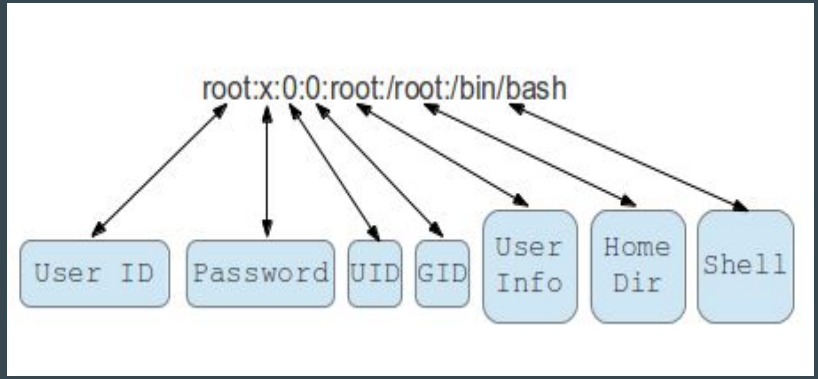
Winbindd no Servidor Dedicado

Definição da ID do usuário

- Um ID de usuário (UID) é um inteiro positivo exclusivo atribuído pelo Linux
- Cada usuário é identificado ao sistema por seu UID, e os nomes de usuários geralmente são usados apenas como uma interface para humanos.
- Os UIDs são armazenados, no arquivo `/etc/passwd`



- Nos kernels 2.4 ou superior, os UIDs são inteiros de 32 bits não assinados que podem representar valores de zero a 4.294.967.296
- O UID de 0 tem um papel especial: é sempre a conta root(ou seja, o usuário administrativo omnipotente)
- O UID 65534 é comumente reservado para `nobody` usado para acesso via ftp e http
- Os UID 1 a 99 são tradicionalmente reservados para usuários especiais do sistema (às vezes chamados de pseudo-usuários) como `daemon, lp, operator, news, mail` , São administradores mas não precisam de poderes de root totais,
- Algumas distribuições de Linux iniciam UIDs para usuários não privilegiados em 100. Outros, como o Red Hat, começam em 500, o Debian, começam em 1000

Não é necessário que cada entrada no campo UID seja única. No entanto, os UID não únicos podem causar problemas de segurança e, portanto, os UIDs devem ser mantidos únicos em toda a organização.

Por quê

- Configurar mapeamento de usuários com winbindd
- Configurar onde as informações serão armazenadas
- Configurar qual irá ser a flexibilidade dessas informações

Como será feito ?

- Teremos que configurar o mapeamento de IDs no servidor membro que funcionará como servidor dedicado .
- Isso é feito usando o backend de mapeamento de IDs usando o parametro `idmap` no smb.conf
- Existem 6 back ends de mapeamentos de IDs cada um com sua características sendo que os principais que nos interessa são 3 :
  - idmap config ad (RFC2307)
  - idmap config rid
  - idmap config autorid

