FACULTAD DE INGENIERÍA

SISTEMAS DISTRIBUIDOS

Proyecto: Implementación de un servidor con sincronización de claves NIS-SAMBA-Active Directory/Kerberos

Alumnos

- Gonzalez Gonzalez Claudio
- Mansur Jiménez Arturo
- Romero Andrade Cristian
- Romero Andrade Vicente

Profesora: Ing. Guadalupe Lizeth Parrales Romay

ÍNDICE

Proyecto: Implementación de un servidor con sincronización de claves NIS-SAMBA-Active Directory/Kerberos

Gonzalez Gonzalez Claudio, Mansur Jiménez Arturo, Romero Andrade Cristian, Romero Andrade Vicente
Sistemas Distribuidos
Facultad de Ingeniería
Universidad Nacional Autónoma de México

Resumen

En el presente trabajo se implementa la sincronización de cuentas así como sus claves a través de una red de área local a distintas máquinas de distintos sistemas operativos.

I. Introducción

En la presente se describe una serie de pasos para llevar a cabo la administración central de usuarios a un servidor basado en Linux. Existen varias herramientas para llevar a cabo esta tarea, para compartir archivos se utilizó SAMBA y para montar los archivos del servidor a varios ordenadores conectados al servidor maestro. Para la autenticación se optó Active Directory y Kerberos para tener compatibilidad tanto con sistemas basados en Linux y Windows.
Estas herramientas son útiles ya que permiten a los hosts, independientemente su sistema operativo, autenticarse a un servidor basado en Linux. Es es una opción excelente en un entorno T.I. (tecnología de la información) heterogéneo con distintos sistemas operativos.

II. Arquitectura

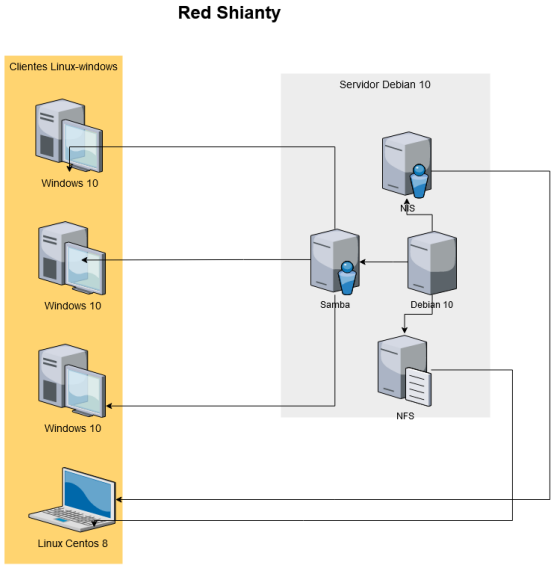

Figura 1. Arquitectura de la red

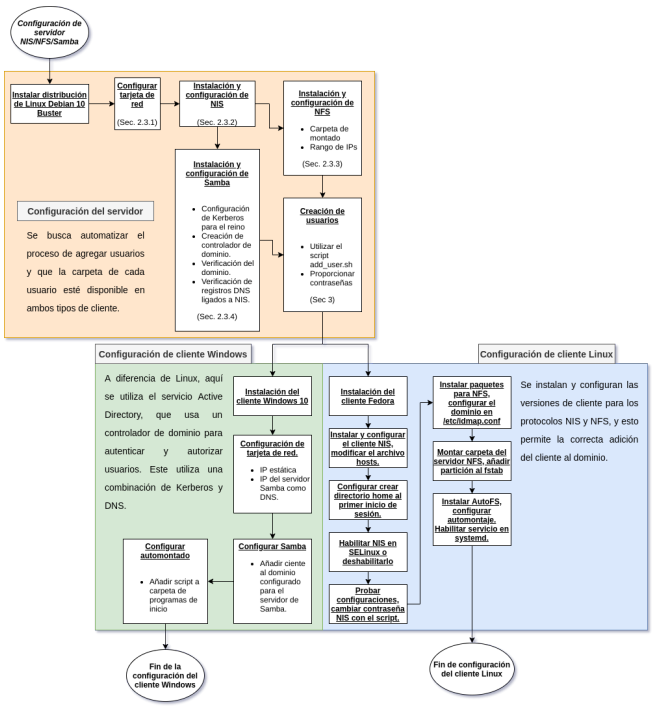

Figura 2. Diagrama cliente-servidor

III. Recursos

III-A. Red Emulada

Segmento:	192.168.100.0/24
Puerta de enlace:	192.168.100.1
Broadcast:	192.168.100.255
Dominio:	`srv.nis`

IV. Servidor

IV-A. Servidor Linux (VM)

Hostname:	Node03
Sistema Operativo:	Debian 10 *Buster*

IV-B. Tarjeta de Red

IP:	192.168.100.119/24
DNS:	192.168.100.119 8.8.8.8

IV-C. Configuración

IV-C1. 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:

```
auto ens33
allow-hotplug ens33
iface ens33 inet static
    address 192.168.100.119
    netmask 255.255.255.0
    network 192.168.100.0
    broadcast 102.168.100.255
    gateway 192.168.100.1
    dns-nameservers 192.168.100.119 8.8.8.8
    dns-search srv.nis
```

Script 1: Archivo /etc/netctl/interfaces.

