterior.

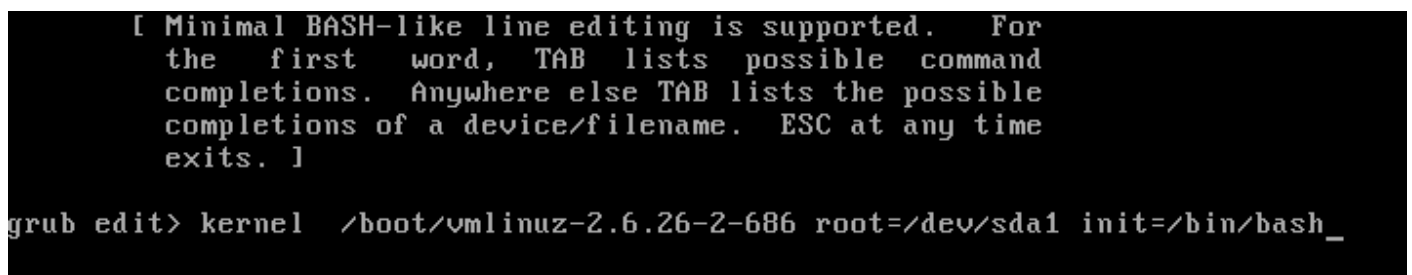


```
GNU GRUB version 0.97 (639K lower / 392128K upper memory)

root (hd0,0)
kernel /boot/vmlinuz-2.6.26-2-686 root=/dev/sda1 ro quiet
initrd /boot/initrd.img-2.6.26-2-686

Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
```

Para iniciar uma recuperação do sistema, vamos habilitar um shell com poderes de root a partir da inicialização. Para isso selecione a linha “kernel” e tecle “e”, e ao final da linha apague “ro quiet” e digite `init=/bin/bash`.



```
[ Minimal BASH-like line editing is supported. For
the first word, TAB lists possible command
completions. Anywhere else TAB lists the possible
completions of a device/filename. ESC at any time
exits. ]

grub edit> kernel /boot/vmlinuz-2.6.26-2-686 root=/dev/sda1 init=/bin/bash_
```

Para continuar nossa recuperação tecle “Enter” e “b” para dar boot com essas novas configurações.

```
[ 7.868281] sd 0:0:0:0: [sda] 20971520 512-byte hardware sectors (10737 MB)
[ 7.869666] sd 0:0:0:0: [sda] Write Protect is off
[ 7.870836] sd 0:0:0:0: [sda] Write cache: enabled, read cache: enabled, does
n't support DPO or FUA
[ 7.874399] sda: sda1 sda2 < sda5 sda6 sda7 sda8 sda9 >
[ 7.949476] sd 0:0:0:0: [sda] Attached SCSI disk
done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... kinit: name_to_dev_t(/dev/sda?) = sda
7(8,7)
kinit: trying to resume from /dev/sda7
[ 8.442424] PM: Starting manual resume from disk
kinit: No resume image, doing normal boot...
done.
[ 8.520311] EXT3-fs: INFO: recovery required on readonly filesystem.
[ 8.521594] EXT3-fs: write access will be enabled during recovery.
[ 8.641038] kjournald starting. Commit interval 5 seconds
[ 8.642264] EXT3-fs: sda1: orphan cleanup on readonly fs
[ 8.940313] EXT3-fs: sda1: 11 orphan inodes deleted
[ 8.940313] EXT3-fs: recovery complete.
[ 8.944514] EXT3-fs: mounted filesystem with ordered data mode.
Begin: Running /scripts/local-bottom ... done.
done.
Begin: Running /scripts/init-bottom ... done.
root@(none):/# _
```

Vamos recuperar a senha do root usando o comando `passwd`.



O que fazer quando recebo a mensagem `bash: passwd: command not found`

Nesta situação o comando `passwd` (`/usr/bin/passwd`) não foi encontrado, devido ao esquema de particionamento, onde o diretório `usr` esta em uma outra partição.

