



FACULTAD DE INGENIERÍA

REDES DE DATOS SEGURAS

Proyecto 3 SHIANTY — SAMBA

Alumnos

- Garrido Czacki Mario Horacio
- Romero Andrade Cristian
- Romero Andrade Vicente

Equipo 3

Profesor: Ing. Edgar Martinez Meza



Índice

1. Recursos	1
1.1. Red Emulada	1
1.2. Servidor	1
1.2.1. Servidor Linux (VM)	1
1.2.2. Tarjeta de Red	1
1.3. Configuración	1
1.3.1. Configurar la tarjeta de red	1
1.3.2. NIS	2
1.3.3. NFS	3
1.3.4. SAMBA AD DC	4

1. Recursos

1.1. Red Emulada

Segmento:	192,168,100,0/24
Puerta de enlace:	192,168,100,1
Broadcast:	192,168,100,255
Dominio:	srv.nis

1.2. Servidor

1.2.1. Servidor Linux (VM)

Hostname:	Node03
Sistema Operativo:	Debian 10 <i>Buster</i>

1.2.2. Tarjeta de Red

IP:	192,16,100,119/24
DNS:	192,168,100,1198,8,8,8

1.3. Configuración

1.3.1. Configurar la tarjeta de red

Se tiene que configurar la tarjeta de red para que adquiera su DNS y ip estática:

- En este caso la interfaz de red es `ens33`, donde este nombre puede variar.
- Se tiene que modificar el archivo `/etc/network/interfaces` y añadir la siguiente configuración:



```

1 auto ens33
2 allow-hotplug ens33
3 iface ens33 inet static
4     address 192.168.100.119
5     netmask 255.255.255.0
6     network 192.168.100.0
7     broadcast 102.168.100.255
8     gateway 192.168.100.1
9     dns-nameservers 192.168.100.119 8.8.8.8
10    dns-search srv.nis
11

```

Asignar Dominio

Se debe de añadir la siguiente línea a `/etc/hosts`.

```

1 192.168.100.119 Node03.srv.nis srv.nis Node03 srv

```

Esto redirecciona todas las peticiones del dominio del servidor a su ip. El gestor de DNS configura de forma automática el registro en `/etc/resolv.conf`, quedando de la siguiente manera:

```

1 # Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
2 #     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
3 nameserver 192.168.100.119
4 nameserver 8.8.8.8
5 search srv.nis

```

1.3.2. NIS

NIS funciona para poder centralizar la autenticación de los clientes Linux.

1. Instalar NIS, en terminal con permisos administrativos:

```

1 apt -y install nis
2

```

Al finalizar aparecerá una pantalla de configuración donde se añadirá el dominio del servidor

```

1 NIS domain:
2
3 srv.nis_____
4
5     <ok>

```

2. Configurar como servidor maestro NIS

Se tiene que modificar el archivo `/etc/default/nis`

```

1 # Línea 6: Poner a NIS como servidor maestro
2 NISERVER=master

```

Adicionalmente en el mismo archivo de configuración, se puede configurar un rango de IPs que pueden hacer peticiones a este servicio

```

1 # Si se deja asi se le dara acceso a todo el mundo
2 0.0.0.0 0.0.0.0
3 # Si se configura asi se le dara acceso solo al rango deseado
4 192.168.100.0 192.168.100.255

```



Reiniciamos el servicio nis para que se efectúen los cambios.

```
1 systemctl restart nis
```

3. Aplicar la configuración al servicio

Ejecutamos el siguiente comando

```
1 /usr/lib/yp/ypinit -m
```

Si todo va bien se tiene que aparecer lo siguiente:

```
1 Node03.srv.nis has been set up as a NIS master server.
2
3 Now you can run ypinit -s Node03.srv.nis on all slave server.
```

4. Cada que se tenga que añadir un nuevo usuario se tiene que actualizar la base de datos de NIS (este ya esta incluido en el script add_user.sh).

Se ejecuta el siguiente comando dentro del directorio /var/yp

```
1 make
```

1.3.3. NFS

NFS crea un sistema de archivos centralizados por redefined

1. Instalar el servidor nfs

```
1 apt -y install nfs-kernel-server
```

2. Configurar el dominio del servidor en el archivo /etc/idmapd.conf

```
1 # Linea 6: Aqui se descomenta y se agrega el dominio
2 Domain = srv.nis
```

3. Añadir la ruta de los directorios home que se van a compartir por NFS, esto es en el archivo /etc/exports

```
1 /home 192.168.100.0/24(rw,no_root_squash,no_subtree_check)
```

- /home es la ruta donde se van a montar los directorios personales de los clientes.
- xx.xx.xx.xx/xx Es la mascara del segmento que puede acceder a estos directorios por NFS.
- (...) Son las opciones de exports.

4. Reiniciar el servicio para ver reflejados los cambios.

```
1 systemctl restart nfs-server
```



1.3.4. SAMBA AD DC

SAMBA es una implementación del protocolo smb, a partir de su versión 4 añade capacidades para crear y gestionar un controlador de directorio activo (active directory) y kerberos, el cual es compatible con la autenticación de red por de windows. Active directory es una implementación del protocolo ldap y kerberos es un protocolo de autenticación.