IV-C1a. Asignar Dominio:
Se debe de añadir la siguiente línea a `/etc/hosts`.

```
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:

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

IV-C2. NIS: NIS funciona para poder centralizar la autenticación de los clientes Linux.

1. Instalar NIS, en terminal con permisos administrativos:

```
$ apt -y install nis
```

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

```
NIS domain:

srv.nis______

    <ok>
```

2. Configurar como servidor maestro NIS
   Se tiene que modificar el archivo `/etc/default/nis`

```
# Linea 6: Poner a NIS como servidor maestro
NISSERVER=master
```

Script 2: Modificación del archivo /etc/default/nis

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

```
# Si se deja asi se le dara acceso a todo el mundo
0.0.0.0 0.0.0.0
# Si se configura asi se le dara acceso solo al rango
↪  deseado
192.168.100.0 192.168.100.255
```

Reiniciamos el servicio nis para que se efectúen los cambios.

```
$ systemctl restart nis
```

3. Aplicar la configuración al servicio
   Ejecutamos el siguiente comando

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

Si todo va bien se tiene que aparecer lo siguiente:

```
Node03.srv.nis has been set up as a NIS master server.

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`

```
$ make
```

IV-C3. NFS: NFS crea un sistema de archivos centralizados por redefined

1. Instalar el servidor nfs

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

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

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

Script 3: Modificación del archivo /etc/idmap.conf

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

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

Script 4: Adición en el archivo /etc/exports

- `/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.

```
$ systemctl restart nfs-server
```

IV-C4. 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 NTP para la sincronización de la hora. Es un requerimiento de Kerberos para los miembros del dominio

```
$ apt install ntp
```

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

```
$ 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:

```
Reino predeterminado de la versión 5 de Kerberos:
SRV.NIS_________
    <Aceptar>
```

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

```
Servidores de Kerberos para su reino:
srv.nis______
    <Aceptar>
```

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

```
Servidor administrativo para su reino de Kerberos:
srv.nis_______
    <Aceptar>
```

3. Creación del controlador de dominio.
   Se detienen los servicios antes de configurar esta parte.

```
$ systemctl stop samba-ad-dc smbd nmbd winbind
$ systemctl disable samba-ad-dc smbd nmbd winbind
```

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

```
$ mv /etc/samba/smb.conf /etc/samba/smb.conf.org
```

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

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

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

```
Realm: srv.nis
```

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

```
Domain [SRV]:
```

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

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

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

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

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

```
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

```
Administrator password:
Retype password:
```

Si todo sale bien mostrara los datos con controlador de dominio

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

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

```
$ systemctl unmask samba-ad-dc
$ systemctl start samba-ad-dc
$ systemctl enable samba-ad-dc
```

4. Probar la configuración
   Verificar el nivel de dominio

```
$ samba-tool domain level show
```

Si todo sale bien debe mostrar lo siguiente

```
Domain and forest function level for domain
↪  'DC=srv,DC=nis'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Verificar el servidor de archivos. `netlogon` y `sysvol`

```
$ smbclient -L localhost -U%
```

Debe mostrar lo siguiente:

```
       Sharename       Type      Comment
        ------       ---       -----
        homes           Disk      Home Directories
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba
↪  4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ------             -----

        Workgroup            Master
        ------             -----
        WORKGROUP            NODE03
        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.

```
$ smbclient //localhost/netlogon -UAdministrator -c
↪  'ls'
```

Si todo sale bien debe mostrar lo siguiente:

```
Enter SRV\Administrator's password:
  .                                   D        0  Sun
↪  May 10 20:07:09 2020
  ..                                  D        0  Sun
↪  May 10 20:07:12 2020

                19478160 blocks of size 1024. 17106040
↪  blocks available
```

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

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

SRV de kerberos usando UDP

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

A del dominio

```
$ 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

V. Creación de Usuarios

Se debe ejecutar el script `add_user.sh`, en este ejemplo añadiremos al un usuario nombrado como *usuario_77*.

```
$ ./add_user.sh usuario_77
```

Si todo sale bien se le pedirá la contraseña de UNIX y la de SAMBA (Usar la misma).