Para descobrir em qual partição se encontra o `usr`, monta-la e assim alterar a senha do root vamos as passos:

Exiba o conteúdo do `/etc/fstab` com o comando `cat`:

```
root@(none):/# cat /etc/fstab
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc defaults 0 0
/dev/sda1 / ext3 errors=remount-ro 0 1
/dev/sda9 /home ext3 defaults 0 2
/dev/sda8 /tmp ext3 defaults 0 2
/dev/sda5 /usr ext3 defaults 0 2
/dev/sda6 /var ext3 defaults 0 2
/dev/sda7 none swap sw 0 0
/dev/hdc /media/cdrom0 udf,iso9660 user,noauto 0 0
```

No nosso exemplo indica que o `usr` esta no `/dev/sda5`, onde pode ser montado usando o comando `mount -t ext3 /dev/sda5 /usr` ou apenas `mount /usr`

```
root@(none):/# mount /usr
[ 515.046031] kjournald starting. Commit interval 5 seconds
[ 516.085288] EXT3 FS on sda5, internal journal
[ 516.085288] EXT3-fs: sda5: 1 orphan inode deleted
[ 516.237106] EXT3-fs: recovery complete.
[ 516.239325] EXT3-fs: mounted filesystem with ordered data mode.
```

Com o `usr` montado podemos usar o comando `passwd` para mudar a senha do `root`. Reinicie a maquina com a combinação `CTRL + ALT + DEL`

```
root@(none):/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: Authentication token lock busy
passwd: password unchanged
```

### Retirar senha do Grub

A recuperação do sistema editando a tela do Grub, é muito útil e também muito utilizada. Mas quando colocado uma senha para aumentar a segurança na tela do Grub, impedindo que alguém edite as configurações, o que se pode fazer para recuperar esta senha. Veja um exemplo:

```
GNU GRUB  version 0.97  (639K lower / 392128K upper memory)

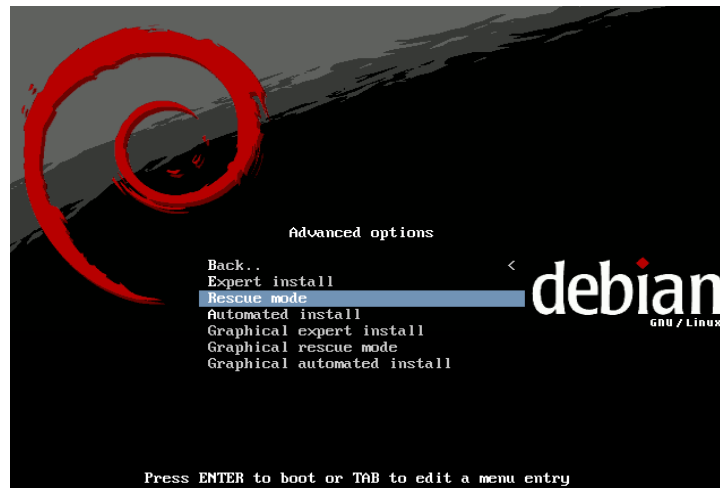
Debian GNU/Linux, kernel 2.6.26-2-686
Debian GNU/Linux, kernel 2.6.26-2-686 (single-user mode)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.

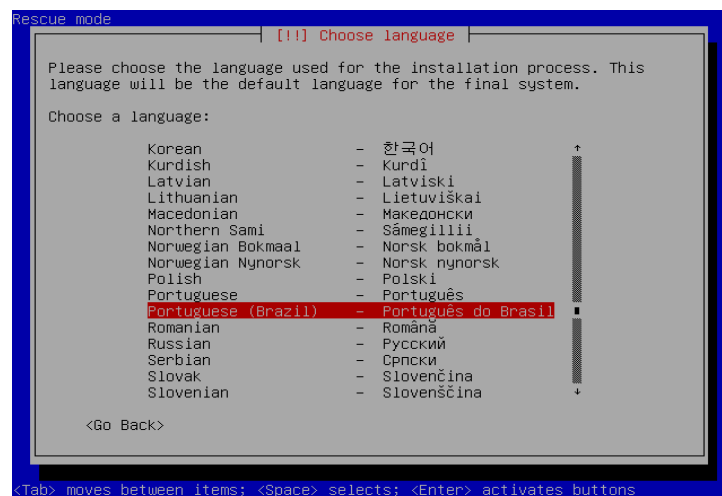
Password: *****
Failed!
Press any key to continue...
```

Para retirar a senha do Grub sera usado um recurso do próprio CD de instalação do Debian, o “Rescue Mode” que é um modo de recuperação. Vamos a prática.

