

Home (/index.php) / Artigos (/artigos/index.php) / Linux (/artigos/categoria/index.php?codigo=1) / Samba (/artigos/verSubCategoria.php?codigo=99) / Compartilhamento do Samba autenticando no AD

## Compartilhamento do Samba autenticando no AD



(/~tiago2001)

tiago2001 (/~tiago2001)

Este artigo é destinado àqueles que ainda utilizam o Windows 2003 como PDC e querem utilizar o Samba como servidor de arquivos, porém querem utilizar os usuários que já estão cadastrados no AD, dessa forma quando o usuário logar, terá acesso aos compartilhamentos que você o habilitou para ele sem a necessidade de digitar a senha novamente.

Por: Tiago Prado em 28/03/2011

[ Hits: 78.139 ]



⚠ Denuncie (/denuncie/index.php) ➕ Favoritos (/addBookmark.php?tipo=artigo&codigo=12453) ✉ Indicar (/formIndicar.php?tipo=artigo&codigo=12453) 🖨 Impressora (/artigos/impressora.php?codigo=12453)



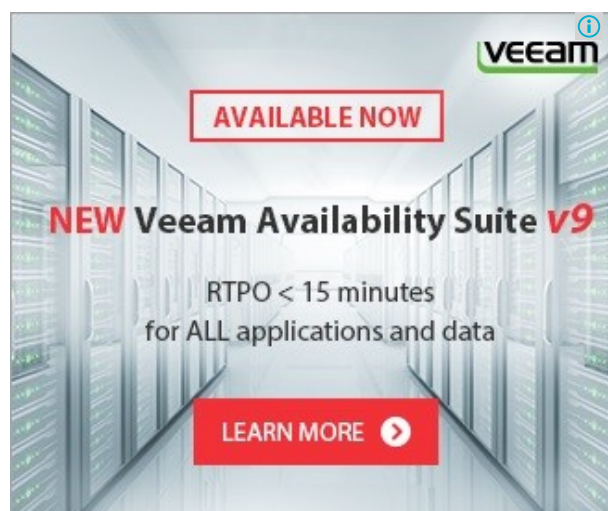
### INGRESSANDO NO DOMÍNIO

Antes de ingressar no domínio é importante sincronizar o horário do seu Debian com o controlador de domínio (Windows 2003), para isso digite:

```
# ntpdate 192.168.1.3
```

Tente ingressar no domínio com o seguinte comando:

```
# net ads join -U administrador
```



Para que tudo esteja correto, deve aparecer a mensagem abaixo:

```
Using short domain name -- INTRAGOV
Joined 'ARQUIVOS' to realm 'intragov.com'
```

Obs.: administrador é o administrador do sistema do seu Windows 2003.

No comando para ingressar o Linux ([//www.vivaolinux.com.br/linux/](http://www.vivaolinux.com.br/linux/)) no domínio, não coloque o "@INTRAGOV.COM" como para o teste no kinit, caso você coloque, será solicitado normalmente a senha, porém será gerado o seguinte erro:



```
[2011/02/14 19:59:40, 0] libads/kerberos.c:ads_kinit_password(356)
kerberos_kinit_password administrador@INTRAGOV.COM@INTRAGOV.COM failed: Malformed
representation of principal
Failed to join domain: failed to connect to AD: Malformed representation of principal
```

Caso apareça o seguinte erro ao tentar o ingresso ao domínio:

```
Using short domain name -- INTRAGOV
Joined 'ARQUIVOS' to realm 'intragov.com'
No DNS domain configured for arquivos. Unable to perform DNS Update.
DNS updatefailed!
```

Isso significa que não está sendo resolvido o nome do seu servidor de arquivos, para arrumar esse problema, vá até o Windows 2003. Iniciar -> Ferramentas Administrativas -> DNS.

Clique na sua máquina, no meu caso INTRANET + Zonas de pesquisa direta clique com o botão esquerdo do mouse em intragov.com-> Novo host (A). Em Nome você digita o nome do seu servidor Linux (como está configurado o nome em netbios name do seu samba), coloque o endereço IP configurado no seu Linux e clique em Adicionar Host. Agora realize o procedimento novamente.

```
# net ads join -U administrador
```

Agora reinicie o Samba e o winbind:

```
# /etc/init.d/samba restart
# /etc/init.d/winbind restart
```

Configure o nsswitch para que os usuários do AD possam ser autenticados no AD (apenas altere as linhas):

```
# vim /etc/nsswitch.conf
```

```
passwd: compat winbind
group: compat winbind
shadow: compat winbind
```

Caso queira sair do domínio, o comando é:

```
# net ads leave -U administrador
```

← Página anterior (/artigo/Compartilhamento-do-Samba-autenticando-no-AD?pagina=2)

→ Próxima página (/artigo/Compartilhamento-do-Samba-autenticando-no-AD?pagina=4)

Páginas do artigo

1. Introdução (/artigo/Compartilhamento-do-Samba-autenticando-no-AD?pagina=1)
2. Configurando o Samba (/artigo/Compartilhamento-do-Samba-autenticando-no-AD?pagina=2)
3. Ingressando no domínio
4. Testando e concluindo (/artigo/Compartilhamento-do-Samba-autenticando-no-AD?pagina=4)

Outros artigos deste autor

Nenhum artigo encontrado.

