

---

# Unidad 10: Sistemas de archivos en red

**Curso de introducción a la administración de servidores GNU/Linux**

**Centro de Formación Permanente  
Universidad de Sevilla**

Enrique Ostúa, Jorge Juan <jjchico@dte.us.es> 2010, 2011, 2012, 2013

Usted es libre de copiar, distribuir y comunicar públicamente la obra y de hacer obras derivadas bajo las condiciones de la licencia Attribution-Share alike de Creative Commons.

Puede consultar el texto completo de la licencia en <http://creativecommons.org/licenses/by-sa/3.0/>

## Contenidos

---

- Acceso remoto a archivos
- NFS
- Samba

# Acceso remoto a archivos

---

- Servidor de archivos: ordenador dedicado a almacenar archivos y carpetas a los que se puede acceder remotamente
  - Contemplan la conexión por parte de distintos usuarios
  - Gestionan los permisos de cada usuario
  - Ejecutan algún tipo de servicio que permite la conexión remota y la transferencia o acceso a los archivos
- Métodos de acceso a archivos
  - SSH
  - Network File System (NFS)
  - Samba (CIFS)
  - File Transfer Protocol (FTP)
  - WebDAV

3

# Acceso remoto a archivos

---

- SSH
  - El servidor de shell remoto ssh permite la transferencia de archivos con varios métodos
  - scp: comando para transferencia de archivos
    - `$ scp carta.txt mipc.casa.org:doc/`
  - SFTP: servicio FTP seguro. Clientes SFTP
    - `sftp://mipc.casa.org/home/pepe/doc`
    - WinSCP ([winscp.org](http://winscp.org)): cliente para MS-Windows(TM)
  - GNOME dispone de módulos para acceso a archivos a través de SSH/SFTP
    - Nautilus: Archivo -> Conectar con el servidor...
    - URL's `ssh://...` o `sftp://...` en aplicaciones GNOME
  - sshfs: permite 'montar' carpetas remotas mediante ssh

4

# Acceso remoto a archivos

---

- Network File System (**NFS**). Sistema de archivos en red
  - Permite 'montar' carpetas compartidas en sistemas remotos y usarlas como si se tratara de carpetas locales
  - Característico de sistemas UNIX
  - Suele combinarse con una gestión centralizada de múltiples ordenadores mediante **NIS**:
    - mismos usuarios
    - mismas claves
    - mismos programas instalados
    - etc.
  - Adecuado para configuraciones fijas hechas por el administrador
  - Inadecuado para conexiones esporádicas hechas por los usuarios

5

# Acceso remoto a archivos

---

- Samba
  - Paquete que implementa el protocolo CIFS para acceso a archivos e impresoras en red
  - Compatible con protocolos de compartir de red de MS-Windows(TM): NetBIOS
  - Samba puede actuar como servidor de archivos e impresoras para redes MS-Windows(TM)
  - Cada equipo puede pertenecer a un “grupo de trabajo” o a un “dominio”
    - Grupo de trabajo: no controlado, a elección del usuario
    - Dominio: controlado, configurado en un servidor de dominios

6

# Network File System (NFS)

---

- El servidor NFS exporta unos directorios y los clientes los pueden montar y trabajar con ellos como si fueran locales
- No hay autenticación, sólo control por IP
- Los cambios se realizarán en el servidor de forma automática y se reflejan en ambos sitios
- El uid/gid en el cliente coincide con el del servidor, pero pueden estar asignados a usuarios/grupos diferentes.
- Una buena organización de usuarios grupos y permisos es muy importantes para poder trabajar bien.
- El *root* del cliente, por defecto, no tiene permisos de root en el directorio montado

## RPC y portmap

---

- *RPC: Remote Procedure Call*
- RPC es un protocolo por el que se pueden ejecutar llamadas a determinadas funciones de forma remota (a otros equipos), sin preocuparse de la forma de comunicación (número de puerto, etc.)
- RPC fue diseñado por Sun y muy utilizado en sistemas UNIX 'clásicos'
- Los servicios RPC utilizan unos demonios propios para establecer la comunicación
- Estos demonios, al lanzarse, se “registran” en *portmap*
- Servicio: “portmap”
- /etc/default/portmap
- /etc/default/rpcbind

# El servidor NFS

---

- NFS es un servicio que trabaja a través de RPC
- Los demonios que se usan en el servidor NFS:
  - rpc.mountd: controla el montaje de directorios
  - rpc.nfsd: controla la exportación de archivos
  - rpc.lockd: controla el bloqueo de archivos
  - rpc.statd: recuperación de archivos en caso de fallo
- Ellos se registran en el demonio 'portmap' local
- El cliente NFS se conectará al servicio portmap para pedirle el acceso a los demonios de NFS

# Instalación de NFS

---

- Dos versiones del servidor:
  - nfs-kernel-server: necesita que el kernel tenga instalado el soporte para nfs (p.e. por módulos)
  - nfs-user-server: no usa ningún recurso del kernel, tiene un rendimiento algo menor.
- Ambos funcionan de forma similar
- En ubuntu podemos usar cualquiera, así que nos decidimos por instalar nfs-kernel-server por su mejor rendimiento
- Servicio: nfs-kernel-server

