

Tutorial samba como controlador de domínio para Ubuntu ou Debian.

Os procedimentos foram testados no ubuntu 10.04, em caso do debian ou outra versão pode mudar alguns detalhes ou algum procedimento como scripts podem não funcionar.

1. Saber instalar debian Linux.
 - a. Em caso de duvidas assista o vídeo instalação do Linux debian
 - i. Link 1= [Instalação sem interface grafica](#)
 - ii. Link 2=[Instalação com interface gráfica.](#)
2. Ter uma maquina virtual Linux para praticar as atividades listadas abaixo.
 - a. Caso não tenha uma maquina virtual debian.
 - i. [Parte1](#),[Parte2](#), [Parte3](#), [Parte4](#), [Parte5](#), [Parte6](#)
 - ii. Login= root, senha= 123456
 - iii. Baixe o vmware player ou virtual box gratuitamente na internet.
3. Ter conhecimentos básicos sobre configuração de redes no debian
 - Em caso de duvidas assista o vídeo
 - a. Link = [Clique aqui](#)
4. Ter conhecimentos básicos do samba3 no debian
 - Em caso de duvidas assista o vídeo
Link = [Clique aqui](#)

Obs. Depois de ter assistido aos vídeos e ter revisado os assuntos preparatórios para esse tutorial, vamos por a mão na massa e configurar o samba 3 como controlador de domínio.

O que é e o que faz o samba?

Em uma pequena rede, manter as senhas dos usuários sincronizadas entre as estações Windows e o servidor Samba não chega a ser um grande problema. No entanto, em redes de maior porte, isso pode se tornar uma grande dor de cabeça e passar a consumir uma boa parte do seu tempo.

Para solucionar o problema, existe a opção de usar o servidor Samba como um controlador primário de domínio (PDC), onde ele passa a funcionar como um servidor de autenticação para os clientes Windows e (opcionalmente) armazena os perfis de cada usuário, permitindo que eles tenham acesso a seus arquivos e configurações a partir de qualquer máquina onde façam logon.

Resumo das atividades

Atividade 1 - Verificar configurações de rede.

Comandos: ping, ifconfig

Verificar as configurações da rede e a conectividade com os clientes via protocolo ip.

Atividade 2 – Instalação do samba.

Instalar o samba no ubuntu.

Atividade 3 - Alterar o arquivo de configuração do samba.

1. Criar a seção global tornando o samba um controlador de domínio.
2. Criar o perfil movel do usuários.
3. Criar o compartilhamento netlogon
4. Criar o compartilhamento homes
5. Criar o compartilhamento profiles

Atividade 4 - Pastas que precisam ser criadas.

1. Netlogon /var/samba/netlogon
2. Profiles /var/profiles

Obs. Caso você queira, crie umas pasta em mnt para ser compartilhada na rede.

Mas lembre-se de delegar permissões e não se esqueça de criar o compartilhamento no smb.conf

Atividade 5 - Usuários que precisam ser criados

Root do samba

Maquina do sistema(xpcliente\$)

Maquina do samba(xpcliente)

Usuário para acesso a rede do sistema(maria)

Usuário para acesso a rede do samba(maria)

Parte 1 - Instalação do samba.

Instalação

Verificando pacotes atualizados disponíveis

```
# apt-get update
```

Instalando pacote samba

```
#apt-get install
```

Assista o video configuração de compartilhamento no samba.

Parte 2 - Verificando as configurações de rede do samba.

O comando ifconfig permite que você verifique o ip do servidor Linux.

Anota o ip do servidor Linux para teste de conectividade.

No Windows XP ou cliente da sua rede, clique em iniciar > executar > cmd

No prompt digite ping ipdoservidorlinux ou ping nomenetbiosdoservidoresamba.

Eu aconselho que as placas de rede do Linux tenha ip fixo, mas com ip dinâmico funciona perfeitamente.

Assista ao vídeo configurações de rede no debian Linux, [link aqui](#).