Leitura recomendada

- Configurando o Samba de maneira simples e funcional (/artigo/Configurando-o-Samba-de-maneira-simples-e-funcional)
- Autenticando Linux num PDC Samba com auto-montagem de unidade por usuários (sem usar LDAP) (/artigo/Autenticando-Linux-num-PDC-Samba-com-automontagem-de-unidade-por-usuarios-(sem-usar-LDAP))
- Servidor de arquivos Samba (parte 1) - Entendendo de forma básica o funcionamento no Insigne Momentum 5.0 (/artigo/Servidor-de-arquivos-Samba-(parte-1)-Entendendo-de-forma-basica-o-funcionamento-no-Insigne-Momentum-5.0)
- Slackware como controlador de domínio (/artigo/Slackware-como-controlador-de-dominio)
- Samba 4 como controlador de domínio (/artigo/Samba-4-como-controlador-de-dominio)

Comentários

[1] Comentário enviado por removido (/~removido) em 29/03/2011 - 17:04h

Ótimo artigo Tiago. Já tive que fazer muito isso .....

Valeu por compartilhar !

Abraço.



[2] Comentário enviado por johnfelix (/~johnfelix) em 29/03/2011 - 17:23h



Estou tentando implementar uma solução que está bem difícil aqui.  
Preciso fazer com que estações linux conectem a um servidor de arquivos e AD que possui como sistema o Windows Server 2003  
Já consegui fazer o ingresso das estações porém o que está difícil é efetuar as montagens nas estações como era antes da instalação do Ubuntu 10.05.

No Windows Server 2003 tem cadastrados grupos que possui vários usuários.

No XP quando um usuário loga ele automaticamente executa um script de logon que cria as unidades com os arquivos.

Bem esse script é em bat e claro não vai funcionar em Linux daí a dúvida como fazer isso funcionar, pensei no pam\_mount mas depois de várias tentativas sem sucesso estou um pouco desanimado.

Então é isso tenho um PDC e AD utilizando de um PC com Windows Server 2003 e preciso efetuar o mapeamento para os usuários utilizando a política de grupos do servidor Windows.

Qualquer ajuda é de grande valia.



[3] Comentário enviado por minibiga (/~minibiga) em 31/03/2011 - 09:02h

Tive problemas com a data entre os 2 sistemas e o ntpdate nao resolveu, o jeito foi mudar o linux(debian) e o windows 2008 r2 para UTC Universal Time e ajustar os relógios manualmente, ótimo artigo funcionou perfeitamente.



[4] Comentário enviado por tgomarino (/~tgomarino) em 02/06/2011 - 11:16h

Muito bom o artigo, funcionou corretamente, mas como eu faço para que ao autenticar no AD o user já compartilhe a pasta no LINUX?

PS: uso o Ubuntu 11.04

Vlw Abraço



[5] Comentário enviado por tiago2001 (/~tiago2001) em 02/06/2011 - 11:59h



tgomarino, vc está utilizando o ubuntu como servidor de arquivos, o win2003 como PDC e como clientes o winxp ou o seven, é isso?

Qual é o seu nível do Linux, sabe criar pastas, dar permissões, trocar donos das pastas?



[6] Comentário enviado por andrecahadas (/~andrecahadas) em 08/06/2011 - 18:23h

Valeu Funcionou 100% agora vou tentar autenticar os usuários no squid



[7] Comentário enviado por rodolfojss (/~rodolfojss) em 08/06/2011 - 20:38h

Alguém sabe se este procedimento também serve para o Win2k8?



[8] Comentário enviado por andrecahadas (/~andrecahadas) em 08/06/2011 - 21:58h

Funciona sim Testado no AD 2008



[9] Comentário enviado por rodolfojss (/~rodolfojss) em 10/06/2011 - 12:47h

@andrecahadas Muito obrigado por responder (:

Muito bom mesmo



[10] Comentário enviado por tgomarino (/~tgomarino) em 13/06/2011 - 10:53h

tiago2001,

isso mesmo quero usar o ubuntu como file server e o win 2003 como pdc, meus clients são xp e vista.  
meu nível de linux é intermediario, sei como criar pasta e dar permissões e modificar donos!



[11] Comentário enviado por aantunes (/~aantunes) em 14/06/2011 - 12:22h

Tiago,

boa tarde, fiz todos o procedimento, a maquina está no AD, porem quando executo o comando getent passwd só traz os usuarios do linux. o wbinfo -u traz os usuarios do AD.

Já fiz um abusca na net e so encontrei para apagar a base de dados do samba, fiz mas não funcionou. tem alguma coisa mais?



[12] Comentário enviado por tiago2001 (/~tiago2001) em 14/06/2011 - 13:01h

aantunes,

Verifica aí no seu smb.conf as seguintes configurações

idmap uid ou winbind uid -> uid de começo e fim para os usuários do AD;

idmap gid ou winbind gid -> gid de começo e fim para os grupos do AD;

winbind enum users = yes -> utiliza-se para que com o comando getent te retorne os usuários;

winbind enum groups = yes -> utiliza-se para que com o comando getent te retorne os grupos;

winbind use default domain = yes -> utilizando essa linha, será removido o prefix de domínio;

winbind separator = + -> é o caractere utilizado para separar o domínio do usuário ou do grupo.