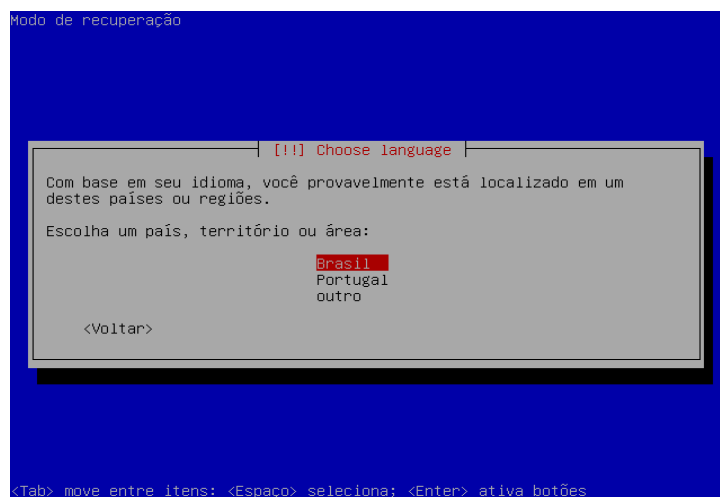
Coloque o CD de instalação do Debian Lenny e na tela inicial escolha “Advanced Options” e a opção “Rescue Mode”.



*Para continuar a recuperação escolha o idioma e tecle Enter.*

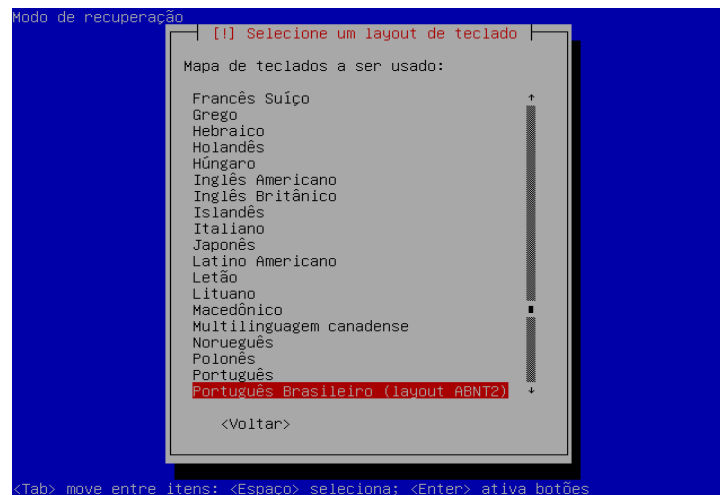


*Na próxima tela escolha o país e tecle Enter.*

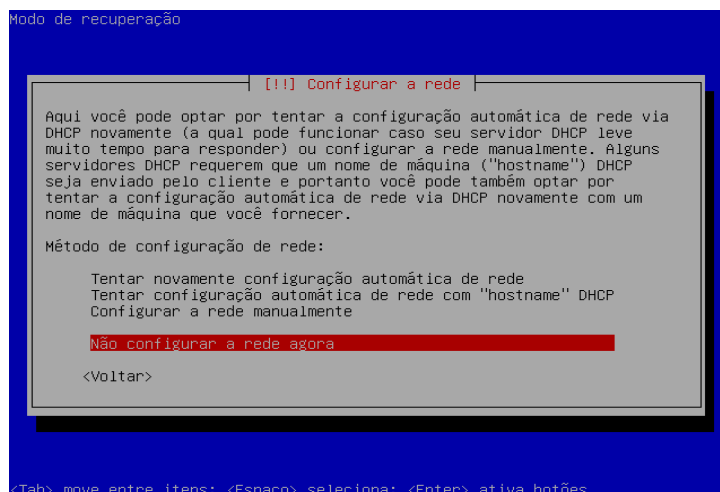
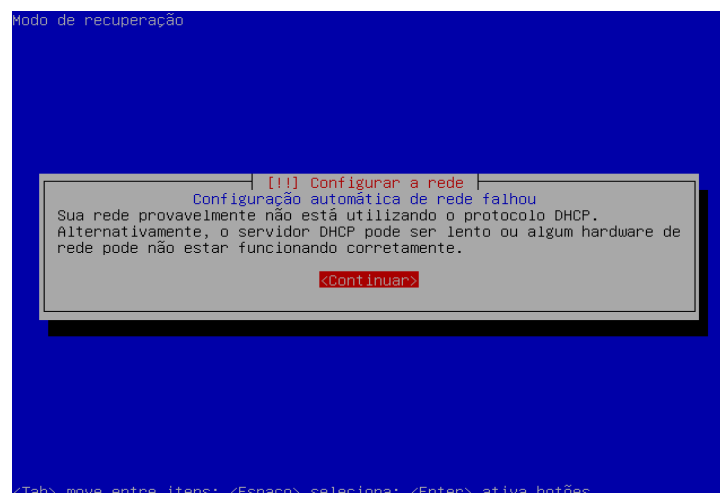


