

Samba Member Server Troubleshooting

...

Esta Aula tratará os problemas comuns ao configurar ou executar um membro do domínio do Samba AD .

Problema

- Você deseja configurar SeDiskOperatorPrivilege em seu servidor membro para gerenciar suas permissões de compartilhamento, mas você recebe um erro como este:

```
net rpc rights grant 'SEUDOMINIO\Domain Admins'  
SeDiskOperatorPrivilege -U'SEUDOMINIO\administrator'  
Enter SEUDOMINIO\administrator's password:  
Could not connect to server 127.0.0.1  
The username or password was not correct.  
Connection failed: NT_STATUS_LOGON_FAILURE
```

Solução

- Neste caso, você precisa criar um arquivo de mapeamento de usuário dentro do diretório etc do seu samba . Ex: `/opt/samba/etc/user.map` com o seguinte conteúdo.

```
!root = SEUDOMINIO\Administrator SEUDOMINIO\administrator
```

- Depois disso, você precisa adicionar um parâmetro à seção `[global]` do seu `smb.conf`:

```
username map = /opt/samba/etc/user.map
```

- Reinicie ou recarregue o samba e você poderá configurar DiskOperatorPrivilege com a conta de administrador:

```
# smbcontrol all reload-config
```

```
# net rpc rights grant 'SEUDOMINIO\Domain Admins'  
SeDiskOperatorPrivilege -U'SEUDOMINIO\administrator'
```

Problema

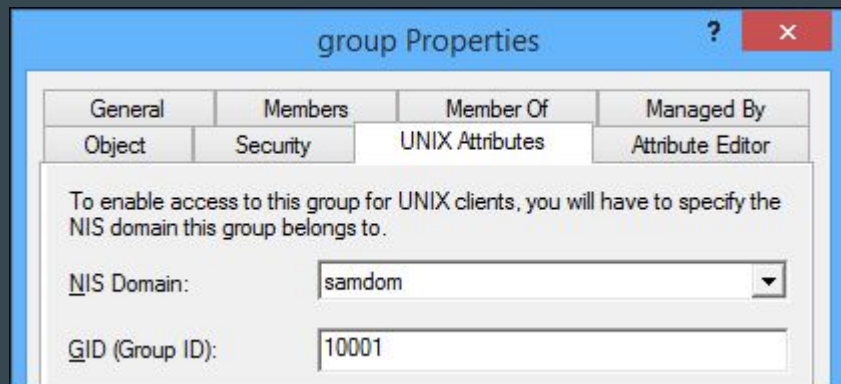
- O comando `getent` não retorna usuários ou grupos de domínio

```
getent group domain admins ( não retorna nada)
```

```
getent passwd alex ( não retorna nada)
```

Soluções

- Verifica se o parâmetro NIS Domain está configurado.
- Verifica se UID está configurado no usuário
- Verifica se o GUID está configurado no grupo



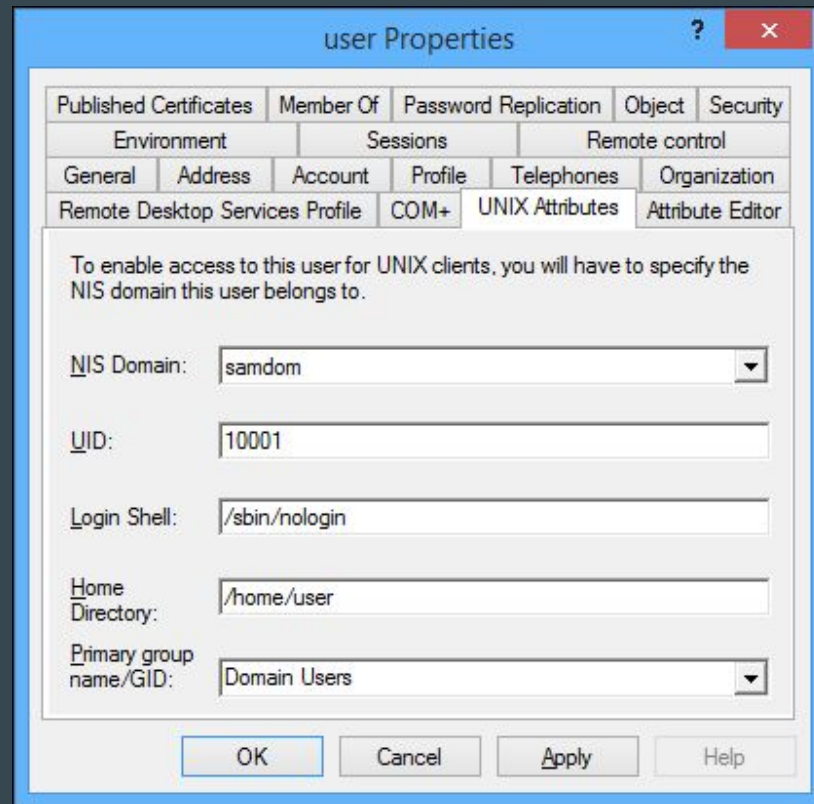
The 'group Properties' dialog box is shown with the 'UNIX Attributes' tab selected. It contains fields for 'NIS Domain' (set to 'sandom') and 'GID (Group ID)' (set to '10001').