[13] Comentário enviado por tiago2001 (/~tiago2001) em 14/06/2011 - 13:21h

tgomarino,

Vai lá no seu win2003, em "Usuários e computadores do Active Directory", crie seus usuários e seus grupos, Ex:

usuário: tgomarino

grupo: ti

Aí vc dá dois cliques no usuário tgomarino, vai em "Membro de", coloque em adicionar e coloque "ti"... agora vc pertence ao grupo ti.

Vai no samba e cria um compartilhamento, como:

[ti]

comment= Arquivos da T.I.

path = /mnt/ti

browseable = yes

valid users = @"INTRAGOV+ti"

write list= @"INTRAGOV+ti"

create mask = 0660

directory mask = 0770

force group = +ti



N esqueça de criar a pasta "/mnt/ti" e de dar as devidas permissões e trocar quem é o grupo do dono da pasta

Obs: INTRAGOV é o nome do seu domínio

Agora digamos que vc queira criar uma unidade de rede pro cara acessar direto, vai novamente no 2003, dá dois cliques no usuário e vá em "Perfil", onde está escrito "Script de logon", dê um nome de um arquivo.bat, ex:

"ti.bat", sem aspas.

Agora vc abre o windows explorer, em endereço digite: "\\win2003", lembrando que win2003 é o nome do seu servidor windows, entre na pasta "NETLOGON" crie aí o arquivo "ti.bat" com o seguinte conteúdo:

```
@echo off
echo Mapeando sua unidades de rede.
echo Z:
net use Z: /del /y
net use Z: \\arquivos\ti
```

O que esse script faz é criar uma unidade de rede, primeiro ele exclui caso tenha alguma unidade Z e depois cria, arquivos é o nome do seu linux que vc deu lá no samba.

Assim vc também pode colocar um atalho automaticamente da unidade de rede na área de trabalho da pessoa, caso queria a dica de como fazer isso é só falar.

Caso queira utilizar perfil móvel e precisa de alguma ajuda, pergunta aí.

Até.



[14] Comentário enviado por tgomarino (/~tgomarino) em 15/06/2011 - 09:33h

Vlw parceiro ajudou muito... muito obrigado



[15] Comentário enviado por aantunes (/~aantunes) em 20/06/2011 - 15:56h

Tiago,

Obrigado, já tinha resolvido problema.



[16] Comentário enviado por rodolfo\_ (/~rodolfo\_) em 03/09/2011 - 17:52h

Muito bom! Consegui fazer, foi bem tranquilo.

Só tive um problema, o usuário não conseguia autenticar, mas não conseguia porque existe um tempo de



resposta que eu não estava respeitando.



[17] Comentário enviado por jgama (/~jgama) em 01/10/2011 - 08:04h

Pessoal, estou com o problma na hopra de fazer o teste com comando

```
root@srv-file:~# wbinfo -t
```

```
checking the trust secret via RPC calls failed
```

```
error code was NT_STATUS_UNSUCCESSFUL (0xc0000001)
```

```
Could not check secret
```

```
root@srv-file:~#
```

Eu já usa esta integração quando tinha o DC com Windows Server 2008, e tive que migrar para o Windows Server 2008 R2.

Apesar do erro acima, os comandos "wbinfo -u e wbinfo -g " estão mostrando os usuarios e grupos do AD.

Tenho que fazer algo para resolver o error do wbinfo -t?

Abraço



[18] Comentário enviado por rodolfo\_ (/~rodolfo\_) em 02/10/2011 - 20:21h

Como faço para adicionar somente usuario do dominio? sem o grupo?



[19] Comentário enviado por tiago2001 (/~tiago2001) em 03/10/2011 - 14:35h

jgama,

Procure dar uma olhada no /etc/nsswitch.conf e no /etc/samba/smb.conf, verifique bem as linhas do winbind, deve ser algum problema com ele.



[20] Comentário enviado por tiago2001 (/~tiago2001) em 03/10/2011 - 14:46h

rodolfo,

Acredito que algumas alterações no smb.conf e no switch.conf vc consiga.





No smb.conf faça o seguinte, está assim:

```
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
winbind separator = +
idmap uid = 10000-20000
idmap gid = 10000-20000
```

Faça assim:

```
winbind enum users = yes
winbind enum groups = no
winbind use default domain = yes
winbind separator = +
idmap uid = 10000-20000
```

No /etc/nsswitch.conf na linha  
group: compat winbind

Altere para:

group: compat

Verifica aí se funciona



[21] Comentário enviado por mackay (/~mackay) em 02/11/2011 - 14:45h

Caro Thiago, primeiramente lhe parablenizo pelo excelente tutorial. Nota 10.

Segui todos os passos e foi tudo bem, até antes do teste final.

Tenho o seguinte compartilhamento:

```
[dinfo]
path = /arquivos/arquivos
available = yes
create mask = 0660
directory mask = 0770
browseable = yes
writable = yes
valid users = @"DINFO+dinfo"
write list = @"DINFO+dinfo"
force group = +dinfo
```

No servidor AD Win2008 criei um grupo chamado "dinfo" e um usuário chamado "teste". Coloquei o usuário teste<sup>^</sup>

dentro do grupo "dinfo". Até aí, tudo bem.

Na máquina cliente (WinXP) entro com o usuário "teste" normalmente. Mas quando vou acessar o compartilhamento \\arquivos\dinfo ele me pede senha. Não deveria entrar automaticamente?

E mais, mesmo eu digitando a senha corretamente dá erro. Sempre fica com a janela de login e senha abertas e nunca abre o compartilhamento.