*Selecione o layout do teclado e tecle Enter para continuar.*

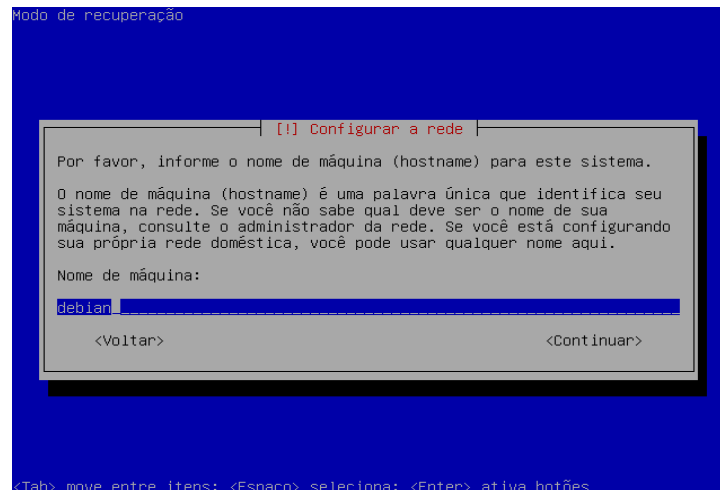




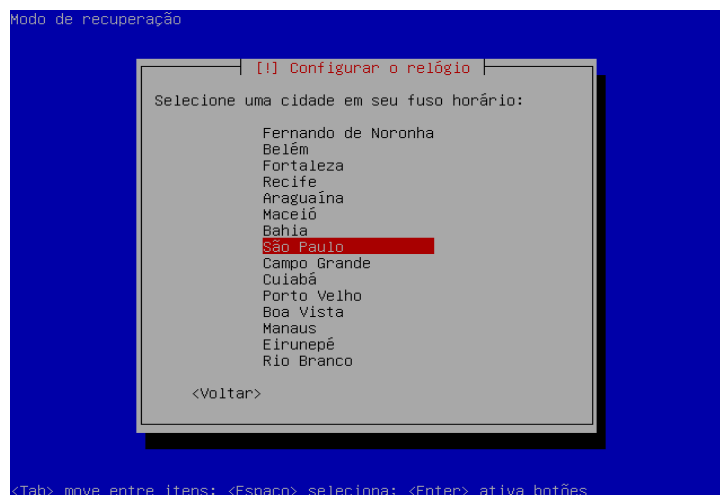
Após carregar alguns componentes básicos, será feita a configuração automática da rede via DHCP. Se você não tiver na rede um servidor DHCP, sem problemas porque esse não é o nosso foco. Use Enter e na próxima tela escolha “Não configurar a rede agora”



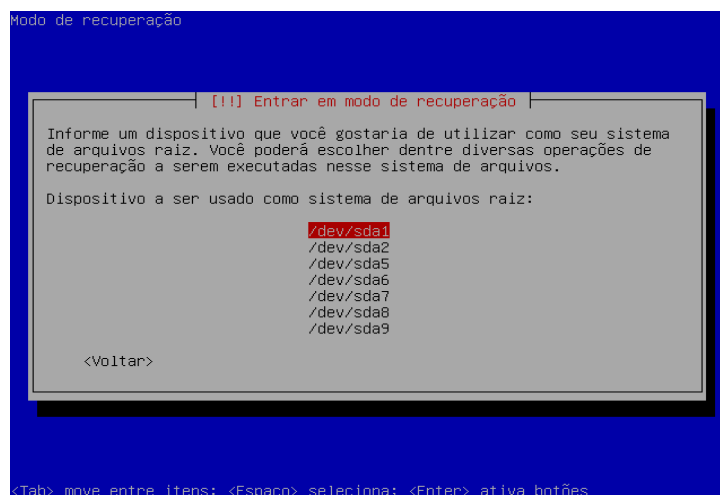
Para continuar a recuperação digite o nome da máquina e tecle Enter.



