

# Resposta do Simulado RHCSA

---

1 – Para alterar a senha do root, é necessário no boot editar o grub, na linha sobre o kernel e adicionar :

**init = /bin/bash**

Após cair no Shell, alterar o o sistema de arquivo da raiz:

**mount -o remount,rw /**

E por fim alterar a senha :

**Passwd**

2 - **useradd maria; useradd João**

3 – **mkdir /publico**

4 – **touch /publico/teste.txt**

5 - **setfacl -m u:maria:r /publico/teste.txt**

**setfacl -m u:joao:rw /publico/teste.txt**

**chown root.root /publico/teste**

6 – Criar o arquivo `/etc/sysconfig/network-scripts/ifcfg-eth1`, com o seguinte conteúdo:

**DEV=eth1**

**ONBOOT=Yes**

**BOOTPROTO=static**

**IPADDR=192.100.0.1**

**NETMASK=255.255.255.0**

Após criar , reiniciar o service de rede:

**service network restart**

6 – A principio parece ser um simples yum install. Mas é uma típica pegadinha da prova, pois só a instalação não garante que ele vai funcionar no próximo boot. Então primeiramente , instalar e configurar para iniciar no boot:

**yum install httpd**

**service httpd start**

**chkconfig httpd on**

O proximo passo é configurar o firewall , o desabilita-lo. Vamos ver primeiramente como desabilitar:

**service iptables stop**

**chkconfig iptables off**

No caso de inserir regras seria da seguinte forma:

**iptables -A INPUT -p tcp --dport 80 -j ACCEPT**

**service iptables save**

7 - Nesta questão, apesar de parecer bem simples, também é uma pegadinha. Não basta copiar somente o arquivo, tem que colocar no contexto, ou verificar o contexto do SeLinux, para que funcione perfeitamente. Então existe duas opções, desabilitar o SeLinux, ou verificar e alterar se for o caso o contexto do Selinux.

No primeiro exemplo vamos desabilitar , após copiar.

**cp /root/arquivo.html /var/www/HTML**

Editar o arquivo /etc/selinux/config e alterar a linha, deixando como a abaixo:

SELINUX=disabled ou SELINUX=permissive (Está opção só será validade, após boot, para efeito imediato , mas não permanente, execute **setenforce=0**)

No segundo caso, alterar o contexto do arquivo HTML:

**#cd /var/www/HTML**

**#ll -Zd**

drwxr-xr-x. root root system\_u:object\_r:httpd\_sys\_content\_t:s0

```
semanage fcontext -a -t httpd_sys_content_t /var/www/html/arquivo.html
```

Mas o grande teste, mesmo sem alterar o contexto, é abrir a página WEB no endereço IP configurado na interface eth0 ou eth1.

8 – Novamente não se trata apenas de instalar e sim de habilitar no boot e permitir no firewall.

```
yum install vsftpd
```

```
service vsftpd start
```

```
chkconfig vsftpd on
```

E caso o firewall esteja iniciado:

```
iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT
```

```
service iptables save
```

10 – Neste caso trata-se de um volume lógico, LVM, para tanto devemos usar os comandos **lvresize** ou **lvextend**, seguidos do **e2fsck**, **resize2fs**:

```
lvextend -L 2G /dev/mapper/vg_redhat-LogVol2
```

```
e2fsck -f /dev/mapper/vg_redhat-LogVol2
```

```
resize2fs dev/mapper/vg_redhat-LogVol2
```

11 – A maneira mais simples para fazer essa configuração é rodando o comando **authconfig-tui**, no modo texto e **system-config-authentication**. Seria necessário instalar os pacotes **authconfig**, **authconfig-gtk**.