Alguma dica?

Abs,



[22] Comentário enviado por tiago2001 (/~tiago2001) em 02/11/2011 - 15:51h

Mackay, obrigado pelos elogios...

É o seguinte, pode ser algumas coisas, verifique as seguintes:

O winxp esta no seu dominio?

verifique tb o horario entre o controlador de dominio, servidor linux e o winxp, n podem estar c mais de 5min de diferenca.

verifique se vai atraves do ip ao invéz do nome do seu server linux



[23] Comentário enviado por diegodtl (/~diegodtl) em 26/01/2012 - 22:44h

Ótimo artigo funcionou perfeitamente.

Uma dúvida: Queria colocar uma pasta no compartilhamento só leitura para um grupo e controle total para um usuário. Como ficaria a configuração?



[24] Comentário enviado por tiago2001 (/~tiago2001) em 26/01/2012 - 23:36h

Diegodtl, é bem tranquilo, só uma pergunta antes de eu te explicar.

Vc entende os esquemas de dar permissão, os comandos chown, chgrp, chmod, o que significa o 666, o 777?

Só me responde isso, que aí eu te explico detalhadamente dependendo da sua resposta.

Tiago



[25] Comentário enviado por diegodtl (/~diegodtl) em 27/01/2012 - 18:31h



Tiago, entendo sim. A minha pergunta não foi lá essas coisas...kkkkk

O que eu gostaria mesmo era de implantar essa ferramenta no samba (<http://www.vivaolinux.com.br/artigo/Howto-Servidor-Samba+-ACL>) agora, com essa configuração do seu tutorial. Existe possibilidade?



[26] Comentário enviado por ticopan (/~ticopan) em 02/02/2012 - 21:05h

Boa noite caro colaborador.

Estou precisando implementar essa solução em um ambiente que já encontra-se em produção. Hoje os usuários autenticam no samba ao entrarem no servidor de arquivos apenas. Para resolver, estou instalando outro servidor samba clone do primeiro, porém antes de colocá-lo em produção preciso fazer com que este autentique direto no AD, e não mais no passwd do linux.

Entendo que, ao que parece, teu artigo deve resolver essa questão, mas tenho algumas dúvidas. Agradeço desde já a ajuda.

1. Minha rede é heterogênea (estações de trabalho windows xp, win7 e ubuntu 10.04): Essa solução vai funcionar com os desktops linux tb? como?
2. Os servidores windows tem aqueles limites das calls... meus clientes vão ser impedidos de logar ou acessar o samba, caso eu não possua essas calls?
3. Há alguma maneira de deixar as estações ubuntu com o compartilhamento montado em forma de atalho na área de trabalho?

Grato!



[27] Comentário enviado por ticopan (/~ticopan) em 11/05/2012 - 00:45h

Prezado, boa noite novamente.

Resolvi colocar em prática e implementar seu artigo.

Tudo aparente ocorreu ok nos testes, apenas um detalhe que no momento de listar usuários e grupos, apenas me mostra os grupos e usuário do linux (passwd e group).

Ao tentar entrar nos compartilhamentos, a tela de login não loga corretamente sem apresentar nenhuma mensagem de erro (estou logando através do ubuntu). Simplesmente volta a tela solicitando usuário e senha novamente. Pode me ajudar a corrigir esse problema?



[28] Comentário enviado por madson0123 (/~madson0123) em 12/09/2012 - 14:03h

[1] Comentário enviado por Thalysson S em 29/03/2011 - 17:04h:

Ótimo artigo Tiago. Já tive que fazer muito isso .....

Valeu por compartilhar !

Abraço.

Pessoal, encontrei um tutorial QUE REALMENTE FUNCIONOU!!!

Ele mostra como instalar o Samba 4 e configurar pelas ferramentas da Microsoft.

EXCELENTE.

<http://www.stato.blog.br/wordpress/?p=683> (<http://www.stato.blog.br/wordpress/?p=683>)



[29] Comentário enviado por valdenilsonsanto (/~valdenilsonsanto) em 11/04/2013 - 16:02h

Gostaria de parabenizar pelo tutorial, muito bom

Se possível alguém poderia me ajudar em algo aqui. Faz pouco tempo que eu estou estudando Linux e não consigo achar o erro. Todos os testes postados no tutorial foram feitos e retorna tudo normal, só que quando vou acessar as pastas pelo Windows e coloco usuário e senha, não consigo acessar as pastas. Apenas mudei o nome das máquinas e do domínio. Domínio: valdenilson.com Server Windows 2003: serverintranet  
Configuração Samba.

