

17. SAMBA



17.1.- Introducción

Samba es un conjunto de programas creados por Andrew Tridgell, actualmente mantenidos por *The Samba Team* bajo licencia GNU y que, desde 1992, implementan en sistemas Linux/Unix el protocolo SMB. Samba permite integrar sistemas Linux/Unix en entornos Active Directory.

Usando Samba los sistemas Linux/Unix pueden proporcionar servicios a los clientes Microsoft Windows y a sistemas Unix/Linux o bien actuar como clientes en redes Microsoft. Para los sistemas Windows los recursos Samba aparecerán como carpetas de red normales y en los sistemas Linux/Unix se montará en un sistema de archivos local el recurso Samba o accederán a él utilizando el comando *smbclient* de forma similar a cómo funciona *ftp*.

Samba implementa el protocolo SMB (Server Message Block) y CIFS (Common Internet File System), dialecto de SMB. A menudo ambos nombres SMB y CIFS se utilizan de forma indistinta. SMB es un protocolo de nivel de red de modelo OSI creado en 1985 por IBM y renombrado a CIFS en 1998 por Microsoft tras incluir modificaciones como el soporte para enlaces simbólicos y físicos y soporte para archivos de gran tamaño. Pese a que inicialmente fue diseñado para trabajar sobre NETBEUI, IPX/SPX o NBT también puede trabajar directamente sobre TCP/IP.

Al igual que en NFS, tenemos dos partes: la parte servidor y la parte cliente.

17.2.- Autenticación en un recurso SMB

El servidor SMB normalmente restringe los accesos a unos usuarios y/o grupos específicos, luego hay que proporcionar al montar el sistema de archivos SMB dichas credenciales como una opción más del montaje.

Se puede poner la opción de montaje *username=<usuario>* y tras ejecutar el comando *mount* pedirá la contraseña o proporcionar además del usuario, la contraseña con *password=<pass>*. Otra forma sería poner las credenciales de acceso en un fichero con el contenido:

```
username=<user>
password=<pass>
domain=<dominio>
```

y con la opción de montaje *credentials=<fichero>* (también se puede usar la abreviatura *cred*) proporcionar dichas credenciales. Dicho fichero debe estar en una ruta con acceso sólo para root o tener los permisos 600.

Para gestionar los usuarios Samba en los servidores Linux que hagan de servidores Samba, hay que crear un usuario en el sistema, preferiblemente con shell */bin/nologin* o */bin/false* para sólo permitir el uso como usuario Samba y luego asignarle contraseña Samba con el comando *smbpasswd* disponible en el paquete *samba-common-tools*. La contraseña Samba no tiene porqué ser igual a la del sistema.

Opciones disponibles del comando *smbpasswd*:

***smbpasswd* <user>**: le doy otra contraseña al usuario Samba existente <user>.

***smbpasswd -a* <user>**: añade el usuario <user> como usuario Samba y le da contraseña.

***smbpasswd -x* <user>**: borra la cuenta samba del usuario <user>.

Con el comando *pdbedit -L* puedo ver los usuarios del sistema que además son usuarios Samba.

17.3.- Configuración en el servidor Samba

Los pasos a seguir son:

- 1.- Instalar el paquete ***samba***, gracias al cual un servidor Linux es capaz de actuar como servidor de recursos compartidos SMB. Dicho paquete está incluido en el grupo de paquetes ***file-server***.
- 2.- Crear el directorio a exportar. No se puede compartir un recurso por NFS y Samba a la vez, ya que su funcionamiento es distinto, p.e. tienen distintos mecanismos de bloqueo, si lo hiciéramos habría corrupción de datos.
- 3.- Configuración de Samba usando el fichero ***/etc/samba/smb.conf***:

Las líneas que comienzan por # o ; son comentarios.

Cada sección en este fichero comienza por el nombre de la sección entre [] y seguido de la lista de parámetros y sus valores.

La primera sección es *[global]* donde aparece la configuración general del servidor

Hay tres cosas a configurar:

- ***workgroup=<grupo>***: grupo de trabajo al que pertenece el servidor. Da igual mayúsculas que minúsculas y su longitud debe ser hasta 12 caracteres alfanuméricos.
- ***security=user***: los clientes deben tener usuario y contraseña que gestiona el servidor SMB.
- ***Host allow= list***: lista de control de acceso. Es una lista de host separados por coma, espacio o tabulador que pueden tener acceso al servidor SMB. Esto se puede configurar en cada recurso o aplica lo que se defina en la sección global. Los *host* se pueden indicar con una IP o un rango de red. Si no se pone nada, cualquier host tendría acceso.