**Via system-config-authentication**

**Configuração da autenticação** [X]

Identidade & Autenticação Opções Avançadas:

**Configuração de Conta de Usuário**

Banco de Dados da Conta de Usuário: LDAP

DN base para pesquisa LDAP: dc=dominiostato,dc=net

Servidor\_LDAP: ldaps://192.168.100.2

Utilizar TLS para criptografar conexões

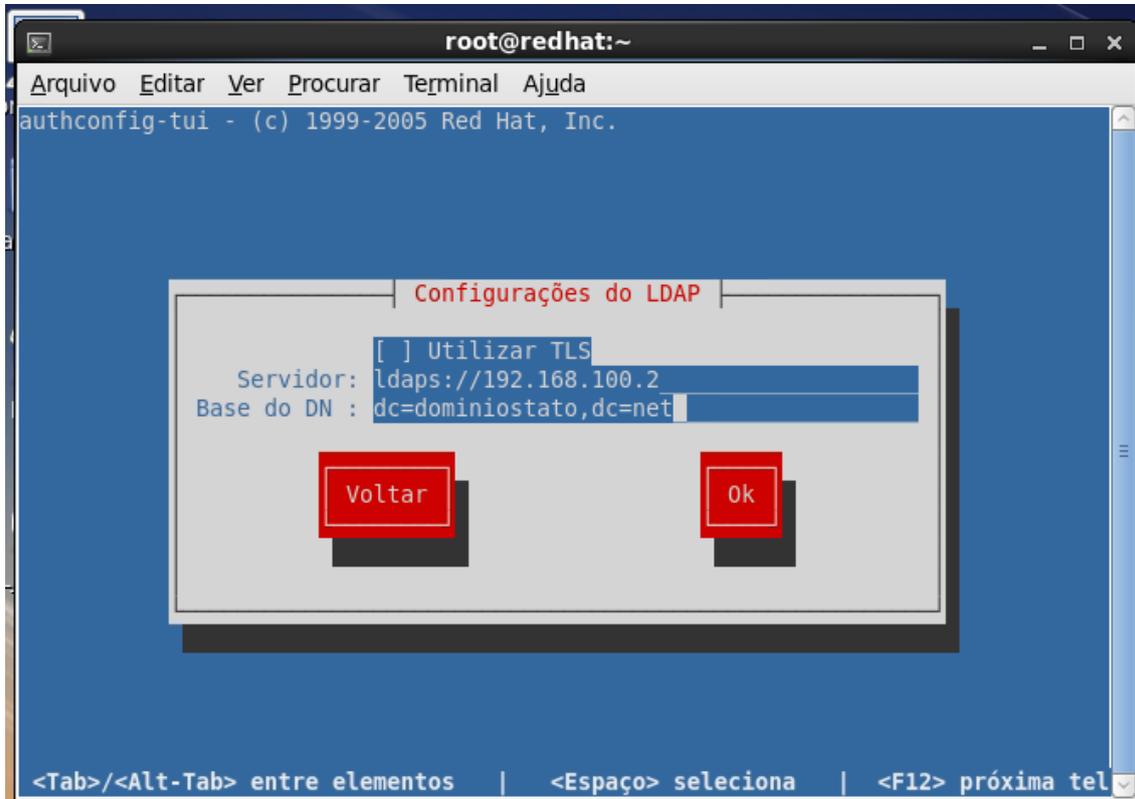
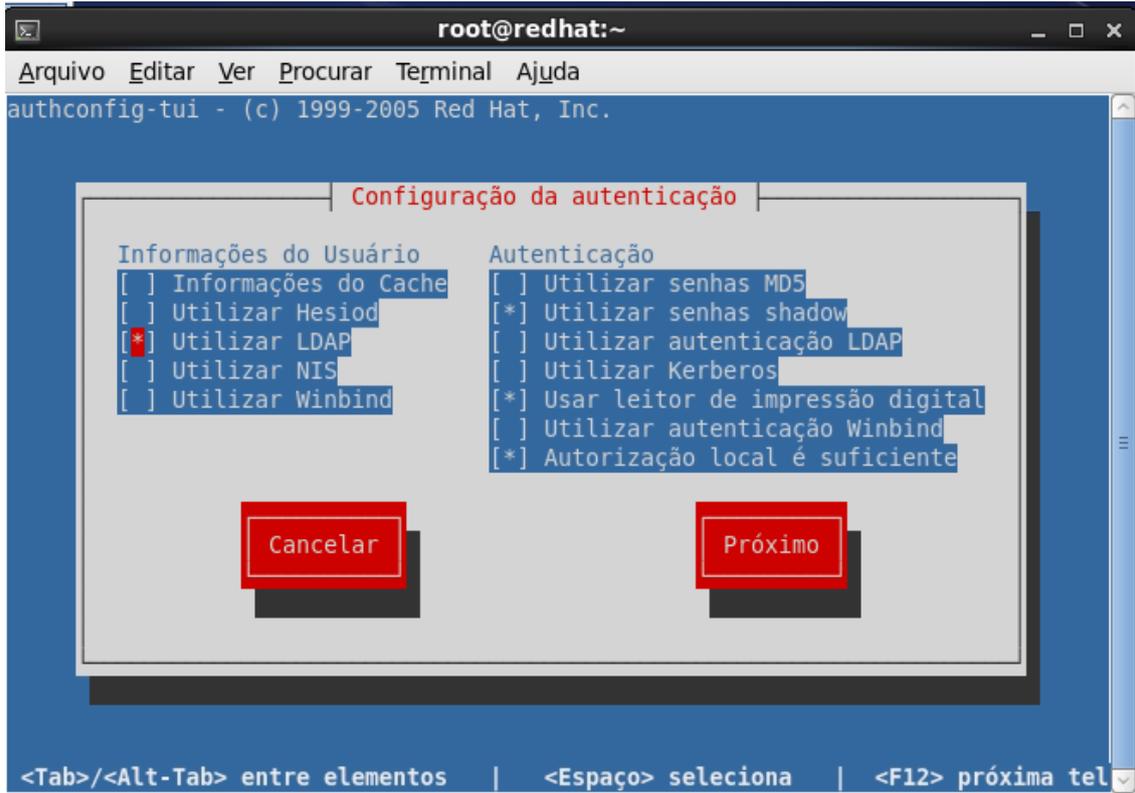