[global]

workgroup = VALDENILSON

server string = Servidor Samba

netbios name = arquivos

realm = VALDENILSON.COM

log file = /var/log/samba/%m.log

os level = 20

max log size = 50

debug level = 1

security = ADS

encrypt passwords = yes

socket options = TCP\_NODELAY SO\_RCVBUF=8192 SO\_SNDBUF=8192

unix charset = iso-8859-1

password server = \*

winbind enum users = yes



```
winbind enum groups = yes
winbind use default domain = yes
winbind separator = +
idmap uid = 10000-20000
idmap gid = 10000-20000
template homedir = /dev/null
template shell = /dev/null
winbind use default domain = yes
```

```
[downloads]
comment= Arquivos T.I.
path = /var/arquivos/informatica
browseable = yes
valid users = @"VALDENILSON+ti"
write list= @"VALDENILSON+ti"
create mask = 0660
directory mask = 0770
force group = +ti
```

```
[teste]
comment= Arquivos Tecnicos
path = /var/arquivos/teste
browseable = yes
valid users = "VALDENILSON+teste"
writelist= "VALDENILSON+teste"
```

```
Configuração krb5.conf
[libdefaults]
default_realm = VALDENILSON.COM
dns_lookup_realm= true
dns_lookup_kdc= true
ticket_lifetime= 24h
forwardable= yes
```

```
# The following krb5.conf variables are only for MIT Kerberos.
```

```
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
```

```
# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# This is the only time when you might need to uncomment these lines and change
# the enctype is if you have local software that will break on ticket
```



```
# caches containing ticket encryption types it doesn't know about (such as  
# old versions of Sun Java).
```

```
# default_tgs_enctypes = des3-hmac-sha1  
# default_tkt_enctypes = des3-hmac-sha1  
# permitted_enctypes = des3-hmac-sha1
```

```
# The following libdefaults parameters are only for Heimdal Kerberos.
```

```
v4_instance_resolve = false  
v4_name_convert = {  
  host = {  
    rcmd = host  
    ftp = ftp  
  }  
  plain = {  
    something = something-else  
  }  
}  
fcc-mit-ticketflags = true
```

```
[realms]  
VALDENILSON.COM= {  
  kdc= serverintranet.valdenilson.com  
  admin_server= serverintranet.valdenilson.com  
  default_domain= VALDENILSON.COM  
}
```

```
[domain_realm]  
.valdenilson.com= VALDENILSON.COM  
valdenilson.com= VALDENILSON.COM
```

```
[login]  
krb4_convert = true  
krb4_get_tickets = false
```



[30] Comentário enviado por tiago2001 (/~tiago2001) em 12/04/2013 - 13:22h

valdenilsonsancto,

Seguinte, no seu diretório [teste] feito na samba, tem um erro, está faltando o "@". Está assim:

```
[teste]  
comment= Arquivos Tecnicos  
path = /var/arquivos/teste  
browseable = yes  
valid users = "VALDENILSON+teste"  
writelist= "VALDENILSON+teste"
```



Deveria estar assim:

[teste]

comment= Arquivos Tecnicos

path = /var/arquivos/teste

browseable = yes

valid users = @"VALDENILSON+teste"

writelist= @"VALDENILSON+teste"

Também é interessante vc utilizar a linha:

force group = +teste

Para que tudo que vc criar seja criado como dono do grupo teste:

outra coisa, também tem que dar permissão no diretório e falar quem é dono, da seguinte forma:

```
# chmod 770 /var/arquivos/teste
```

```
# chgrp teste /var/arquivos/teste
```

## NO WINDOWS

Vc precisa ter o grupo chamado "teste" e colocar seu usuário dentro dele.

Caso a maquina que vc esteja tentando acessar a pasta não esteja no domínio, ele vai solicitar senha para entrar na pasta. Então deve ser colocar o nome de usuario e senha da seguinte forma:

nome de usuário: VALDENILSON\seuusuario

senha: senhadoseuusuario

Qq coisa, posta aí.




[31] Comentário enviado por valdenilsonsanto (/~valdenilsonsanto) em 16/04/2013 - 17:33h

Valeu tiago2001 pela dica, já tinha feito o que vc me pediu, grato, mas o problema não foi esse. Instalei agora em uma máquina no Debian 5 e funcionou normal.

Agora no Debian 6 squeeze, o winbind não está retornando os grupos do AD, o comando wbinfo -g não retorna nada, enquanto todos outros os testes estão normais, e ai não consigo se conectar nas pastas compartilhadas, pesquisei em alguns fórum e me parece que há um erro mesmo quando se instala no Debian 6.0. Se tiver alguma solução, por favor poste para nós. Abraços.



[32] Comentário enviado por tiago2001 (/~tiago2001) em 16/04/2013 - 23:13h

Valdenilsonsantos, já tive esse problema com Debian 6.0, utilizei uma solução bem simples. Basta você utilizar 

repositório do sid "instável" que aí vai de boa.

Antes de tudo, tire o servidor do domino.

Vai lá no repositório.

/etc/apt/source.list

Comenta com # todas as linhas, e coloca as seguintes linhas .

deb http://ftp.br.debian.org/debian (http://ftp.br.debian.org/debian) sid main contrib non-free

deb-src http://ftp.br.debian.org/debian (http://ftp.br.debian.org/debian) sid main contrib non-free

Da Um :

# aptitude update

Desinstala os pacotes winbind, o samba, samba-common, krb-user.

Agora instala eles novamente e coloca no domínio.

Pode testar que o winbind vai te retornar os usuários e grupos.

Qualquer coisa, posta aí .



[33] Comentário enviado por valdenilsonsanto (/~valdenilsonsanto) em 29/04/2013 - 15:42h

Amigão, obrigado pela ajuda, deu certo agora, abraços



[34] Comentário enviado por glauberviera (/~glauberviera) em 03/05/2013 - 16:40h

Tiago,

Tenho esse ambiente configurado aqui em uma VM, agora ele não está trazendo os grupos pelo comando \$getent groups, apenas esse comando não retorna os grupos do AD. com isso não consigo gerenciar os compartilhamentos do samba com os grupos do AD.