# Configuración. /etc/exports

---

```
/opt          master(rw) trusty(rw,no_root_squash)
/projects     proj*.linux.curso(rw)
/usr         *.linux.curso(ro) 10.1.15.120(rw)
# mapea el acceso al HOME de JOE de "cualquier usuario" a JOE
/home/joe     pc001(rw,all_squash,anonuid=150,anongid=100)
# carpeta de acceso publico, solo-lectura
/pub         (ro)
```

# Configuración. /etc/exports

---

- La lista de directorios exportados se almacena en /etc/exports, con un formato sencillo.
- Los permisos y opciones se indican con el formato:
  - cliente(opciones)
- Los "cliente" pueden ser una IP, nombre de máquina, IP/máscara o dominio con comodines (Ej: \*.curso.linux)
- Las opciones se separan por comas y se aplican al cliente correspondiente
- Al cambiar algo se ejecutará:
  - # exportfs -ra
- Más información:
  - man exports

# Opciones de exports

---

- rw, ro: exporta lectura-escritura o sólo lectura
- async o sync: escrituras asíncronas o síncronas
- (in)secure: sólo root puede montar en el cliente (secure) o cualquiera (insecure)
- mountpoint=path: sólo exporta si path es un punto de montaje y está montado (en el servidor)
- (no\_)root\_squash: mapea (o no) el usuario root como usuario nobody en el servidor
- (no\_)all\_squash: mapea (o no) todos los usuarios como usuario nobody en el servidor
- anonuid=65534 y anongid=65534: el uid/gid del usuario anónimo en el servidor
- (no\_)subtree\_check: comprueba (o no) pertenencia a carpeta compartida (normalmente no).

# Comprobación y control

---

- rpcinfo -p
  - Comprobar servicios RPC
- showmount -a
  - Comprobar clientes conectados
- exportfs -ra
  - Actualizar lista de carpetas compartidas
- service nfs-kernel-server start/stop/restart
  - Control del servidor

# Cliente

---

- Paquete: nfs-common
  - instala portmap automáticamente
- mount -t nfs
  - opción para montar carpetas compartidas por NFS

```
# mount -t nfs servidor:ruta_en_servidor punto_de_montaje
```

## Ejemplo NFS

---

```
# /etc/exports
/srv/share      10.1.15.120(rw,sync,no_subtree_check) \
                10.1.15.0/24(ro,sync,no_subtree_check)
```

```
# servidor
exportfs -ra
```

```
# cliente
mount -t nfs 10.1.15.124:/srv/share /mnt

touch /mnt/test_xxx.txt
ls /mnt
mount
...
```



# Samba

---

- Implementa el protocolo CIFS para acceso a archivos e impresoras en red
- Compatible con protocolos de compartir de red de MS-Windows(TM): NetBIOS
  - Samba puede actuar como servidor de archivos e impresoras para redes MS-Windows(TM)
- Cada ordenador tiene un nombre netbios independiente del nombre DNS (recomendado que coincidan)
- Cada usuario tiene una clave independiente de la del sistema para acceder a recursos compartidos (recomendado que coincidan)
- Cada equipo puede pertenecer a:
  - Grupo de trabajo: no controlado, a elección del usuario
  - Dominio: controlado, servidor de dominios

17

# Browsing

---

- Formato URL
  - Windows: \\ordenador\recurso
  - Samba: //ordenador/recurso
- Localización de recursos cooperativa y descentralizada
  - Local browser, master browser, etc.
- Servidores Wins

18

# Samba: funciones

---

- Compartir carpetas (servidor de archivos)
- Compartir impresoras
- Servidor WINS
- Servicio de autenticación: Domain Controller
- Directorio Activo (experimental)

19

## Samba. Ejemplo

---

- Servidor de archivos para múltiples usuario
  - Compartir carpetas de usuarios
- Servidor de archivos público
- Autenticación de clientes Windows
  - Primary Domain Controller
  - Autenticación centralizada

20

# Permisos

---

- Samba respeta los permisos de archivos y carpetas en el sistema de archivos
- Los permisos deben ajustarse a los privilegios que se deseen para el usuario que se conecta
- Permisos de archivos y carpetas creados con samba:
  - create mask; force create mode
  - directory mask; force directory mode
- Hay opciones para forzar ciertos permisos (admin users) pero debe limitarse su uso.