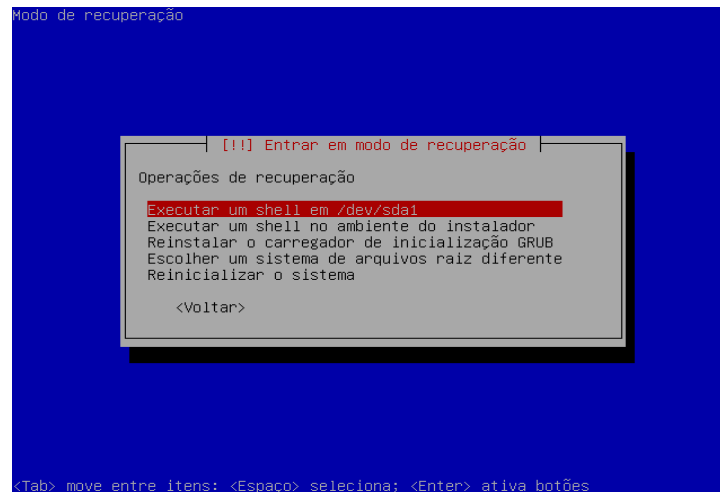
Na próxima tela selecione a sua cidade e tecle Enter para continuar.



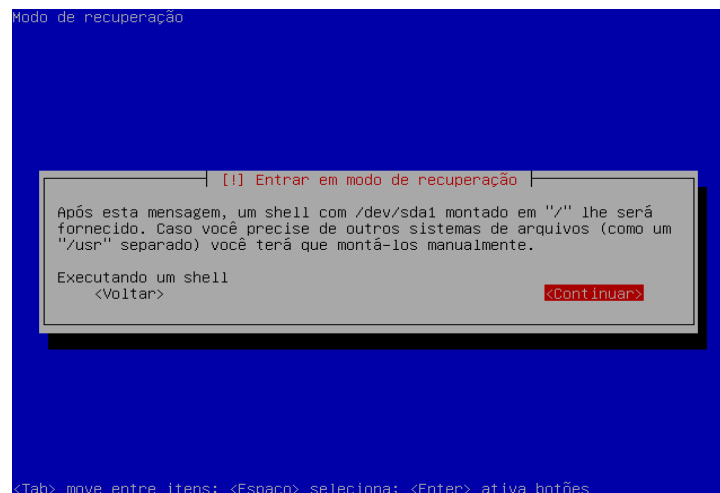
Chegou a hora mais importante do Rescue Mode!!! Selecione a partição onde a raiz ( / ) sera montada e tecle Enter.



A próxima tela exibe opções para a recuperação como por exemplo executar um shell, reinstalar o Grub, escolha outro sistema raiz e reiniciar o sistema. Selecione “Executar um shell em /dev/(depende de qual partição você escolheu)” e tecle Enter para continuar.



A próxima tela informa que a raiz ( / ) será montado na partição escolhida, e outros diretórios com o usr será preciso montado manualmente. Tecle Enter para continuar.



*Para descobrir em qual partição se encontra o usr, monta-la e assim desativar a senha do Grub. Vamos as passos:*

*Exiba o conteúdo do /etc/fstab com o comando cat:*

```
sh-3.2# cat /etc/fstab
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc defaults 0 0
/dev/sda1 / ext3 errors=remount-ro 0 1
/dev/sda9 /home ext3 defaults 0 2
/dev/sda8 /tmp ext3 defaults 0 2
/dev/sda5 /usr ext3 defaults 0 2
/dev/sda6 /var ext3 defaults 0 2
/dev/sda7 none swap sw 0 0
/dev/hdc_ /media/cdrom0 udf,iso9660 user,noauto 0 0
```

No nosso exemplo indica que o `usr` esta no `/dev/sda5`, onde pode ser montado usando o comando `mount -t ext3 /dev/sda5 /usr` ou apenas `mount /usr`



Mas porque é tão importante montar o diretório `usr`?

Comandos que serão usados na recuperação do sistema, como `passwd`, `vim`, `nano`, entre outros estão em `/usr/bin`.