[35] Comentário enviado por valdenilsonsanto (/~valdenilsonsanto) em 07/05/2013 - 11:16h

Blz glauberviera, tive o mesmo problema no Debian 6 squeeze, se for essa versão que estiver usando, o Thiago postou a solução ai em cima.

Valdenilsonsantos, já tive esse problema com Debian 6.0, utilizei uma solução bem simples. Basta você utilizar O repositório do sid "instável" que aí vai de boa.

Antes de tudo, tire o servidor do domino.





Vai lá no repositório.

```
/etc/apt/source.list
```

Comenta com # todas as linhas, e coloca as seguintes linhas .

```
deb http://ftp.br.debian.org/debian (http://ftp.br.debian.org/debian) sid main contrib non-free
```

```
deb-src http://ftp.br.debian.org/debian (http://ftp.br.debian.org/debian) sid main contrib non-free
```

Da Um :

```
# aptitude update
```

Desinstala os pacotes winbind, o samba, samba-common, krb-user.

Agora instala eles novamente e coloca no domínio.

Pode testar que o winbind vai te retornar os usuários e grupos.

Qualquer coisa posta ai



[36] Comentário enviado por snowblack85 (/~snowblack85) em 23/06/2013 - 13:57h

Tiago.

Otimo tutorial.

Fiz tudo seguindo os passos agora na hora de adicionar no domino da certo mas apresenta a mensagem de erro.

```
root@srvproxy:~# net ads join -U administrador
```

```
Enter administrador's password:
```

```
Using short domain name -- PRATICA
```

```
Joined 'PROXY' to realm 'pratica.local'
```

```
DNS Update for proxy.pratica.local failed: ERROR_DNS_UPDATE_FAILED
```

```
DNS update failed!
```

não sei porque tá acontecendo isso já refiz tudo mas sempre da esse erro.

segue as configuração:

```
# /etc/nsswitch.conf
```

```
#
```

```
# Example configuration of GNU Name Service Switch functionality.
```

```
# If you have the `glibc-doc-reference' and `info' packages installed, try:
```

```
# `info libc "Name Service Switch"' for information about this file.
```

```
passwd: compat winbind
```

```
group: compat winbind
```

```
shadow: compat winbind
```



hosts: files dns

networks: files

protocols: db files

services: db files

ethers: db files

rpc: db files

netgroup: nis

#####

[global]

workgroup = PRATICA

server string = Servidor Proxy

netbios name = proxy

load printers = no

log level = 5

log file = /var/log/samba/%m.log

max log size = 500

realm = PRATICA.LOCAL

security = ads

auth methods = winbind

password server = 192.168.0.1

winbind separator = +

encrypt passwords = yes

socket options = TCP\_NODELAY SO\_RCVBUF=8192 SO\_SNDBUF=8192

unix charset = iso-8859-1

winbind cache time = 15

winbind enum users = yes

winbind enum groups = yes

winbind use default domain = yes

winbind uid = 10000-20000

winbind gid = 10000-20000

local master = no

os level = 233

domain master = no

preferred master = no

domain logons = no

wins server = 192.168.0.1

dns proxy = no

ldap ssl = no

#####

root@srvproxy:~# vi /etc/krb5.conf

[libdefaults]

default\_realm = PRATICA.LOCAL

^

```
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
forwardable = yes
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
```

```
v4_instance_resolve = false
v4_name_convert = {
host = {
rcmd = host
ftp = ftp
}
plain = {
something = something-else
}
}
fcc-mit-ticketflags = true
```

```
[realms]
PRATICA.LOCAL = {
kdc = server01.pratica.local
admin_server = server01.pratica.local
default_domain = PRATICA.LOCAL
}
```

```
[domain_realm]
.pratica.local = PRATICA.LOCAL
pratica.local = PRATICA.LOCAL
```

```
[login]
krb4_convert = true
krb4_get_tickets = false
```

```
[logging]
```

```
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmin.log
#####
/etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
```

```
domain pratica.local
```



```
search pratica.local
nameserver 192.168.0.1
~
```



[37] Comentário enviado por tiagor7 (/~tiagor7) em 03/07/2013 - 10:30h

Tiago beleza ?  
fiz os procedimentos certinho, consigo acessar as pastas nem pediu a senha ficou perfeito  
agora na hora de criar uma pasta dentro do compartilhamento fala que nao tem permissão  
essa é minha configuração do samba

```
[downloads]
writeable = yes
path = /mnt/arquivos/informatica
write list = @ti
force group = +ti
create mask = 0660
directory mask = 0770
comment = Arquivos T.I.
valid users = @ti
```

```
[teste]
comment= Arquivos Tecnicos
path = /mnt/arquivos/teste
browseable = yes
valid users = "NONOCARTORIO+tiago"
writelist= "NONOCARTORIO+tiago"
```

bom tutorial amigo.

valeu



[38] Comentário enviado por tiagor7 (/~tiagor7) em 03/07/2013 - 10:34h

meu parceiro deu certinho, nao entendo muito de linux, trabalho mais com windows server  
nao sabia que tinha que instalar esses pacotes

```
aptitude update; aptitude install gcc make g++ wget libreadline-dev zlib1g-dev
```



voce merece um UISQUE ..rs

Obrigação mesmo pela força



[39] Comentário enviado por tiago2001 (/~tiago2001) em 03/07/2013 - 18:23h

tiagor7,

acredito que seja apenas problemas de permissão na sua pasta downloads.