Parte 3 - Configuração do smb.conf

```
#####smb.conf comentado#####
```

```
### inicio da sessão global ###
```

```
### Esse script foi testado no ubuntu 10.04###
```

```
[global]
#Nome do domínio ou grupo de trabalho
  workgroup = santiago.com
#Nome que será visível na rede
  netbios name = servidorubuntu
#Nome e comentário do servidor na rede
  server string = Samba PDC
#Definição como controlador de domínio sim/não
  domain master = Yes
#Primeiro servidor a responder na rede
  preferred master = yes
  local master = yes
#Login no dominio
  domain logons = Yes
##Descomente a linha abaixo para add usuário maquina automaticamente
##essa linha foi testada e não funcionou no debian##
  #add machine script = /usr/sbin/useradd -s /bin/false -d /var/lib/nobody %u

##Descomenta a linha abaixo para inserir usuário maq no samba automaticamente
##essa linha foi testada e não funcionou no debian##
  #add user script = /usr/sbin/adduser --quiet --disabled-password --gecos ""%u

#essa linha indica que os usuarios vão utilizar script de logon
```

```

#muito utilizado para mapeamentos e etc
    logon script = netlogon.bat
# essas linhas abaixo vamos criar um perfil
#%L indica o nome do servidor, %U o nome do usuário que fez o logon
#e mapeia o usuário # \\nomeservidor\profiles\usuario
    logon home = \\%L\%U\.profiles
#essa linha abaixo mapeia \\nomeservidor\profiles\usuario
    logon path = \\%L\profiles\%U
#exige autenticação para acesso ao domínio e compartilhamentos
    security = user
#Aa senhas serão criptografadas
    encrypt passwords = yes
#Quanto maior for o valor, maior será o servidor na rede
    os level = 100

## Definição de pastas e compartilhamentos ##

[netlogon]
##comentário da pasta
    comment = Serviço de logon
##caminho da pasta
    path = /var/samba/netlogon
##Visível na rede
    guest ok = yes
##Não acessível via browser
    browseable = no

[homes]
    comment = directorio home
##Valido apenas para usuarios cadastrados
    valid users = %S
##visível na rede
    guest ok = yes
## Não acessível via browser
    browseable = no

[profiles]
## Caminho da pasta
    path = /var/profiles
## Gravavel
    writeable = yes
## Não acessível via browser
    browseable = no
## Permissão apenas para o dono
    create mask = 0600
##Permissão apenas para o dono
    directory mask = 0700

```

testar se o samba este configurado como PDC.

Depois de configurar o samba precisamos testar.

#testparm

Ao configurar o Samba como PDC, ele deve exibir a mensagem: "Server role: ROLE_DOMAIN_PDC".

Caso necessário, use o comando "**smbpasswd -a root**" para cadastrar o root.

Parte 4 - Criar a pasta netlogon que é a nossa pasta profile.

para criar a pasta "/var/samba/netlogon" e configurar corretamente as permissões:

```
# mkdir -p /var/samba/netlogon
# chmod 775 /var/samba/netlogon
```

Parte 5 - Criando a pasta var profiles para salvar o perfil móvel dos usuários.

Crie a pasta "/var/profiles", com permissão de escrita para todos os usuários:

```
Criando a pasta
# mkdir /var/profiles
```

```
Alterando as permissões da pasta.
# chmod 1777 /var/profiles
```

Parte 6 - Cadastrar os usuários no sistema.

Cadastre agora os logins dos usuários, com as senhas que eles utilizarão para fazer login a partir das máquinas Windows.

```
# adduser João
```

Parte 7 - Cadastrar os usuários no samba.

```
# smbpasswd -a João
```

Parte 8 - Cadastrando as máquinas no sistema e no samba.

Para logar no domínio os computadores precisam estar cadastrados no sistema como máquinas, usuários máquina bloqueados e sem senha.

Lembre-se que você pode descomentar a linha descrita abaixo no smb.

```
#add user script = /usr/sbin/adduuser --quiet --disabled-password --gecos ""%u
```

Você pode adicionar como descrito abaixo ou descomentar essa linha no smb.conf que deixe de exemplo.