Para retirar a senha do Grub você pode comentar ou apagar a linha `password -md5` no arquivo `menu.lst`, vamos a prática:

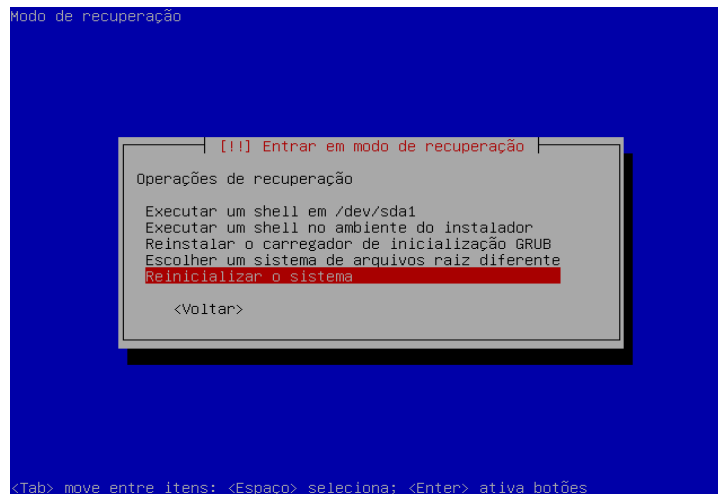
Use o comando `vim /boot/grub/menu.lst` para editar o arquivo do Grub

```
sh-3.2# vim /boot/grub/menu.lst
```

Tecla `/` e digite `password`, tecla `n` para achar a próxima palavra até encontrar “`password -md5 .....`”

```
password --md5 $1$uj5Fc/$28a8fAyuGlojzecz4/T//W.
/password
```

Use duas vezes a tecla `d` (`dd`) para apagar a linha da senha e digite `:x` para salvar e sair do `vim`. Feito isso digite `exit` para voltar a tela de opções do Rescue Mode, selecione “Reinicializar o sistema” e não esqueça de retirar o CD de instalação



### *Recuperar o Grub com Rescue Mode*

Além de mudar a senha do root, retirar a senha do Grub, é possível a recuperação do Grub. Você precisa seguir todos os passos do Rescue Mode até chegar a tela de “Operação de recuperação” e selecionar a opção “Reinstalar o carregador de inicialização Grub”

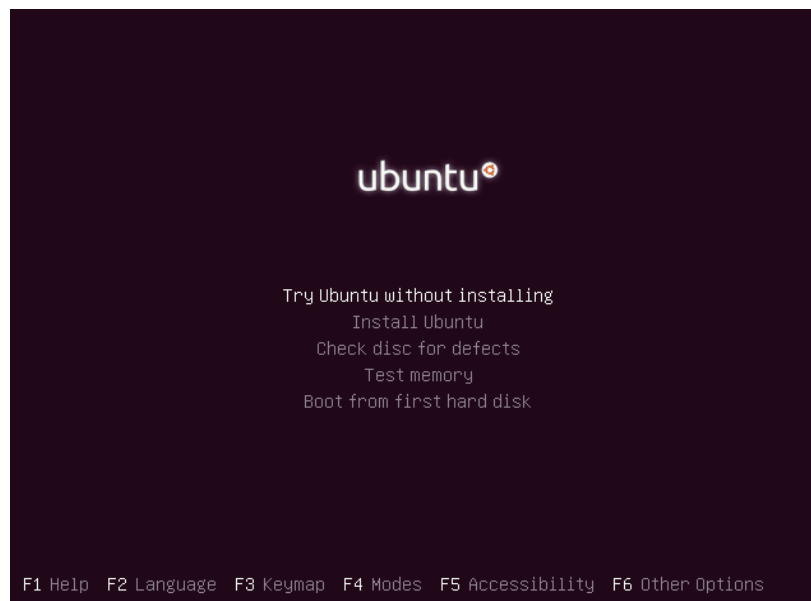
### *Manutenção do sistema com Live CD*

*A manutenção do sistema pode ser feita através de um Live CD Linux, para recuperar um sistema danificado, recuperar arquivos de HDs em máquinas Linux e Windows, fazer backup dos dados, recuperar senha do Grub, senha do root, reinstalar o Grub, entre outros.*

*A primeira etapa é conseguir um Live CD, em nosso exemplo será usado o CD do Ubuntu na versão 10.04, que pode ser baixado no site <http://www.ubuntu-br.org/download>. Clique em “Baixar Ubuntu 10.04 Desktop (i386) - Download Direto” e salve o arquivo .iso em sua máquina.*