A continuación vienen la secciones de recursos que se indica de la forma:

[nombre_recurso]: El nombre del recurso debe ser de hasta 12 caracteres alfanuméricos de longitud.

comment=<comentario>: descripción del recurso.

path=<dir_exportado_smb>: directorio donde está el recurso en el servidor.

writable=yes|no: si se pone a *yes*, los usuarios autenticados tendrán acceso de escritura y si se pone *no*, sólo tendrán acceso de lectura, salvo que aparezcan en la lista de *write list*.

browseable=yes|no: define si se permite mostrar el recurso en las listas de recursos.

readonly=yes|no: si se pone a *yes* es lo mismo que *writable=no* y a la inversa.

write list: lista de usuarios o grupos separados por comas con permisos de escritura si se configuró *writable* a *no*. Los grupos se indican con una *@* delante de su nombre.

valid users: lista de usuarios o grupos separados por comas que tiene acceso al recurso. Si está en blanco, todos los usuarios autenticados tienen acceso.

La sección de *[homes]* es especial, hace que los directorios home de los usuarios del sistema estén disponibles por SMB. Se necesita activar el *booleano* de SELinux *samba_enable_home_dirs*. Otra cosa es el *booleano use_samba_home_dirs* que hace que el recurso samba pueda ser montado como *homedir* de Linux.

Una vez realizados los cambios en el fichero de configuración, se puede verificar su sintaxis con el comando *testparm*.

- 4.- Abrir el firewall para permitir los accesos por SMB: los puertos que utiliza Samba son *445/tcp*, *137/udp*, *138/udp* y *139/tcp*. Existe un servicio predefinido en FirewallD que se llama *samba*.

5.- Configuración SELinux:

El contexto SELinux para ficheros y directorios *samba_share_t* permite a Samba acceso de lectura y escritura.

También se puede utilizar el contexto *public_content_t* pero sólo garantiza la lectura. Para permitir también la escritura en el recurso exportado, el contexto *public_content_t* se debe cambiar por *public_content_rw_t* y activar el *booleano smbd_anon_write*.

Otros booleanos interesantes son *samba_export_all_rw* que permite compartir todos los recursos en modo lectura y escritura y *samba_export_all_ro* que permite compartir todos los recursos en modo sólo lectura.

6.- Arranque y activación del servicio *smb* y *nmb*. Samba periódicamente chequea el fichero */etc/samba/smb.conf* y si ha habido cambios en la configuración, Samba los recarga. Esto no afecta a las conexiones ya establecidas. Aun así, si se quiere recargar los servicios nada más modificar el fichero de configuración, se puede hacer un *systemctl reload smb nmb* o incluso reiniciar por completo el servicio con *systemctl restart smb nmb*.

17.4.- Configuración en el cliente Samba

Se necesita tener instalado el paquete *cifs-utils* para poder montar recursos SMB. El comando *mount* y el servicio *autofs* se apoyan en este paquete para montar sistemas de archivos CIFS.

Existe otro paquete que, pese a no ser obligatorio instalarlo, si es recomendable: *samba-client*, ya que contiene algunas utilidades como *mbclient* que nos ayudan a identificar los recursos exportados por el servidor SMB.

Pasos a seguir:

1.- Identificar los recursos exportados por el servidor Samba:

Usando el comando *mbclient* con la opción *-L* e indicando con *//* delante el nombre del servidor, listaremos los recursos que exporta por SMB siempre que el servidor no haya marcado como no *browseable* los recursos; en ese caso el recurso es accesible de forma explícita pero no se puede listar.

2.- Crear el punto de montaje local donde se montará el recurso exportado por SMB. En el caso de usar automonter para montar el recurso remoto, este paso no es necesario, lo creará automonter cuando se acceda al recurso.

3.- Montar el recurso remoto.

Al igual que en NFS, se puede hacer de forma manual con el comando *mount*, de forma persistente con un montaje automático en el fichero */etc/fstab* o con automonter.

→ Manual: usaremos el comando *mount* de la forma:

```
mount -t cifs -o <ops> //<server_smb>/<recurso_smb> <pto_montaje>
```

donde:

<server_smb>: sistema remoto que hace de servidor SMB.

<recurso_smb>: directorio que exporta el servidor SMB.

<pto_montaje>: punto de montaje local creado en el punto anterior.

<ops>: opciones de montaje. Pueden ser:

- *guest* si quiero acceder con una cuenta sin permisos.

- `username=<user>` para acceder con una cuenta Samba y su contraseña asociada que me pedirá tras ejecutar comando mount.
- `username=<user>,password=<pass>` para acceder con una cuenta Samba facilitando directamente la contraseña.
- `credentials=<fich>` donde fich contiene las credenciales.

→ Automático: usando el fichero `/etc/fstab`: donde se añade una línea por recurso remoto con el formato:

```
//<server_smb>/<recurso_smb> <pto_montaje> cifs <ops> 0 0
```

donde:

`<server_smb>`: sistema remoto que hace de servidor SMB.

`<recurso_smb>`: directorio que exporta el servidor SMB.

`<pto_montaje>`: punto de montaje local creado en el punto anterior.

`<ops>`: opciones de montaje. Las mismas usadas en el montaje manual.

→ Automonter: usando el servicio `autofs` que de forma automática monta bajo demanda recursos SMB compartidos y los desmonta cuando no están en uso.

→ Pasos para crear un automontaje:

1.- Instalar el paquete `autofs` en el cliente SMB.