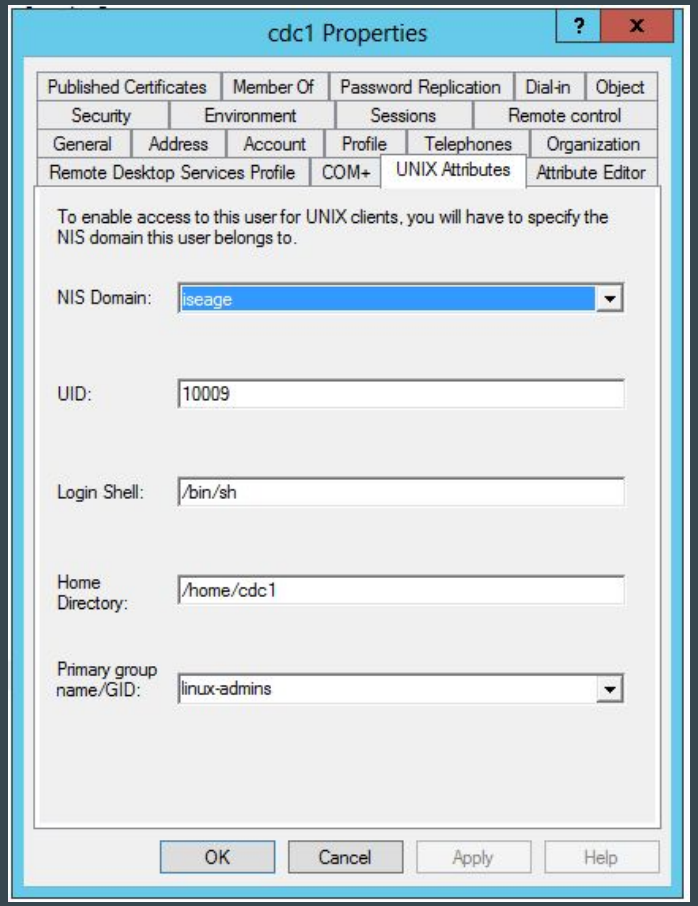
Vantagens e Desvantagens

...

Vantagens e Desvantagens do ‘ad’ Back End

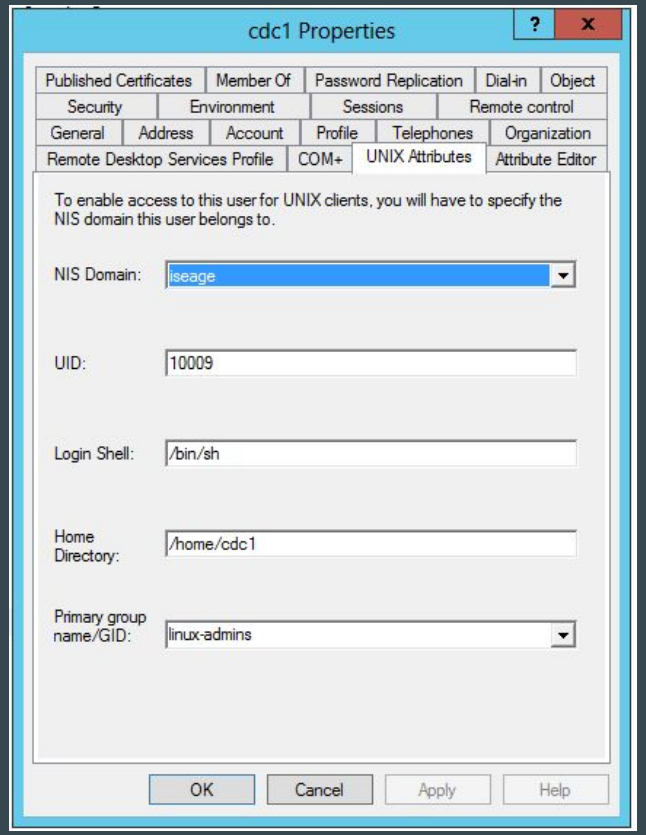
- Vantagens:
  - Administração central de IDs dentro do Active Directory (AD).
  - IDs consistentes em todos os clientes e servidores Samba usando o ‘ad’ back-end.
  - Os atributos necessários apenas precisam ser criados uma vez, isso pode ser feito quando o usuário ou grupo é criado
  - Os IDs não são armazenados em um banco de dados local que pode corromper e, assim, os proprietários de arquivos não são perdidos.

- Desvantagens:
  - Se o programa Windows Active Directory Users and Computers(ADUC) não for utilizado, você deve rastrear manualmente os IDs usados para evitar duplicados.
  - Os valores para os atributos RFC2307 devem ser configurados manualmente.
- Funções específicas de modo de informação do Winbind NSS:
  - rfc2307: Shells de login individuais e caminhos do diretório inicial para usuários.
  - template: Os shells de login e os caminhos do diretório home são os mesmos para todos os usuários.

