

Configurando o Winbind em um DC Samba

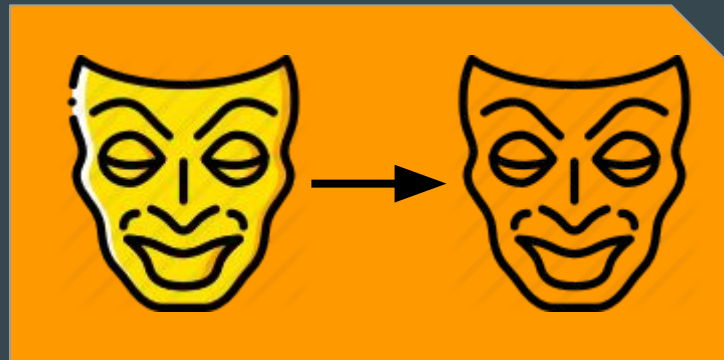
...

- O Winbind é um programa que permite aos usuários em uma rede heterogênea fazer login usando estações de trabalho que possuem sistemas operacionais Linux ou Windows NT s.
- O programa faz estações de trabalho usando o Linux funcional em domínios NT, fazendo com que o NT pareça ser Linux para cada estação de trabalho Linux .
- Assim como o DNS mapeia nomes para IPs, o Winbind mapeia usuários linux para Windows e vice e versa.



Benefícios .

- Configurar permissões para usuários e grupos do domínio como se fossem do linux.
- Usar usuários e grupos de domínio em comandos locais, como chown e chgrp.



Usuário no Active Directory

- Quando criamos um usuário no Active Directory ele é representado pelo SID é um identificador de segurança. É a "chave primária" para qualquer objeto em um Active Directory

S-1-5-21-3623811015-3361044348-30300820-1013

- Composto pelo domain SID e o RID

Usuário no Linux

- Quando criamos um usuário no Linux ele é representado pelo UID (user identifier) e o GUID (Group identifier) e assim eles encontrados no Linux
- Além disso todo usuário tem uma shell e um diretório home.

```
bob:x:1002:1002:~/home/bob:/bin/bash
```



Diferenças entre Winbind e o serviço Winbindd

- A partir do Samba 4.2 é permitido que o utilitário winbindd fosse usado em controladores de domínio (DC).
- E é isso que vamos aprender a configurar em um DC Samba 4
- E só vale para a versão 4.2 ou superior .



Diferenças do Windbindd em DC e Membro de domínio

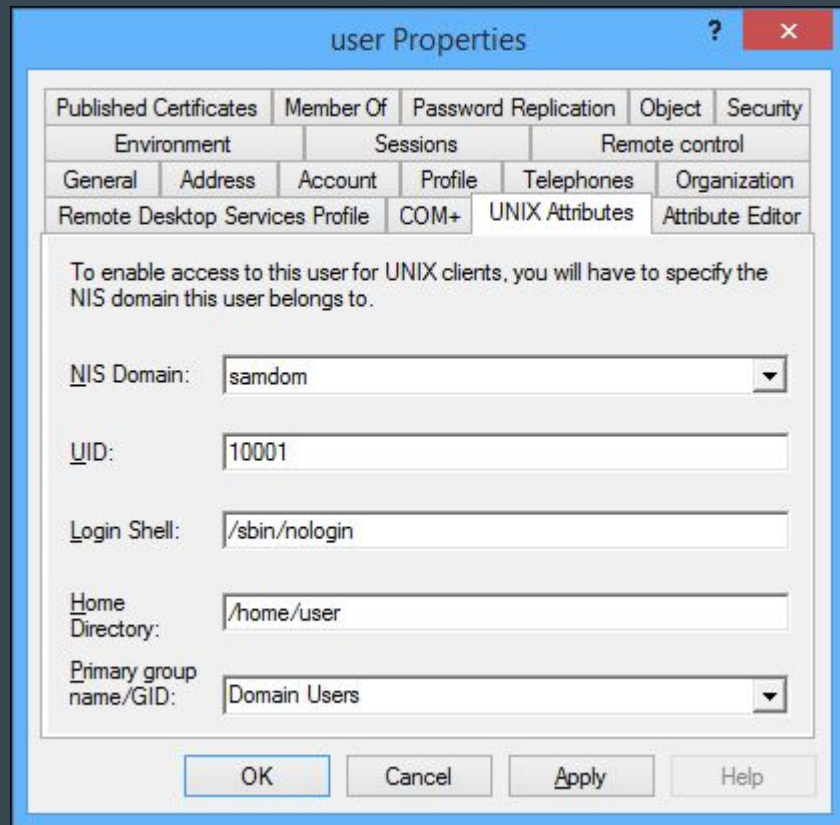
- O Mapeamento de Identidade funciona diferente em um controlador de domínio Samba (DC) do que em um membro do domínio.
- Em um DC do Samba Active Directory, Winbindd sempre lê IDs de usuário (UID) e IDs de grupo (GID) a partir dos valores definidos nos atributos uidNumber e gidNumber definidos nos objetos AD.