21

# Samba. Claves de usuario

---

- Añadir una clave samba para un usuario
  - # smbpasswd -a <usuario>
- Cambiar la clave samba de un usuario
  - # smbpasswd <usuario>
- Deshabilitar la clave de un usuario
  - # smbpasswd -d <usuario>
- Habilitar la clave de un usuario
  - # smbpasswd -e <usuario>
- Borrar la clave de un usuario
  - # smbpasswd -x <usuario>

22

# Instalación

---

- Instalación
  - # apt-get install samba
- Configuración por defecto
  - Grupo de trabajo: MSHOME
  - Nombre NetBIOS: el mismo que DNS
  - Carpetas de usuarios compartidas (no publicadas)
    - Recurso: \\<ordenador>\<usuario>
    - <ordenador>: NetBIOS, nombre DNS o dirección IP
    - Sólo lectura
  - Se comparten impresoras instaladas
  - Los usuarios no tienen clave para samba inicialmente
- /etc/samba/smb.conf: archivo de configuración

23

## Samba. Configuración básica

---

- Editar archivo /etc/samba/smb.conf
- Cambiar parámetros de configuración
- Comprobar configuración ejecutando 'testparm'
- Reiniciar el servidor (o recargar configuración)
  - restart nmbd; restart smbd
- En caso de errores
  - /var/log/samba/log.{nmbd,smbd}
- Cambiar grupo de trabajo
  - workgroup = <nombre\_grupo>
- Operar como servidor WINS
  - wins support = yes
- Usar un servidor WINS
  - wins server = <dir\_ip\_servidor\_wins>

24

# Samba. Configuración básica

---

- Ejemplo

```
[global]
workgroup = CURSO
# wins support = no
; wins server = w.x.y.z
# domain master = auto
```

25

# Samba. Comprobación

---

- smbclient
  - smbclient -L maquina
  - smbclient //maquina/recurso
  - smbclient -U usuario ...
- Nautilus
  - Ir → Lugar (Ctrl-L)
    - smb://maquina/recurso
  - Ir → Red → Red de Windows

26

# Ejemplo: carpetas de usuarios

---

- Servidor de archivos
  - Permitir acceso de lectura/escritura a las carpetas de usuario
  - Los usuarios se conectarán usando una clave
  - Clientes Windows/Linux

```
[homes]
comment = Home Directories
browseable = yes
read only = no
create mask = 0660
directory mask = 0770
valid users = %S
```

27

# Ejemplo: carpeta Web

---

- Compartir una carpeta con los contenidos de la web
  - Acceso a los archivos servidos por la web para su edición
  - Archivos y carpetas con permiso de escritura para el grupo
  - Archivos y carpetas heredan el grupo de carpeta padre

```
[web]
comment = Contenidos Web
path = /var/www
browseable = yes
writable = yes
create mask = 0664
force create mode = 0664
directory mask = 2774
force directory mode = 2774
```

28

# Ejemplo: carpeta pública

---

- Crear una carpeta compartida pública
  - Pueden conectarse todos los usuarios
  - Tendrá acceso sólo de lectura, salvo para los miembros del grupo 'admin'
  - Acceso limitado a ciertos ordenadores

```
[share]
comment = Carpeta pública
path = /srv/share
browseable = yes
guest ok = yes
read only = yes
admin users = @admin
deny hosts = ALL
allow hosts = 10.1.15. mipc.casa.com .us.es
```

29

# Ejemplo: primary domain controller (PDC)

---

- Ventajas
  - Centralización de autenticación (Single Sign On)
  - Centralización de archivos
  - Centralización de preferencias
- Requisitos
  - Compartir carpetas de usuarios
  - Configuración del dominio: rutas y BD de máquinas
  - Carpeta para servicio de autenticación
  - Carpeta para almacenar preferencias de los usuarios (puede ser en la misma carpeta del usuario)
  - Grupo de máquinas controladas (machines)
  - Usuario y grupo administrador windows (Domain Admins)
  - Asignar privilegios a grupo de administradores

30

# PDC

---

- Referencias

- <https://help.ubuntu.com/12.04/serverguide/samba-dc.html>
- <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html>

31

## PDC. Configuración dominio

---

```
##### Domains #####  
  
domain logons = yes  
logon path = \\%N%\%U\profile  
logon drive = H:  
logon home = \\%N%\%U  
logon script = logon.cmd
```

```
add machine script = /usr/sbin/useradd -g machines \  
-c "%u machine account" -d /var/lib/samba -s /bin/false %u  
  
sudo addgroup --system machines
```

32



# PDC. Servicio autenticación

---

```
#### Misc ####

[netlogon]
comment = Network Logon Service
path = /srv/samba/netlogon
guest ok = yes
read only = yes
; share modes = no (deprecated)
```

```
sudo mkdir -p /srv/samba/netlogon
sudo touch /srv/samba/netlogon/logon.cmd

sudo restart smbd
sudo restart nmbd
```

33

# PDC. Administrador Windows

---

```
# Crear usuario y grupo para administradores Windows

adduser --system sysadmin
addgroup --system sysadmin
adduser sysadmin sysadmin
adduser sysadmin admin
smbpasswd -a sysadmin
```

```
# Asignar varios privilegios

net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d

net rpc rights grant -U sysadmin "CURSO\Domain Admins" \
SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege \
SeDiskOperatorPrivilege SeRemoteShutdownPrivilege
```

34

# PDC. Configuración clientes

---

- Unir al dominio
  - Mi PC -> Propiedades -> Nombre de equipo -> Cambiar
    - Dominio: CURSO
    - Usuario: sysadmin
    - Clave: \*\*\*\*
  - Reiniciar
- Iniciar sesión
  - Usuario: curso
  - Clave: \*\*\*\*
  - Unir a: CURSO