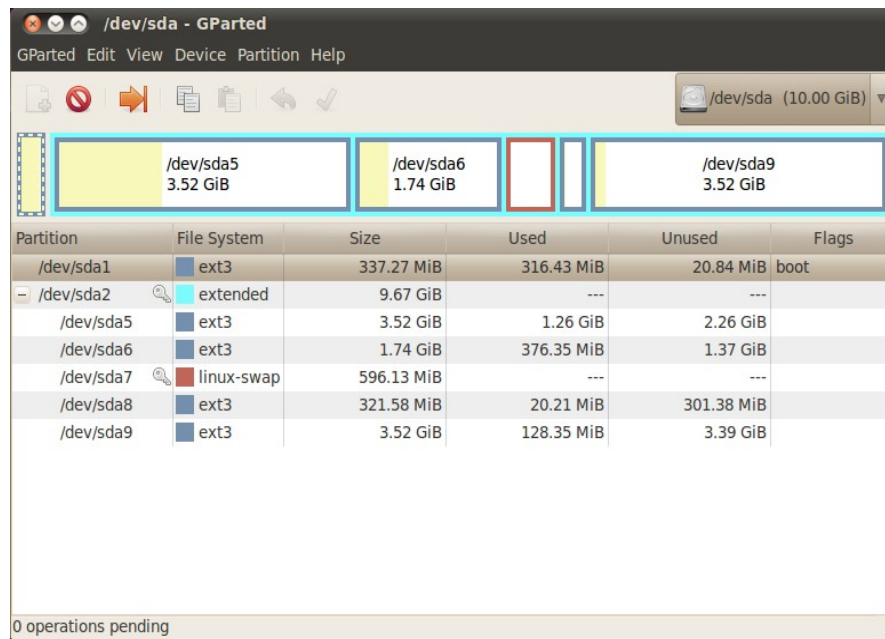
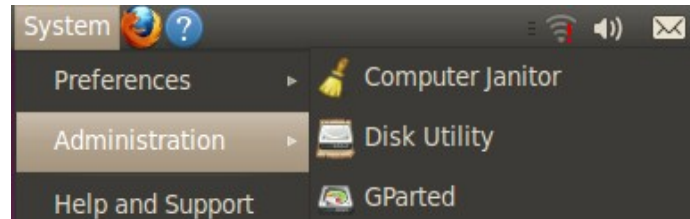
*O segundo passo é gravar a imagem do Ubuntu em um CD, colocar na máquina danificada e dar o boot. Na tela inicial do Ubuntu tecle Esc (2x) e selecione "Try Ubuntu without installing" que significa Testar o Ubuntu sem instalar.*



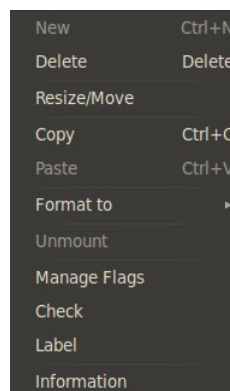
### *Particionamento de disco*

*A primeira manutenção que será feita é o particionamento de disco para criar, aumentar ou excluir partições. Na maioria dos Live Cds você pode usar o cfdisk ou fdisk, no Ubuntu é possível usar o Gparted, que é um particionador gráfico. Vamos a prática:*

Clique no menu System – Administration - Gparted

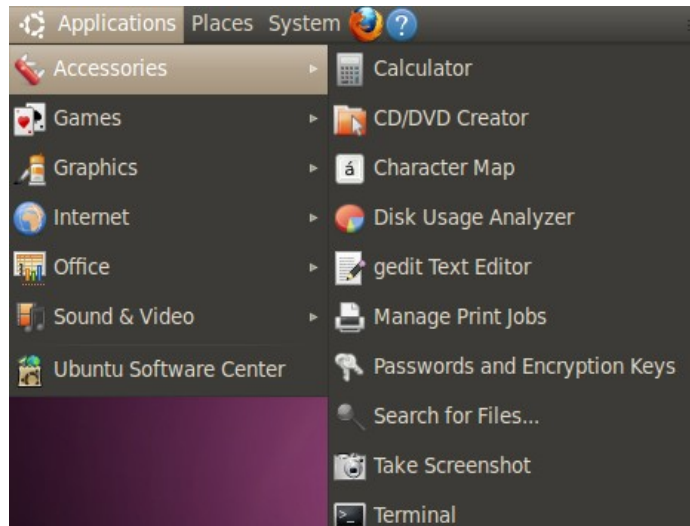


Para interagir com as partições, clique com o botão de contexto sobre uma partição na lista e escolha uma opção.