Seguinte, vá lá em /mnt/arquivos:

```
# cd /mnt/arquivos
```

Dê a permissão 770 nas suas pastas, ou seja, usuário e grupo pode fazer tudo e os "outros" nada podem:

```
# chmod -R 770 informatica
```

Informe quem é o "grupo" dono da pasta

```
# chgrp -R ti informatica
```

E faltou um detalhe no write list e valid users, que é quem pode escrever na pasta:

```
[downloads]
```

```
path = /mnt/arquivos/informatica
```

```
write list = @"NONOCARTORIO+ti"
```

```
force group = +ti
```

```
create mask = 0660
```

```
directory mask = 0770
```

```
comment = Arquivos T.I.
```

```
valid users = @"NONOCARTORIO+ti"
```

Siga a mesma lógica para a pasta teste, vendo o detalhe que se tiago é um usuário e não um grupo, de a permissão ao usuário na pasta, pode ficar assim:

```
# chmod -R 700 teste
```

Fale quem é o usuário dono da pasta

```
# chown -R tiago teste
```

O "-R" é para recursividade, se já tiverem arquivos e subpastas dentro, elas herdam as atribuições determinadas.

Espero ter ajudado, qq coisa, posta aí.



[40] Comentário enviado por fabiano12 (/~fabiano12) em 02/02/2015 - 17:23h

Tiago2001 boa tarde,

Gostaria de parabenizá-lo pelo post, com riqueza de detalhes e simplicidade na explicação! Parabéns!

Vi em um dos comentários/explicação para um dos usuários, tgomarino, no dia 14/06/2011, onde vc cita sobre perfil móvel no samba.

Haveria a possibilidade de colocar algum exemplo sobre isso? Estou esbarrando nisso para virar o parque computacional da empresa para Ubuntu.

Certo de sua atenção.

Sds,

Fabiano Lima



[41] Comentário enviado por tiago2001 (/~tiago2001) em 03/02/2015 - 08:01h

[40] Comentário enviado por fabiano12 em 02/02/2015 - 17:23h

Tiago2001 boa tarde,

Gostaria de parabenizá-lo pelo post, com riqueza de detalhes e simplicidade na explicação! Parabéns!

Vi em um dos comentários/explicação para um dos usuários, tgomarino, no dia 14/06/2011, onde vc cita sobre perfil móvel no samba.

Haveria a possibilidade de colocar algum exemplo sobre isso? Estou esbarrando nisso para virar o parque computacional da empresa para Ubuntu.

Certo de sua atenção.

Sds,

Fabiano Lima

Então Fabiano,

Não recomendo muito vc utilizar perfil móvel pq dá um tráfego muito grande na rede, experiência própria. Tirei dos dois Hospitais que administro por conta da lentidão na hora de fazer login. Sou muito mais fazer umas Unidades de Rede subir automaticamente com atalhos na área de trabalho do usuário e passar um comunicado^

que só pode gravar nesses atalhos.

Bom, mas eu usava da seguinte maneira o perfil móvel no samba:

Compartilhei uma pasta no samba com o nome perfil, deixei como dono um grupo chamado publico e todos pertencendo ao grupo público, com permissão 777. Dentro da pasta perfil tinha a pasta de cada usuário, com o mesmo nome do usuário gerado no AD, com permissão 700.

No caminho do perfil no Servidor Windows eu colocava o caminho da seguinte maneira: \\192.168.1.6\perfil\%username%.

O 192.168.1.6 como sendo seu Servidor Samba, basta selecionar todos os usuários que deseja colocar o perfil, clicar com o botão direito e em propriedades, clicar na aba "Perfil" e colocar o caminho como falei. O %username% será substituído por cada conta de usuário.

Espero que tenha ajudado.



[42] Comentário enviado por o\_krah (/~o\_krah) em 12/07/2015 - 19:07h

Tiago, parabens pelo seu artigo.

estou com problema em implementar sua solucao no server 2012 e samba4, como la em cima, o wbinfinfo retorna os users do AD, mas o getent nao... e tambem nao acessa as pastas compartilhadas... continua pedindo senha constantemente...



[43] Comentário enviado por o\_krah (/~o\_krah) em 13/07/2015 - 00:28h

[42] Comentário enviado por o\_krah em 12/07/2015 - 19:07h

Tiago, parabens pelo seu artigo.

estou com problema em implementar sua solucao no server 2012 e samba4, como la em cima, o wbinfinfo retorna os users do AD, mas o getent nao... e tambem nao acessa as pastas compartilhadas... continua pedindo senha constantemente...

Consegui resolver da seguinte forma: removi os pacotes, usei o repositorio SID, mas mesmo assim continuava o mesmo problema, aí instalei as dependencias: apt-get install libnss-winbind libpam-winbind

Pronto... getent retornou todos os usuarios do AD, e assim a estacao windows entrou corretamente nas pastas conforme as permissoes.



[44] Comentário enviado por tiago2001 (/~tiago2001) em 13/07/2015 - 13:17h

[43] Comentário enviado por o\_krah em 13/07/2015 - 00:28h

[42] Comentário enviado por o\_krah em 12/07/2015 - 19:07h

Tiago, parabens pelo seu artigo.

estou com problema em implementar sua solucao no server 2012 e samba4, como la em cima, o wbinfo retorna os users do AD, mas o getent nao... e tambem nao acessa as pastas compartilhadas... continua pedindo senha constantemente...