1. Instalar el protocolo para la sincronización de la hora. Es un requerimiento de kerberos para los miembros del dominio

```
1 apt install ntp
```

2. Instalar los paquetes necesarios para el servidor de Samba 4 con AD DC

```
1 apt install samba smbclient attr winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config
   krb5-user
```

Mostrara una ventana de configuración que pedirá algunos parámetros

- a) El primero es el del REALM o reino:

```
1 Reino predeterminado de la versión 5 de Kerberos:
2 SRV.NIS-----
3   <Aceptar>
4
```

- b) El siguiente es el nombre del host, el cual se usara el mismo que el reino pero en minúsculas

```
1 Servidores de Kerberos para su reino:
2 srv.nis-----
3   <Aceptar>
```

- c) La ultima ventana pedirá el nombre del host administrativo. Se pone el mismo que el del servidor

```
1 Servidor administrativo para su reino de Kerberos:
2 srv.nis-----
3   <Aceptar>
```

3. Creación del controlador de dominio.

Se detienen los servicios antes de configurar esta parte.

```
1 systemctl stop samba-ad-dc smbd nmbd winbind
2 systemctl disable samba-ad-dc smbd nmbd winbind
```

Se elimina o se respalda el archivo de configuración de SAMBA por defecto

```
1 mv /etc/samba/smb.conf /etc/samba/smb.conf.org
2
```

Se inicia la creación del controlador de forma interactiva, dotándole de compatibilidad con extensiones NIS RFC2307.

```
1 samba-tool domain provision --use-rfc2307 --interactive
```

En la parte de Realm introducir el usado en este manual.



```
1 Realm: srv.nis
```

En domain dejar el que esta por defecto, solo pulsar enter

```
1 Domain [SRV]:
```

En Server Role dejar el que esta por defecto [dc]

```
1 Server Role (dc, member, standalon) [dc]:
```

```
2
```

DNS backend, dejar el que esta por defecto que es SAMBA_INTERNAL

```
1 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
```

DNS forwarder IP address. Dejar la IP del servidor que en este caso es 192.168.100.119

```
1 DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]: 192.168.100.119
```

Administrator password: Esta es la contraseña de administrador, poner una que sea mayor a 8 caracteres con una mayúscula y un dígito

```
1 Administrator password:
```

```
2 Retype password:
```

Si todo sale bien mostrara los datos con controlador de dominio

```
1 Server Role:          active directory domain controller
2 Hostname:             Node03
3 NetBIOS Domain:      SRV
4 DNS Domain:          srv.nis
5 DOMAIN SID:          S-1-5-21-3772837808-1505251784-1375148484
```

Iniciar la familia de los demonios del samba-ad-dc

```
1 systemctl unmask samba-ad-dc
2 systemctl start samba-ad-dc
3 systemctl enable samba-ad-dc
```

4. Probar la configuración

Verificar el nivel de dominio

```
1 samba-tool domain level show
```

Si todo sale bien debe mostrar lo siguiente

```
1 Domain and forest function level for domain 'DC=srv,DC=nis'
2
3 Forest function level: (Windows) 2008 R2
4 Domain function level: (Windows) 2008 R2
5 Lowest function level of a DC: (Windows) 2008 R2
```

Verificar el servidor de archivos. netlogon y sysvol

```
1 smbclient -L localhost -U%
```

Debe mostrar lo siguiente:



```

1      Sharename      Type      Comment
2      -----      -
3      homes          Disk      Home Directories
4      netlogon        Disk
5      sysvol          Disk
6      IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
7 Reconnecting with SMB1 for workgroup listing.
8
9      Server          Comment
10     -----
11
12     Workgroup        Master
13     -----
14     WORKGROUP        NODE03
15     WORKSOMCH        VENGANZASS

```

En el caso anterior se mostró los directorios configurados y los workgroups existentes de otras maquinas Windows en la red.

Verificar la autenticación usando el usuario de administrador del dominio.

```
1 smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

Si todo sale bien debe mostrar lo siguiente:

```

1 Enter SRV\Administrator's password:
2 .                                D          0 Sun May 10 20:07:09 2020
3 ..                               D          0 Sun May 10 20:07:12 2020
4
5      19478160 blocks of size 1024. 17106040 blocks available
6
7

```

5. Verificar los registros de DNS. Importante que si los muestre ya que sin estos Windows no sera capaz de detectar el dominio

SRV de ldap usando TCP

```
1 host -t SRV _ldap._tcp.srv.nis
```

SRV de kerberos usando UDP

```
1 host -t SRV _kerberos._udp.srv.nis
```

A del dominio

```
1 host -t A Node03.srv.nis
```

6. Si todo salio bien entonces el servidor ya esta correctamente configurado
A veces hay que abrir los puertos en el firewall en caso de tener problemas