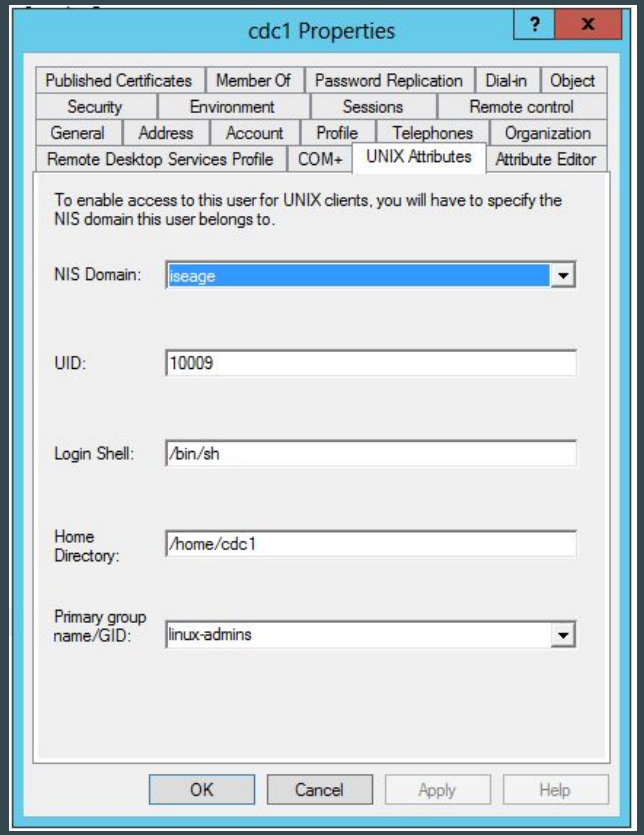


Pré-requisitos

- Os usuários devem ter pelo menos os conjuntos de atributos uidNumber e gidNumber.
- As contas de usuário também devem ter o loginShell, unixHomeDirectory e primaryGroupID definidos.
- Computadores, ou: 'contas de rede da máquina', devem ter o atributo uidNumber definido para acessar compartilhamentos em membros do domínio samba.
-



- O usuários, computadores e os IDs de grupo devem estar dentro do intervalo configurado no smb.conf.
- Se o (ADUC) for usado para atribuir os atributos UNIX, as extensões NIS devem ser instaladas.



- As IDs do usuário e do computador devem ser únicas para todos os usuários e computadores e as IDs de grupo devem ser exclusivas para todos os grupos. Duplicar IDs ou reutilizar IDs de contas excluídas anteriormente permitem que o novo usuário, computador ou grupo acesse arquivos criados pelo outro proprietário ou ID anterior.
- Ao usar o ADUC, os IDs de usuário e grupo são rastreados automaticamente dentro do AD e aumentados ao criar um novo usuário ou grupo.
- Os IDs do computador (atributo uidNumber) não são rastreados automaticamente dentro do AD e devem ser configurados manualmente na guia Editor de Atributo unix no ADUC quando um computador é ingressado ao domínio.

Antes do Samba versão 4.6.0:

- O ad back end do mapeamento de ID suporta dois modos, defina o parâmetro na seção [global] do arquivo smb.conf:
- `winbind nss info = rfc2307`: Todas as informações são lidas do Active Directory (AD):
  - **Usuários**: nome da conta, UID, shell de login, caminho do diretório hone grupo primário.
  - **Grupos**: nome do grupo e GID.
- `winbind nss info = template`: Somente os seguintes valores são lidos do AD:
  - **Usuários**: nome da conta, UID e grupo principal. O shell de login e o diretório inicial são definidos automaticamente pelas configurações independentes do usuário no arquivo smb.conf.
  - **Grupos**: nome do grupo e GID

Da versão 4.6.0 para cima:

- Você não usa mais o parâmetro `winbind nss info`, foi substituído por `idmap config DOMAIN : unix_nss_info`
- O ‘ad’ back end do mapeamento de ID suporta dois modos, defina o parâmetro `idmap config DOMAIN : unix_nss_info` na seção [global] do arquivo smb.conf:
- `idmap config DOMAIN : unix_nss_info = yes`: Todas as informações são lidas do Active Directory (AD):
  - **Usuários**: nome da conta, UID, shell de login, caminho do diretório home e grupo primário.
  - **Grupos**: nome do grupo e GID.
  - Essas configurações são definidas em uma base DOMAIN, isso significa que você pode ter configurações diferentes para cada DOMÍNIO.

- Se um usuário não possui os atributos RFC2307, o shell de logon e o diretório inicial são definidos automaticamente por configurações independentes no arquivo smb.conf.
- `idmap config DOMAIN : unix_nss_info = no`: Somente os seguintes valores são lidos do AD:
    - **Usuários**: nome da conta, UID e grupo principal. O shell de login e o diretório home são definidos automaticamente pelas configurações independentes do usuário no arquivo smb.conf.
    - **Grupos**: nome do grupo e GID
    - Esta é a configuração padrão.