Montar a partição com chroot

A nossa próxima configuração pode ser usada em diversas situações, como por exemplo alterar a senha do root, retirar senha do Grub, fazer backup dos arquivos via ssh, entre outros. Abra o terminal no Ubuntu clicando em Applications – Accessories - Terminal



A primeira coisa que você precisa fazer é descobrir em qual partição esta a raiz do sistema que você precisa recuperar. Use o comando `sudo fdisk -l`

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	43	345366	83	Linux
/dev/sda2		44	1305	10137015	5	Extended
/dev/sda5		44	502	3686886	83	Linux
/dev/sda6		503	729	1823346	83	Linux
/dev/sda7		730	805	610438+	82	Linux swap / Solaris
/dev/sda8		806	846	329301	83	Linux
/dev/sda9		847	1305	3686886	83	Linux

No nosso exemplo a raiz esta em `/dev/sda1`. O próximo passo é criar um diretório, montar a partição raiz e no diretório criado, e montar o dev e proc. Veja o exemplo:

```
ubuntu@ubuntu:~$ sudo mkdir /mnt/sda1
ubuntu@ubuntu:~$ sudo mount /dev/sda1 /mnt/sda1
ubuntu@ubuntu:~$ sudo mount --bind /dev /mnt/sda1/dev
ubuntu@ubuntu:~$ sudo mount -t proc none /mnt/sda1/proc
```

Agora preciso deixar em chroot o `/mnt/sda1`, montar o `/usr` e `/var` e assim ter todo o sistema em funcionamento. Veja no exemplo os comandos:

```
ubuntu@ubuntu:~$ sudo chroot /mnt/sda1
root@ubuntu:/# pwd
/
root@ubuntu:/# ls /
bin    dev    initrd.img  media  proc  selinux  tmp  vmlinuz
boot  etc    lib         mnt    root  srv      usr
cdrom  home  lost+found  opt   /sbin  sys      var
```

Monte os diretórios `/usr` e `/var`



```
root@ubuntu:/# mount /usr
root@ubuntu:/# mount /var
```



*Agora você tem sistema de volta!!!*

*Dicas de comandos para ser usado.*

*dhclient* – Comando para obter um ip automaticamente e assim pode atualizar a lista de pacotes, instalar, remover programas.

*scp* – A maquina tendo acesso a rede você pode enviar arquivos de modo seguro para outra maquina. Veja um exemplo:

```
root@ubuntu:/# scp /etc/*.conf root@10.0.2.2:/root/backup
The authenticity of host '10.0.2.2 (10.0.2.2)' can't be established.
RSA key fingerprint is 41:34:12:6d:01:2f:54:91:ad:a0:0e:59:22:67:bc:1c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.2' (RSA) to the list of known hosts.
#Debian GNU/Linux 5.0
Conex\303\243o SSH
root@10.0.2.2's password:
```

*passwd* – Alterar/recuperar a senha do root. Veja um exemplo:

```
root@ubuntu:/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

*Para terminar... Depois de fazer a manutenção/recuperação digite exit e reinicie a maquina sem o Live CD.*

# Capítulo 2

## Gerenciando

### 2.1. Objetivos

- Troubleshooting: Recuperar o arquivo menu.lst deletado usando um Live CD em chroot

### 2.1. Troubleshooting



*Como eu faço para recuperar o Grub e reconstruir o arquivo menu.lst:*

O Grub usa o arquivo menu.lst para sua configuração, que é lido cada boot. Caso você apague este arquivo, veja a tela exibida no boot:

```
GNU GRUB version 0.97 (639K lower / 392128K upper memory)

[ Minimal BASH-like line editing is supported. For
the first word, TAB lists possible command
completions. Anywhere else TAB lists the possible
completions of a device/filename. ]

grub> _
```

Para recuperar o grub em modo chroot com Live CD, use o comando `grub-install /dev/sda` para instalar o Grub na MBR e `update-grub` para recriar o arquivo `menu.lst`. Veja o exemplo:

Instalar o Grub:

```
root@ubuntu:/# grub-install /dev/sda
Searching for GRUB installation directory ... found: /boot/grub
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

(hd0)    /dev/sda
```

Recriar o `menu.lst`:

```
root@ubuntu:/# update-grub
Searching for GRUB installation directory ... found: /boot/grub
Searching for default file ... found: /boot/grub/default
Testing for an existing GRUB menu.lst file ...

Generating /boot/grub/menu.lst
Searching for splash image ... none found, skipping ...
Found kernel: /boot/vmlinuz-2.6.26-2-686
Updating /boot/grub/menu.lst ... done
```