Configurando o Samba como Membro do Domínio...

Introdução

- Um membro do domínio Samba é uma máquina Linux ingressada ao domínio que está executando o Samba e não fornece serviços de domínio, como um controlador de domínio.
- O que você pode fazer com um membro de domínio:
  - Use usuários de domínio e grupos em ACLs locais em arquivos e diretórios.
  - Configurar compartilhamentos para atuar como um servidor de arquivos.
  - Configurar os serviços de impressão para atuar como um servidor de impressão.
  - Configurar o PAM (Pluggable Authentication Module) para permitir que usuários de domínio façam login localmente ou autentiquem em serviços instalados locais.

Preparação

- Verifique se nenhum processo do Samba está sendo executado se tiver pare todos:

```
ps ax | egrep "samba|smbd|nmbd|winbindd"
```

- Se você já executou anteriormente uma instalação do Samba neste host remova o arquivos smb.conf
- Remova todos os arquivos de banco de dados do Samba, como *.tdb e *.ldb Para listar as pastas que contêm bancos de dados Samba execute:

```
smbd -b | egrep "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR"
```

- Configure o arquivo resolv.conf e aponte para o ip do AD samba

```
nameserver 10.99.0.1
search nomedoseudominio.com
```

- Configure (se não existir crie) o arquivos /etc/krb5.conf com o seguinte conteúdo

```
[libdefaults]
    default_realm = SEUDOMINIO.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

A equipe do Samba NÃO recomendam que se estabeleçam parâmetros adicionais no arquivo /etc/krb5.conf

- Configurando Sincronização de Tempo - O Kerberos requer o tempo sincronizado em todos os membros do domínio. Portanto, é recomendável configurar um cliente NTP. Instale o ntp como comando

```
apt-get install ntp
```

- Configure o arquivo ntp apontando para os DCs da sua rede , como no exemplo a seguir .

```
# Local clock. Note that is not the "localhost" address!
server 127.127.1.0
fudge  127.127.1.0 stratum 10

# Where to retrieve the time from
server DC1.seudominio.com     iburst prefer
server DC2.seudominio.com     iburst

driftfile /var/lib/ntp/ntp.drift
logfile   /var/log/ntp

# Access control
# Default restriction: Disallow everything
restrict default ignore

# No restrictions for "localhost"
restrict 127.0.0.1

# Enable the time sources only to only provide time to this host
restrict DC1.samdom.example.com   mask 255.255.255.255    nomodify notrap nopeer noquery
restrict DC2.samdom.example.com   mask 255.255.255.255    nomodify notrap nopeer noquery
```

Seu NTP sincroniza o tempo com os controladores de domínio Samba Active Directory DC1 e DC2 e não fornece serviços de tempo para outros hosts.

- Configure o arquivos hosts

```
127.0.0.1   localhost
10.99.0.5   servidor.meudominio.com servidor
```

- Para verificar se o seu nome de host resolve corretamente, use o comando `getent`

```
 getent hosts servidor
10.99.0.5 servidor.meudominio.com servidor
```

- O nome do host e o FQDN não devem resolver o endereço IP 127.0.0.1 ou qualquer outro endereço IP diferente do usado na interface LAN do membro do domínio.
- Se nenhuma saída for exibida ou o host for resolvido para o endereço IP errado e você não estiver usando dhcp, defina a entrada correta no arquivo /etc/hosts.

- Se você estiver usando dhcp, verifique se /etc/hosts apenas contém a linha '127.0.0.1' apontada para localhost.
- Se continuar a ter problemas, ajuste o seu DHCP.
- Nos sistemas relacionados com Debian, você também verá a linha

```
127.0.1.1 hostname
```

em / etc / hosts, remova-o antes de instalar o samba.

- Instale o Samba compilado como já visto em aula já ministrada

- Configurando um arquivo smb.conf básico

```
[global]

        security = ADS
        workgroup = SEUDOMINIO
        realm = SEUDOMINIO.COM
        log file = /var/log/samba/%m.log
        log level = 1
        idmap config * : backend = tdb
        idmap config * : range = 3000-7999
       idmap config *: backend = tdb
       idmap config *: range = 3000-7999
```

- Mapear a Conta do Administrador de domínio para o Usuário Local root
- Adicione o seguinte parâmetro à seção [global] do seu arquivo smb.conf:

```
[global]

        security = ADS
        workgroup = SEUDOMINIO
        realm = SEUDOMINIO.COM
        log file = /var/log/samba/%m.log
        log level = 1
        idmap config * : backend = tdb
        idmap config * : range = 3000-7999
        idmap config *: backend = tdb
        idmap config *: range = 3000-7999
        username map = /usr/local/samba/etc/user.map
```

- Crie o arquivo /pasta de instalação/samba/etc/user.map com o seguinte conteúdo:

```
!root = DOMINIO\Administrator
```

Não configure o atributo uidNumber para a conta de administrador do domínio. Se a conta tiver o conjunto de atributos, o valor substituirá o UID local 0 do usuário root e, assim, o mapeamento falhará.

- Ingresse ao domínio

```
net ads join -U administrator
```

Não ingresse um membro do domínio usando o samba-tool. Essas opções não são suportadas e podem causar problemas com sua replicação AD. As opções serão removidas do samba-tool em uma versão futura.

- Configurar o nssswitch

Para habilitar a biblioteca de chave de serviço de nome (NSS) para tornar usuários e grupos de domínio disponíveis para o sistema local:

- Edite o arquivo /etc/nsswitch.conf e coloque o parametro winbind dessa forma :

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

Não use os mesmos nomes de usuário no arquivo /etc/passwd local como no domínio.

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

Sistemas operacionais baseados em Debian 32 e 64 bits

```
ln -s /pasta de instalação/samba/lib/libnss_winbind.so.2 /lib64/
ln -s /lib64/libnss_winbind.so.2 /lib64/libnss_winbind.so
ldconfig
```

- Iniciando os Serviços

Inicie o serviço winbindd para habilitar a biblioteca do NSF (service service) para pesquisar usuários e grupos de domínio:

```
winbindd
```

Se você for configurar compartilhamentos de arquivos ou serviços de impressora no membro do domínio, suba também os serviços smb nmbd:

```
smbd
nmbd
```

Você não deve iniciar o serviço samba em um membro do domínio. Este serviço é necessário apenas em controladores de domínio do Active Directory (AD) (DC).

- Testando a conectividade Winbindd

Para verificar se o serviço Winbindd pode se conectar aos Controladores de Domínio (DC) do Active Directory (AD) ou a um controlador de domínio primário , digite:

```
wbinfo --ping-dc
```

Se o comando anterior falhar, verifique:

Que o serviço `winbindd` está funcionando.
Seu arquivo `smb.conf` está configurado corretamente.

- Testando a conectividade Winbindd

Para verificar se o serviço Winbindd pode se conectar aos Controladores de Domínio (DC) do Active Directory (AD) ou a um controlador de domínio primário , digite:

```
wbinfo --ping-dc
```

Se o comando anterior falhar, verifique:

Que o serviço `winbindd` está funcionando.
Seu arquivo `smb.conf` está configurado corretamente.

Links úteis

...

- Solução de problemas de membros do domínio do Samba

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

Prática

...