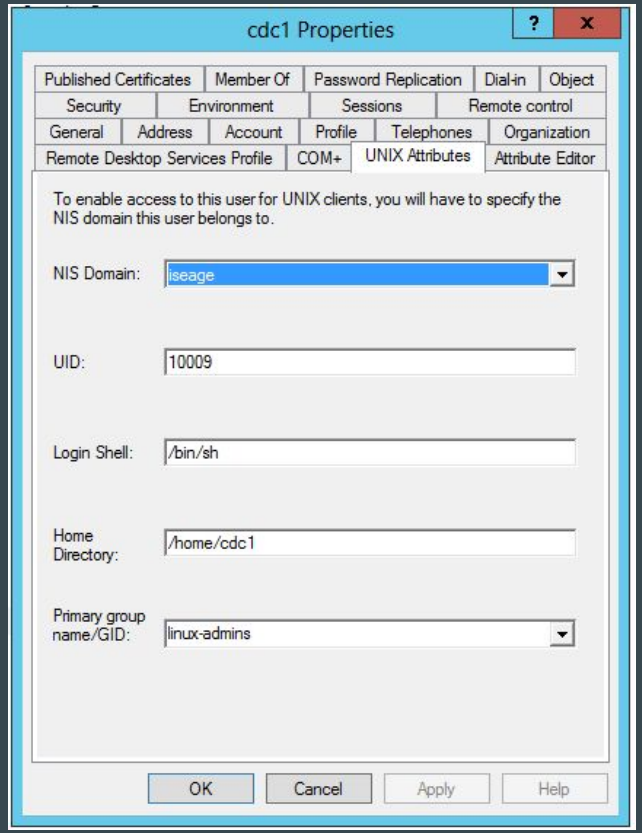
- Existe agora uma nova configuração `unix_primary_group`, isso permite que você use outro grupo para o grupo principal de usuários em vez de usuários do domínio.
- Se isso for definido `unix_primary_group = yes`, o grupo primário de usuários é obtido a partir do atributo gidNumber encontrado no objeto AD de usuários.
- Se isso for definido `unix_primary_group = no`, o grupo primário dos usuários é calculado através do atributo "primaryGroupID".
- O padrão é ‘no’

Configurando o ‘ad’ Back End

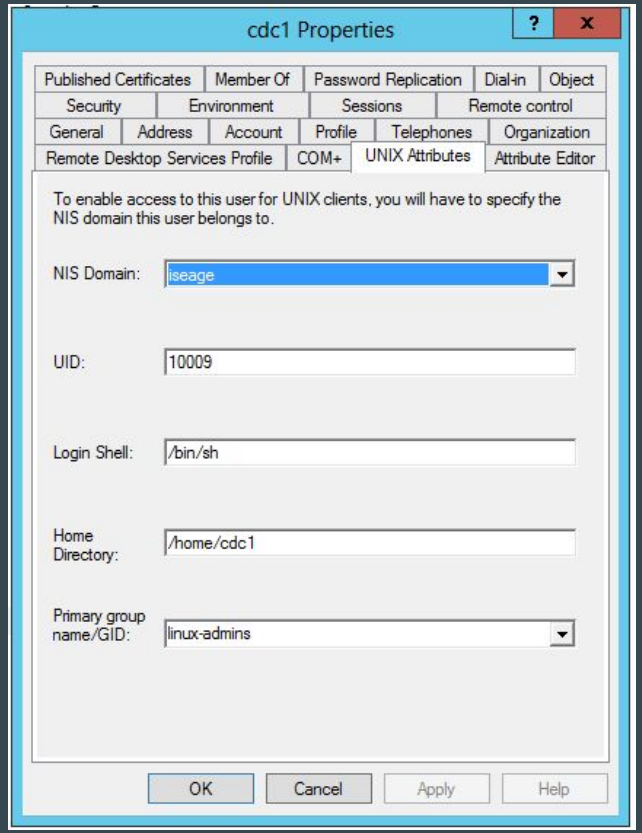
- Configure o seguinte na seção [global] do seu arquivo smb.conf:

```
idmap config * : backend = tdb
idmap config * : range = 3000-7999
idmap config DOMINIO:backend = ad
idmap config DOMINIO:schema_mode = rfc2307
idmap config DOMINIO:range = 10000-999999
idmap config DOMINIO: unix_nss_info = yes
template shell = /bin/bash
template homedir = /home/%U
```

- O Samba configura o grupo primário do Windows como grupo principal para entradas de usuário de domínio mapeado no Unix. O grupo primário do Windows é recuperado do atributo primaryGroupID de cada entrada de usuário, geralmente é o grupo Domain Users. Esse RID é então usado para obter o atributo gidNumber do grupo primário do Windows.