Criando o grupo máquinas.

Se preferir, você pode adicionar as contas de máquina dentro de um grupo do sistema ("máquinas" ou "machines" por exemplo).

```
#groupadd máquinas
```

Agora adicione o usuário máquina dentro do grupo máquinas(veja que quando criamos usuário máquina usamos o \$ no final do nome do usuário).

Criando usuários e adicionando ao grupo maquinas.

```
# useradd -g maquinas -d /dev/null -s /bin/false athenas$
```

Limpando a senha do usuário maquina do sistema.

```
# passwd -l athenas$
```

Cadastrando usuário maquina no samba como maquina (-a -m)

```
# smbpasswd -a -m athenas
```

Obs. Se quiser descomentar a linha abaixo no smb o samba adiciona a maquina no samba automaticamente
#add machine script = /usr/sbin/useradd -s /bin/false -d /usr/lib/nobody %u

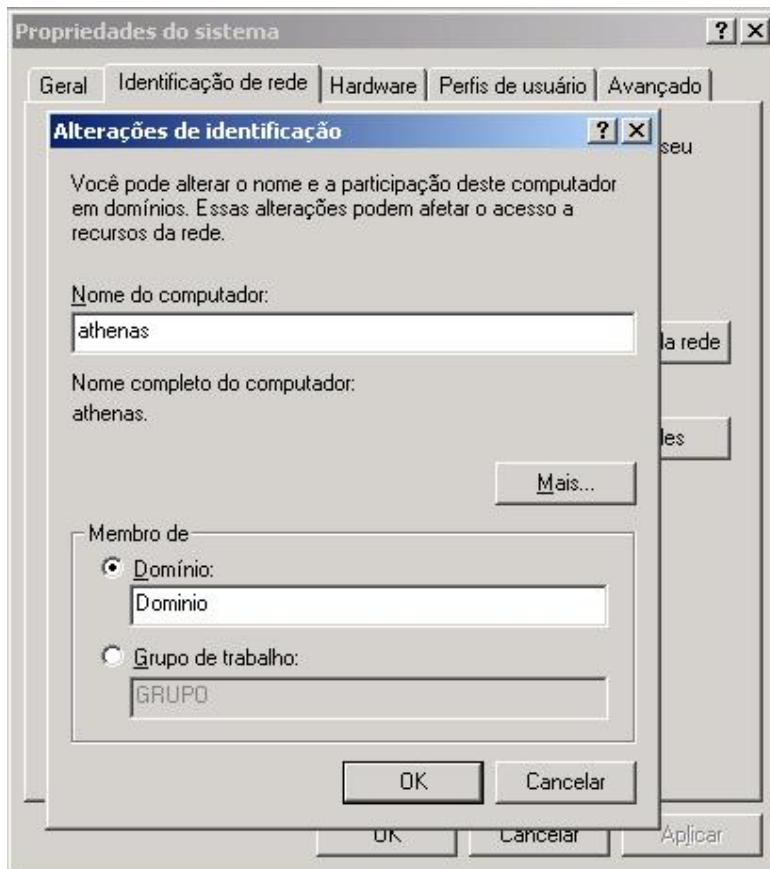
O gran-finali seria inserir os pcs clients no dominio.

Logando Clientes Windows

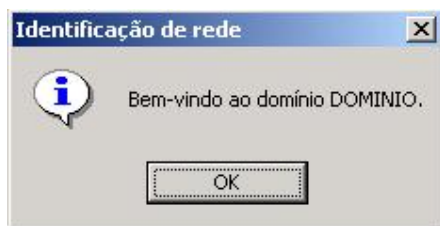
Neste ponto a configuração do servidor Samba está pronta. Falta apenas configurar os [clientes](#) Windows para efetuarem logon no domínio.

Nem todas as versões do Windows suportam este recurso. Como controladores de domínio são usados principalmente em redes de médio ou grande porte em [empresas](#), a Microsoft não inclui suporte no Windows XP Home e no XP Starter (também chamado jocosamente de "Miserable Edition"), de forma a pressionar as empresas a comprarem o XP Professional, que é mais caro.