General	Members	Member Of	Managed By
Object	Security	UNIX Attributes	Attribute Editor

To enable access to this group for UNIX clients, you will have to specify the NIS domain this group belongs to.

NIS Domain:

GID (Group ID):



The 'user Properties' dialog box is shown with the 'UNIX Attributes' tab selected. It contains fields for 'NIS Domain' (set to 'sandom'), 'UID' (set to '10001'), 'Login Shell' (set to '/sbin/nologin'), 'Home Directory' (set to '/home/user'), and 'Primary group name/GID' (set to 'Domain Users').

Published Certificates	Member Of	Password Replication	Object	Security
Environment		Sessions	Remote control	
General	Address	Account	Profile	Telephones
Remote Desktop Services Profile		COM+	UNIX Attributes	Organization
Attribute Editor				

To enable access to this user for UNIX clients, you will have to specify the NIS domain this user belongs to.

NIS Domain:

UID:

Login Shell:

Home Directory:

Primary group name/GID:

OK Cancel Apply Help

- Crie links para a biblioteca Libnss winbind

```
ln -s /usr/local/samba/lib/libnss_winbind.so.2 /lib/x86_64-linux-gnu/  
ln -s /lib/x86_64-linux-gnu/libnss_winbind.so.2 /lib/x86_64-linux-gnu/libnss_winbind.so  
ldconfig
```

- Você tem usuários de domínio que também são usuários locais? Execute isso no servidor de arquivos para conferir:

```
cat /etc/passwd | grep <usuário do domínio>
```

- Você não pode ter usuários locais que também são usuários do domínio. Se você tiver algum, decida qual você deseja manter e exclua o outro.

- Você tem um arquivo keytab no servidor de arquivos? verifique com o comando :

```
klist -k
```

```
Nome do Keytab: FILE: /etc/krb5.keytab
```

```
KVNO Principal
```

```
-----
```

```
1 host/Member1.SEUDOMINIO.example.com@SEUDOMINIO.EXAMPLE.COM
1 host/Member1.SEUDOMINIO.example.com@SEUDOMINIO.EXAMPLE.COM
1 host/Member1.SEUDOMINIO.example.com@SEUDOMINIO.EXAMPLE.COM
1 host/Member1.SEUDOMINIO.example.com@SEUDOMINIO.EXAMPLE.COM
1 host/Member1.SEUDOMINIO.example.com@SEUDOMINIO.EXAMPLE.COM
1 host/Member1@SEUDOMINIO.EXAMPLE.COM
```

- Se não houver nenhum keytab, verifique se o computador está ligado ao domínio:

```
sudo net ads testjoin
```

Join is OK (se não retornar ok ingresse no domínio)

- Se o computador está ingressado no domínio , retornando ok para o comando anterior e mesmo assim o arquivo keytab não foi criado , então talvez esteja faltando os seguintes parâmetros em seu smb.conf na seção global :

```
dedicated keytab file = /etc/krb5.keytab
```

```
kerberos method = secrets and keytab
```

```
winbind refresh tickets = Yes ( Sem ele, os tickets do kerberos expirarão e não serão renovados.
```

- Adicione as linhas acima e em seguida, remova do domínio e ingresse novamente aí o keytab será criado automaticamente :

```
net ads leave -U Administrator
```

```
net ads join -U Administrator
```

- Verifique as configurações de DNS do servidor membro, primeiro, os nomes FQDN dos servidores membros:

```
hostname -f
```

- Tem que retornar algo como :

```
Member1.seudominio.com
```

- Em seguida, verifique se o domínio coincide com o realm kerberos, usando o comando :

```
hostname -d
```

```
seudominio.com
```

- Finalmente, verifique se o nome de host curto é apenas uma palavra

```
hostname -s
```

```
Member1
```

- Se você não conseguir os resultados corretos, verifique se o `/etc/hosts` está configurado corretamente:

```
127.0.0.1 localhost
```

```
192.168.1.100 Member1.seudominio.com Member1
```

- verifique o arquivo resolv.conf

```
search samdom.example.com
```

```
nameserver 192.168.1.16 <--- Este deve ser o IP do seu DC
```

- Verifique o arquivo /etc/krb5.conf

```
[libdefaults]
```

```
    default_realm = SEUDOMINIO.COM
```

```
    dns_lookup_realm = false
```

```
    dns_lookup_kdc = true
```

- Verifique o arquivo `/etc/nsswitch.conf`

```
passwd: files winbind  
group:  files winbind  
hosts:  files dns  
networks: files dns
```

- Se você obtiver resultados, mas eles não são exatamente o esperado, tente remover o cache do winbind:

```
net cache flush
```

FIM

...