- Se você estiver executando o Samba 4.6.0 ou posterior, você pode configurar o Samba para usar o grupo primário definido no atributo gidNumber na entrada dos usuários. Por exemplo, ao usar o ADUC, este atributo é exibido na guia `UNIX Attributes`. Para usar o ID de grupo definido no atributo gidNumber de usuários como grupo primário para cada usuário em vez do grupo primário do Windows, ative o seguinte parâmetro na seção[global] em seu arquivo smb.conf:




```
idmap config DOMINIO: unix_primary_group = yes
```

Seja qual for a configuração que você use, o grupo (ou grupos) definido como o grupo primário dos usuários deve ter o conjunto de atributos gidNumber. Por exemplo, se você usar apenas o grupo Domain Users como grupo primário para todas as contas, o grupo Domain Users deve ter um conjunto de atributos gidNumber. Winbind é incapaz de mapear contas que usam grupos primários que não possuem o conjunto de atributos gidNumber.

- Agora recarregue as configurações

```
smbcontrol all reload-config
```

Vantagens e Desvantagens do ‘rid’ Back End

- Vantagens:
  - Fácil de configurar.
  - Os IDs usados são rastreados automaticamente.
  - Requer apenas acesso de leitura aos controladores de domínio.
  - Todas as contas e grupos de usuários do domínio estão automaticamente disponíveis no membro do domínio.
  - Nenhum atributo precisa ser definido para usuários e grupos de domínio.

- Desvantagens
  - Todos os usuários do membro do domínio obtêm o mesmo shell login e o caminho base do diretório home.
  - Se os mesmos intervalos de identificação estiverem configurados para o domínio ,as IDs de usuário e de grupo são as mesmas em outros membros do domínio usando o back-end ‘rid’, Todas as contas e grupos estão automaticamente disponíveis no membro do domínio e as entradas individuais não podem ser excluídas.
  - Não recomendado para ambientes multi-domínio porque objetos em diferentes domínios com o mesmo identificador relativo (RID) obtêm a mesma ID atribuída.

Configurando o ‘rid’ Back End

- Configure o seguinte na seção [global] do seu arquivo smb.conf:

```
idmap config * : backend = tdb
idmap config * : range = 3000-7999
idmap config DOMINIO:backend = rid
idmap config DOMINIO:range = 10000-999999
winbind nss info = template
template shell = /bin/bash
template homedir = /home/%U
```

- Agora recarregue as configurações

```
smbcontrol all reload-config
```

Vantagens e Desvantagens do ‘autorid’ Back End

- Vantagens:
  - Todos os usuários e grupos de domínio cujo UID e GID calculado ,estão dentro do intervalo configurado estão automaticamente disponíveis no membro do domínio.
  - Não é necessário atribuir manualmente IDs, diretórios home e shells de logon.
  - Não há IDs duplicados, mesmo que múltiplos objetos em um ambiente multi-domínio tenham o mesmo RID.
  -

- Desvantagens:
  - IDs de usuário e grupo não são iguais em todos os membros do domínio Samba.
  - Todos os usuários do domínio obtêm o mesmo log de login e o diretório home atribuídos. No entanto, você pode usar variáveis.
  - Não é possível excluir que usuários ou grupos individuais estejam disponíveis no membro do domínio, exceto que o UID calculado ou o GID esteja fora do intervalo configurado.

Configurando o ‘autorid’ Back End

- Configure o seguinte na seção [global] do seu arquivo smb.conf:

idmap config * : backend = autorid
idmap config * : range = 10000-24999999
idmap config * : rangesize = 200000 (opicional)
template shell = /bin/bash
template homedir = /home/%U

- Agora recarregue as configurações

```
smbcontrol all reload-config
```

Resumindo

- Para escolher o melhor Back end para você, leve em consideração as vantagens de desvantagens de cada um , para então tomar uma decisão . Na dúvida use o back end ‘ad’ onde fica tudo centralizado no AD
-

Nenhum dos backends usados aqui podem ser usados em controladores de domínio samba . Somente em servidores membros.

Links úteis

...

- Saiba mais sobre backend idmap

https://wiki.samba.org/index.php/Identity_Mapping_Back_Ends

Prática

...