A configuração muda de acordo com a versão do Windows: No Windows 2000, acesse o "Meu [Computador](#) > Propriedades > Identificação de rede > Propriedades". Coloque aqui o nome do computador (que precisa ser um dos logins de máquinas adicionados na configuração do Samba) e o nome do Domínio, que é definido na opção "workgroup =" do smb.conf. Para ter acesso a esta opção você deve estar logado como administrador.



Na tela de identificação que será aberta a seguir, logue-se como "root", com a senha definida no Samba. É normal que a [conexão](#) inicial demore dois ou três minutos. Se tudo der certo, você é saudado com uma mensagem "Bem-vindo ao domínio DOMINIO".



É necessário identificar-se como root ao fazer a configuração inicial, para que seja criada a relação de confiança entre o servidor e o cliente. A partir daí aparece a opção opção "Efetuar logon em: DOMINIO" na tela de login, permitindo que o usuário faça logon usando qualquer uma das contas cadastradas no servidor. Continua disponível também a opção de fazer um login local.

No Windows 98 ou ME: Comece logando-se na rede (na tela de login aberta na inicialização) com o mesmo usuário e senha que será usado para fazer logon no domínio. Acesse agora o "Painel de Controle > Redes > Cliente para redes Microsoft > Propriedades". Marque a opção "Efetuar Logon num domínio NT", informe o nome do domínio e marque a opção "Efetuar logon e restaurar conexões". Ao terminar, é preciso fornecer o CD de instalação e reiniciar a máquina.

Note que as máquinas com o Windows 98/ME não são compatíveis com todos os recursos do domínio, elas acessam o domínio dentro de uma espécie de modo de compatibilidade, onde podem acessar os compartilhamentos, mas não têm acesso ao recurso de perfis móveis, por exemplo.

No Windows XP Professional o procedimento varia de acordo com a versão do Samba usada. Se você está usando uma versão recente do Samba, da versão 3.0 em diante, a configuração é bem mais simples, basta seguir os mesmos passos da configuração no Windows 2000.

Se por outro lado você ainda está usando o Samba 2.x, a configuração é um pouco mais complicada. Comece copiando o arquivo "/usr/share/doc/samba-doc/registry/WinXP_SignOrSeal.reg" (do servidor), que fica disponível ao instalar o pacote "samba-doc". Esta é uma chave de registro que precisa ser instalada no cliente.

Acesse agora as propriedades do "Meu Computador" e na aba "Nome do Computador" clique no botão "ID de rede". Será aberto um Wizard que coleta o nome do domínio, nome da máquina e login de usuário. Lembre-se que é necessário efetuar o primeiro logon como root.

Se não der certo da primeira vez, acesse o "Painel de controle > Ferramentas administrativas > Diretiva de segurança local > Diretivas locais > Opções de segurança" e desative as seguintes opções:

- Membro do domínio: criptografar ou assinar digitalmente os dados de canal seguro (sempre)
- Membro do domínio: desativar alterações de senha de conta da máquina
- Membro do domínio: requer uma chave de sessão de alta segurança (Windows 2000 ou posterior)

Para confirmar se os clientes estão realmente efetuando logon no servidor, use o comando "smbstatus" (no servidor). Ele retorna uma lista dos usuários e máquina logadas.

**Depois de criar esse servidor com domíno super básico vc já etara pronto para montar servidores mais complexos com mais recursos.
Veja esse exemplo de smb.conf**

<http://www.guiadohardware.net/dicas/lixeria-samba.html> ou esse logo abaixo.

Nessa conf teremos uma boa ideia de como funciona o Samba atuando como controlador de domínio primário em uma rede corporativa. Em uma rede acima de 10 máquinas, já aconselho utilizar um controlador de domínio com perfil móvel para maior facilidade de administração dos usuários.