2.- Añadir un fichero de mapeo principal en `/etc/auto.master.d/`

Fichero con extensión `.autofs`. En este fichero añadir una entrada de mapeo de la forma:

- para mapeo indirecto: `/<dir> /etc/auto.<detalles_montaje>`
- para mapeo directo: `/- /etc/auto.<detalles_montaje>`

3.- Crear el fichero con los detalles del montaje con el nombre `auto.<detalles_montaje>` en `/etc` con la línea:

- para mapeo indirecto: `* - <ops> ://<server_smb>/<recurso_smb>/&`
- para mapeo directo: `<pto_montaje> - <ops> ://<server_smb>/<recurso_smb>`

donde:

`<server_smb>`: es el sistema remoto que hace de servidor SMB.

`<recurso_smb>`: nombre del recurso que exporta el servidor SMB.

`<pto_montaje>`: punto de montaje local que no hace falta que exista previamente.

`<ops>`: opciones de montaje. Iguales a las vistas en el montaje manual y debemos añadir la opción `fstype=cifs` para indicar que es un montaje de Samba y `domain=<dominio>` para indicar el nombre del grupo de trabajo de Windows.

4.- Arrancar y activar el servicio *autofs* en el cliente Samba.

17.5.- Caso práctico

Tenemos el sistema **central** que hará de servidor Samba exportando el recurso */shares/iwin* con el nombre *infowin* para que los sistemas de su propia red puedan tener acceso de lectura y escritura y el sistema con la IP *172.25.6.18* sólo tenga acceso de lectura y el recurso */shares/cwin* con el nombre *corpwin* con acceso de sólo lectura para cualquier red. Se configurará Samba para que el acceso a los archivos se base en los permisos estándar Linux, exporte los contextos de SELinux adecuados y se abrirá el *firewall* para poder permitir el acceso de los clientes.

Como cliente Samba, el sistema **server1** montará en su sistema de archivos local */datoswin* el recurso exportado por el sistema **central** llamado *corpwin* con la información accesible para toda la organización usando automonter y el recurso *infowin* de **central** de forma automática en */remotowin*.

RESOLUCIÓN

→ Configuración como servidor Samba de **central**:

- Instalamos el paquete *samba*:

```
[root@central ~]# yum install -y samba
```

- Creamos los directorios a exportar */shares/cwin* y */shares/iwin*:

```
[root@central ~]# mkdir -p /shares/{c,i}win
```

```
[root@central ~]# chown nfsnobody /publico
```

- Configuración en el archivo */etc/exports*:

```
[root@central ~]# echo '/publico 172.25.1.0/24(rw) 172.25.6.18(ro) ' >> /etc/exports
```

```
[root@central ~]# exportfs -r (no es necesario ya que aun no se ha arrancado el servicio)
```

- Configuramos el firewall:

```
[root@central ~]# firewall-cmd --permanent --add-service=samba
```

```
[root@central ~]# firewall-cmd --reload
```

- Configuramos SELinux: Añado a las políticas de SELinux que los directorios */shares/cwin* y */shares/iwin* tengan el contexto adecuado. Vamos a utilizar el contexto SELinux *samba_share_t* para */shares/iwin* y el contexto *public_content_t* para */shares/cwin* permitiendo el acceso de lectura y escritura en el primero y de sólo lectura en el segundo.

```
[root@central ~]# semanage fcontext -a -t samba_share_t '/shares/iwin(/.*)?'
```

```
[root@central ~]# semanage fcontext -a -t public_content_t '/shares/cwin(/.*)?'
```

```
[root@central ~]# restorecon -vvFR /shares
```

- Arrancamos y activamos los servicios *smb* y *nmb*:

```
[root@central ~]# systemctl start smb nmb; systemctl enable smb nmb
```

- Configuración de **server1** como cliente NFS:

- Instalamos el paquete *nfs-utils* (ya realizado en el punto anterior) y el paquete *autofs*:

```
[root@server1 ~]# yum install -y autofs
```

- Creamos los directorios locales **corporativo** y **folletos**:

```
[root@server1 ~]# mkdir /{corporativo,folletos}
```

- Para el montado automático del recurso **marketing** del servidor NFS **general** con el archivo */etc/fstab*, añadimos la siguiente línea:

```
[root@server1 ~]# echo 'general:/marketing /folletos nfs sync,sec=sys,v4.2 0 0'  
>>/etc/fstab
```

- Para el montado indirecto del recurso **corp** usando automonter, creamos el fichero de mapeo principal con la configuración que apunta al fichero con la descripción del montaje:

```
[root@server1 ~]# echo '/corporativo /etc/auto.corporativo' >  
/etc/auto.master.d/corporativo.autofs
```

y creamos el fichero con la descripción del montaje:

```
[root@server1 ~]# echo '* -rw,sync,sec=v4.2 general:/corp/&' > /etc/auto.corporativo
```

- Arrancamos y activamos el servicio *autofs*:

```
[root@server1 ~]# systemctl start autofs; systemctl enable autofs
```