The screenshot shows the 'user Properties' dialog box with the 'UNIX Attributes' tab selected. The dialog box contains the following fields and options:

- Published Certificates**, **Member Of**, **Password Replication**, **Object**, **Security**
- Environment**, **Sessions**, **Remote control**
- General**, **Address**, **Account**, **Profile**, **Telephones**, **Organization**
- Remote Desktop Services Profile**, **COM+**, **UNIX Attributes**, **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:** samdom
- UID:** 10001
- Login Shell:** /sbin/nologin
- Home Directory:** /home/user
- Primary group name/GID:** Domain Users
- OK**, **Cancel**, **Apply**, **Help**

Diferenças do Windbindd em DC e Membro de domínio

- Para usuários e grupos que não tenham atribuídos UID ou GID, uma ID é gerada localmente no DC e armazenada no arquivo `/CAMINHO/DE/INSTALAÇÃO/samba/private/idmap.ldb`.



The screenshot shows the 'user Properties' dialog box with the 'UNIX Attributes' tab selected. The dialog has a blue title bar and a tabbed interface. The 'UNIX Attributes' tab is active, displaying fields for NIS Domain, UID, Login Shell, Home Directory, and Primary group name/GID. The NIS Domain is set to 'samdom', UID to '10001', Login Shell to '/sbin/nologin', Home Directory to '/home/user', and Primary group name/GID to 'Domain Users'. There are buttons for OK, Cancel, Apply, and Help at the bottom.

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:

Pimary group name/GID:

OK Cancel Apply Help

winbindd configurações

- Para executar Winbindd em um controlador de domínio Samba Active Directory (AD), na maioria dos casos, nenhuma configuração no smb.conf arquivo é necessária.
- IDs de usuário e grupo, são carregados a partir do Active Directory (AD) ou gerados automaticamente localmente.
- Em um Samba DC, apenas o **winbind template mode** é suportado. Neste modo 2 coisas acontecem :
 - O caminho do diretório inicial (home) é definido no parâmetro `template homedir`. O valor padrão desse parâmetro é `/home/%D/%U`
 - O shell é atribuído no parâmetro `template shell`. O valor padrão desse parâmetro é `/bin/false`.

Personalizando as configurações

- Para atribuir a shell `/bin/bash` e o caminho `/home/%U` como caminho do diretório inicial (home) para todos os usuários de domínio fornecidos por Winbindd, Adicione os seguintes parâmetros à seção `[global]` do seu arquivo `smb.conf`:

```
template shell = /bin/bash
```

```
template homedir = /home/%U
```

- Reinicie o serviço samba.

- Para tornar usuários e grupos de domínio disponíveis para o sistema local edite o arquivo `/etc/nsswitch.conf` insira o parâmetro `winbind` na frente dos parâmetros `passwd` e `group`.

```
passwd: files winbind
group:  files winbind
shadow: files
```



PULO DO GATO 1

- Não adicione a winbind ao shadow, isso pode causar falha no wbinfo.

```
passwd: files winbind  
group:  files winbind  
shadow: files ( AQUI NÃO)
```

- Não use os mesmos nomes de usuário no linux local e no domínio.



PULO DO GATO 2

- Se você compilou o Samba, adicione links simbólicos da biblioteca `libnss_winbind` ao caminho da biblioteca do sistema operacional.
- Se você usou pacotes para instalar o Samba, o link geralmente é criado automaticamente.



Criando o Link

1. Verificar plataforma do seu sistema linux:

```
uname -i
```

2. Localizando a Biblioteca `libnss_winbind.so.2`

```
smbd -b | grep LIBDIR
```

```
LIBDIR: / usr / local / samba / lib /
```

3. Link a biblioteca deste diretório no diretório da biblioteca do seu linux.

Sistemas operacionais baseados em Debian

x86_64

```
ln -s /pasta/de/instalação/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

O serviço Winbindd

- Não inicie o Serviço winbindd manualmente em um controlador de domínio Samba Active Directory (AD) (DC). O serviço é iniciado automaticamente como um subprocesso do processo `samba`.

Para verificar:

```
ps axf
```

```
2158 ?    S   0:00  |_ /usr/local/samba/sbin/samba -D
```

```
2172 ?    R   0:00  |_ /usr/local/samba/sbin/winbindd -D --option=server role check:inhibit=yes --foreground
```


Testando Mapeamento de usuários e grupos

- Testando mapeamento de usuários

```
getent passwd "DOMÍNIO\\USUÁRIO"
```

- Testando mapeamento de grupos

```
getent "group DOMÍNIO\\GRUPO"
```

- Configurar permissões

```
chown "DOMÍNIO\\usuário:DOMÍNIO\\group" file.txt
```

Prática

...