Mostrarei como configurar um controlador de domínio de maneira simples e com lixeira de arquivos, fazendo a recuperação dos arquivos delatados ser mais ágil. Nosso arquivo de configuração terá além de lixeira e exclusões de arquivos tmp, grupos e níveis de acessos. Tudo bem comentado para melhor entendimento.

Nesta conf vou explicar apenas do smb.conf, pois é o arquivo de configuração principal do Samba, nos compartilhamentos dá para entender legal onde ficam os arquivos que guardarão os perfis, homes, .recycle e compartilhamentos acessados.

[global]

Nome do domínio e Grupo o mesmo será para as estações..


```

workgroup = Meu-dominio
## Forma que será visível na rede
netbios name = SPBRFS01
## Nome e comentário do servidor na rede
server string = SPBRFS01 SAMBA
wins support = yes
## servidor responde por Dns tbm no nosso caso não
dns proxy = no
## hora ajustável do serve
time server = yes
## Conf padrão
name resolve order = lmhosts host wins bcst
## Ip do maquina onde funcionará o serve
interfaces = 127.0.0.0/8 192.168.1.12
## Visibilidade na rede Sim
bind interfaces only = yes
## arquivo de log padrão
log file = /var/log/samba/log.%m
## Tamanho Maximo a gravar log
max log size = 5120
## ver os log nos clientes não
syslog only = no
## Nivel do log
syslog = 0
## arquivo padrão do samba
panic action = /usr/share/samba/panic-action %d
## criptografando a senha do usuário
encrypt passwords = true
## Padrão do samba
passdb backend = tdbsam
## restringir usuários por acessos
obey pam restrictions = yes
## fazer requisição de password nos acessos de compartilhamento
unix password sync = yes
## Local onde buscara as senhas
passwd program = /usr/bin/passwd %u
## padrão do samba
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retye\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
## padrão do samba aconselhável para PDC
password level = 8
## padrão do samba aconselhável para PDC
username level = 16
## forçar autenticação
pam password change = yes
## aqui decide se é controlador de domínio ou não
domain logons = yes
## busca dos profiles que cada usuário terá
logon path = \\%L\profiles\%U
## aqui determinamos os mapeamentos via .BAT
logon script = %U.bat
## add usuarios no samba
add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u
## add maquinas cliente no samba.
add machine script = /usr/sbin/useradd -g machines -c "%u machine account" -d /dev/null -s /bin/false %u
add group script = /usr/sbin/addgroup --force-badname %g
add user to group script = /usr/sbin/adduser %u %g
delete user script = /usr/sbin/userdel %u
delete group script = /usr/sbin/groupdel %g
delete user from group script = /usr/sbin/deluser %u %g
set primary group script = /usr/sbin/usermod -g %g %u
load printers = no
## não será servidor e impressão
#printing = cups
#printcap name = cups
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
## primeiro servidor a responder na rede
## seguir essas conf. até o hosts
preferred master = yes
local master = yes
domain master = yes
os level = 255
log level = 2
unix charset = iso8859-1
display charset = cp850
max mux = 100
max open files = 100000
kernel oplocks = no
oplocks = no
remote announce = 192.168.1.255
## broadcast da sua rede
remote browse sync = 192.168.1.255
## Range de ip da rede no meu caso local, rede interna e VPN
hosts allow = 127., 192.168.1.,192.168.3.
block size = 4096
level2 oplocks = no

## aqui irei bloquear arquivos com essas extensões na minha rede
veto files = /*.mp3/*.*.wmv/*.*.wma/*.*.ogg/*.*.mpeg/*.*.mpg