**Configuração da autenticação**

Método de Autenticação: Senha LDAP

Reverter Cancelar Aplicar

Via authconfig-gtk:



12 – A primeira coisa a ser feita é editar o arquivo auto.master, e adicionar a seguinte linha:

**auto.user**                    **/diretório**

Já o arquivo auto.user não existe, dessa forma deverá ser criado com a seguinte informação:

**joao**                            **192.168.100.1:/home/joao**

**maria**                           **192.168.100.1:/home/maria**

13 – Nesse caso deverá ser adicionado um arquivo em /etc/yum.repos.d. O nome é indiferente, sendo que a extensão deverá ser .repo. O seu conteúdo deverá ter toda estrutura, mas a linha que faz referencia para o servidor, deverá estar como abaixo:

baseurl=http://200.0.0.1

14 – Deverá ser incluído a entrada no lvm, que é o dispositivo /dev/mapper/vg\_redhat-lv\_root.

Para tanto execute o comando :

**blkid /dev/mapper/vg\_redhat-lv\_root**

```
[root@redhat ~]# blkid /dev/mapper/vg_redhat-LogVol02
/dev/mapper/vg_redhat-LogVol02: UUID="af710d5a-6345-4969-8acf-98c987ccee9a" TYPE
="ext4"
```

Esse será o retorno que deverá ser adicionado em fstab:

UUID=af710d5-6345-4969-8acf-98c987ccee9a /usr/local ext4 defaults 1 2

15 – Executar o comando **free -m** e enviar a resposta para /root/memória.txt

**free -m >/root/memoria.txt**