Consegui resolver da seguinte forma: removi os pacotes, usei o repositorio SID, mas mesmo assim continuava o mesmo problema, aí instalei as dependencias: apt-get install libnss-winbind libpam-winbind

Pronto... getent retornou todos os usuarios do AD, e assim a estacao windows entrou corretamente nas pastas conforme as permissoes.

o\_krah, obrigado pelo feedback da solução, pode ter certeza que isso ajuda muitas pessoas.



[45] Comentário enviado por AndressaCPD (/~AndressaCPD) em 29/09/2015 - 07:52h

Gostei mesmo do artigo, agora gostaria de saber se voce pode me ajudar.

Tenho um servidor samba funcionando onde a autenticação é feita pelos usuario do AD porém queria liberar a pasta home dos usuario para que cada usuario grave seus arquivos. tenho a seguinte situação no smb.conf

```
[homes]
path=home/%u/share
valid users=%S
read only= no
create mask= 0700
directory mask= no
writable= no
```

Ao entrar no Samba mostra a pasta do uruario porém não tenho acesso.



[46] Comentário enviado por cmaia (/~cmaia) em 30/09/2015 - 07:37h





Bom dia Tiago

Parabens pelo post, esta bastante claro e é muito util.

Acabei de implementa-lo e quase tudo correu bem....quase, porque ele não esta registrando no DC. Digito o comando "net ads join -U admin" de seguida introduzo a password do admin como solicitado e surge as seguintes frases " Using short domain mane -- DOMAIN", "Joined 'maquina' to dns domain 'domain.com'", "No DNS domain configured for maquina. Unable to perform DNS Update." e "DNS update failed: NT\_STATUS\_INVALID\_PARAMETER"

Ja adicionei a maquina no servidor DNS e continua a dar o mesmo erro o que não permiti aceder a maquina atraves de outro PC. O que estou achando estranho é que quando avanço no post e executo os comandos "net ads testjoin" recebo a mensagem OK e tambem vejo todas as listas pedidas nos comandos "wbinfo" e "getent"

Obrigado pela ajuda,



[47] Comentário enviado por juniolemos (/~juniolemos) em 11/12/2015 - 17:21h

Bom tarde Tiago, Ótimo post

fiz tudo certo esta autenticando, só não consigo escrever na pasta pelo meu usuario cadastrado no grupo Ti, oque posso fazer?

Segue o smb.conf

[global]

workgroup = UNYLEYA

server string = Samba Server

netbios name = conopus

realm = UNYLEYA.CORP

passdb backend = tdbsam

password server = 192.168.7.2

idmap uid = 10000-20000

idmap gid = 10000-20000

winbind enum users = yes

winbind enum groups = yes

winbind use default domain = yes

winbind nested groups = yes

winbind cache time = 86400

winbindseparator=+

max connections = 0

socket options = TCP\_NODELAY SO\_RCVBUF=8192 SO\_SNDBUF=8192

unix charset = iso-8859-1

template shell = /bin/false



```
template homedir = /dev/null
enhanced browsing = no

log file = /var/log/samba/%m.log
max log size = 1000
syslog = 0
encrypt passwords = true
security = ADS
password server = 192.168.7.2
preferred master = no
wins server = KUMA.UNYLEYA.CORP
dns proxy = no
load printers = no
map to guest = bad user
```

```
[bkp_full_tag]
comment = pasta para bkp taguatinnga
path = /home/bkp_full_tag
read only = no
browseable = yes
valid users = @"UNYLEYA.CORP+ti"
write list = @"UNYLEYA.CORP+ti"
create mask = 0660
directory mask = 0770
force group = +ti
```



[48] Comentário enviado por juniolemos (/~juniolemos) em 11/12/2015 - 17:35h

Não precisa mais, desativei o Selinux e funcionou !



## Contribuir com comentário



Enviar



A maior comunidade GNU/Linux da América Latina! Artigos, dicas, tutoriais, fórum, scripts e muito mais. Ideal para quem busca auto-ajuda.

[FAQ - Perguntas frequentes \(/faq.php\)](/faq.php)

---

[Estatísticas do site \(/estatisticas.php\)](/estatisticas.php)

---

[Equipe de moderadores \(/equipe/\)](/equipe/)

---

[Membros da comunidade \(/membros/\)](/membros/)

---

[Anuncie \(/anuncie/\)](/anuncie/)

---

[Contato \(/falecom/\)](/falecom/)

---

[Política de privacidade \(/privacidade/\)](/privacidade/)

---

[Quem somos \(/quemsomos/\)](/quemsomos/)

---

[Termos de uso \(/termos-de-uso/\)](/termos-de-uso/)

---

Site hospedado por:



[\(/verBanner.php?codigo=247\)](/verBanner.php?codigo=247)



Visite também: [BR-Linux.org \(/verBanner.php?codigo=134\)](#) · [Dicas-L \(/verBanner.php?codigo=135\)](#) · [Diolinux \(/verBanner.php?codigo=506\)](#) · [SoftwareLivre.org \(/verBanner.php?codigo=133\)](#) · [UnderLinux \(/verBanner.php?codigo=131\)](#) · [Blog do Edivaldo \(/verBanner.php?codigo=565\)](#)