```

```

## Criação da auditoria do meu Samba..
vfs objects = full_audit
full_audit:success = write, unlink, rename, mkdir, rmdir, chmod, chown
full_audit:failure = write, unlink, rename, mkdir, rmdir, chmod, chown
full_audit:prefix = %u|%i|%S

## criação da minha lixeira da rede
vfs objects = recycle
recycle:versions = yes
recycle:touch = yes
recycle:keeptree = yes
recycle:exclude = *.tmp *.temp *.o *.obj ~$*
recycle:exclude_dir = tmp, cache

#===== Share Definitions =====

[homes]
comment = Home escolher o nome que quiser apenas comentário
browseable = no // acessar via browser NÃO
read only = no // visível na rede NÃO
create mask = 0700 // Total apenas para o dono
directory mask = 0700 // Total apenas para o dono
valid users = %S // valido somente para o usuário
vfs objects = recycle, full_audit // aqui chamo a auditoria
recycle:repository = .recycle // aqui chamo a lixeira

[netlogon]
comment = Network Logon Service
path = /home/samba/netlogon /Criar a pasta onde ficará os netlogon
guest ok = yes
read only = yes
share modes = no

[profiles]
comment = Users profiles // Comentário
path = /home/samba/profiles // pasta do profile CRIAR
read only = no // NÃO visível
guest ok = no // NÃO visível
browseable = no // NÃO acessível via browser
create mask = 0600 // Permissão apenas para o dono
directory mask = 0700 // Permissão apenas para o dono

[geral]
comment = Area de transferencia
path = /home/Meu-dominio/misc/gera // Comentário
read only = no
guest only = yes // Visível na rede
guest ok = yes // Todos
force create mode = 0755 // Permissão vale para todos
force directory mode = 0755 // Permissão vale para todos
vfs objects = recycle, full_audit // auditoria e lixeira
recycle:maxsize = 524288000 // tamanho da lixeira nesse compartilhamento.
recycle:repository = .recycle

[sistemas]
comment = Sistemas interno
path = /home/Meu-dominio/systems/sistemas
read only = no
force create mode = 0777
force directory mode = 0777
guest only = yes
guest ok = yes
default case = upper
delete readonly = yes
vfs objects = recycle, full_audit
recycle:maxsize = 524288000
recycle:repository = .recycle

[suporte]
comment = Suporte - Directorio do TI
path = /home/Meu-dominio/ti/suporte
valid users = @grif_suporte // acesso somente a usuários adicionada no grupo grif_suporte
write list = @grif_suporte // somente que faz parte da lista grif_suporte
read only = no
force create mode = 0777 // Permissão total para o dono, grupo e usuários
force directory mode = 0777 // Permissão total para o dono, grupo e usuários
vfs objects = recycle, full_audit // auditoria e lixeira
recycle:maxsize = 209715200
recycle:repository = .recycle

[controle]
comment = Controle de qualidade
path = /home/Meu-dominio/department/cq/controle
valid users = @grif_cq // Recapitulando
write list = @grif_cq // acesso somente para o grupo grif_cq

```

```
read only = no
force create mode = 0777 // Permissão total para o dono, grupo e usuários
force directory mode = 0777 // Permissão total para o dono, grupo e usuários
vfs objects = recycle, full_audit // arquivo de auditoria e lixeira
recycle:maxlength = 209715200 // tamanho Maximo lixeira
recycle:repository = .recycle // nome da lixeira
```

[orcamento]

```
comment = Orcamentos // Comentário
path = /home/Meu-dominio/department/orc // Criar pasta
valid users = @grif_orc // Somente
write list = @grif_orc // Somente
read only = no
force create mode = 0777 // Permissão total para o dono, grupo e usuários
force directory mode = 0777 // Permissão total para o dono, grupo e usuários
vfs objects = recycle, full_audit // auditoria e lixeira
recycle:maxlength = 209715200 // tamanho Maximo
recycle:repository = .recycle // nome da lixeira
```

Após essas conf. restart o samba

```
/etc/init.d/samba restart em Debian e Ubuntu
/etc/usr/local/etc/samba restart Derivações Bsd
```

Vale lembrar que o arquivo de configuração do samba é igual para todos os outros, após concluir a conf do samba, aconselhável nas máquinas clientes configurar em opções de pastas para não visualizar pastas ocultas, sendo assim os usuários não verão a lixeira estando legível apenas para o administrador da rede.

Não se esqueça de verificar tudo quando terminar em busca de erros.
Assista meus vídeos no canal wilfilmes do youtube.

Abraços e até a próxima.