```
Añadiendo el usuario 'usuario_77' ...
make: se entra en el directorio '/var/yp'
make[1]: se entra en el directorio '/var/yp/srv.nis'
Updating netid.byname...
make[1]: se sale del directorio '/var/yp/srv.nis'
make: se sale del directorio '/var/yp'
Añadiendo el nuevo grupo 'usuario_77' (1010) ...
make: se entra en el directorio '/var/yp'
make[1]: se entra en el directorio '/var/yp/srv.nis'
Updating group.byname...
Updating group.bygid...
Updating netid.byname...
make[1]: se sale del directorio '/var/yp/srv.nis'
make: se sale del directorio '/var/yp'
Añadiendo el nuevo usuario 'usuario_77' (1010) con
↪  grupo 'usuario_77' ...
make: se entra en el directorio '/var/yp'
make[1]: se entra en el directorio '/var/yp/srv.nis'
Updating passwd.byname...
Updating passwd.byuid...
Updating netid.byname...
Updating shadow.byname...
make[1]: se sale del directorio '/var/yp/srv.nis'
make: se sale del directorio '/var/yp'
Creando el directorio personal '/home/usuario_77' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para usuario_77
Introduzca el nuevo valor, o pulse INTRO para usar el
↪  valor predeterminado
        Nombre completo []: Usuario 77
        Número de habitación []: 12b
        Teléfono del trabajo []: 5567382132
        Teléfono de casa []: 5536271232
        Otro []:
£Es correcta la información? [S/n] S
Ingresa la contraseña SAMBA del usuario
New Password:
Retype Password:
User 'usuario_77' created successfully
make[1]: se entra en el directorio '/var/yp/srv.nis'
Updating passwd.byname...
Updating passwd.byuid...
Updating netid.byname...
Updating shadow.byname...
make[1]: se sale del directorio '/var/yp/srv.nis'
```

El contenido de `add_user.sh` es el siguiente:

```
#!/bin/sh
usuario=$1
adduser $usuario
uid=$(id -u $usuario)
echo "Ingresa la contraseña SAMBA del usuario"
samba-tool user create $usuario -uid-number $uid
cd /var/yp
make
```

Script 5: Contenido de add_user.sh

VI. Clientes

VI-A. VM cliente Linux

hostname:	Node02
Sistema Operativo:	Centos 8

VI-B. Tarjeta de red

IP:	192.168.100.28/24
Puerta de Enlace	192.168.100.1
Broadcast:	192.168.100.255
DNS:	192.168.100.119 8.8.8.8
Dominio AC:	SRV

VI-C. Configuración

VI-C1. Linux:

VI-C1a. Añadir dominio:

1. Se debe modificar el archivo `/etc/hosts` añadiendo el dominio del servidor.

```
192.168.100.119 Node03.srv.nis srv.nis Node03 srv
```

Script 6: Modificación del archivo /etc/hosts

VI-C1b. NIS:

1. Instalar los paquetes necesarios.

```
$ dnf -y install ypbind rpcbind oddjob-mkhomedir
```

2. Configurar el dominio del NIS
   Usar `ypdomainname` como usuario administrativo.

```
$ ypdomainname srv.world
```

Añadir el dominio a `/etc/sysconfig/network`

```
$ echo "NISDOMAIN=srv.world" » /etc/sysconfig/network
```

Script 7: Modificación del archivo /etc/sysconfig/network

Añadir el servidor al la configuración de NIS `/etc/yp.conf`

```
# [domain (NIS domain) server (NIS server)]
domain srv.nis server Node03.srv.nis
```

Script 8: Modificación del archivo /etc/yp.conf

3. Configurar el método de autenticación del cliente
   Añadir NIS como método de autenticación

```
$ authselect select nis -force
profile "nis" was selected.
The following nsswitch maps are overwritten by the
↪  profile:
- aliases
- automount
- ethers
- group
- hosts
- initgroups
- netgroup
- networks
- passwd
- protocols
- publickey
- rpc
- services
- shadow

Make sure that NIS service is configured and enabled.
↪  See NIS documentation for more information.
```

4. Añadir la característica para crear directorio de home al primer inicio de sesión

```
$ authselect enable-feature with-mkhomedir
```

5. Habilitar NIS en SELinux (o desactivar SELinux si no es indispensable).

```
$ setsebool -P nis_enabled on
```

6. Habilitar el servicio en Systemd

```
$ systemctl enable -now rpcbind ypbind nis-domainname
↪  oddjobd
```

7. Probar la correcta configuración del cliente
   Confirma si el enlazador tiene comunicación con el servidor NIS

```
$ ypwhich
```

8. Si todo sale bien debe aparecer el servidor en el dominio

```
Node03.src.nis
```

9. Cambiar contraseña de NIS (Se proporcionara un script bash para automatizar este proceso)

```
$ yppasswd
```

VI-C1c. NFS:

1. Instalar los paquetes necesarios para NFS

```
$ dnf -y install nfs-utils
```

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

```
# linea 5 donde esta el dominio por defecto poner el
↪  del servidor
Domain = srv.nis
```

Script 9: Modificación del archivo /etc/idmapd.conf

3. Probar que hay acceso al servidor NFS
   Montar la carpeta del servidor NFS

```
$ mount -t nfs Node03.srv.nis:/home /home
```

Si todo sale bien correr el siguiente comando que mostrará que efectivamente esta operativa la partición del tipo NFS4

```
df -hT /home
S.ficheros           Tipo Tamaño Usados  Disp Uso%
↪  Montado en
Node03.srv.nis:/home nfs4    19G   1.3G   17G   8%
↪  /home
```

4. Añadir la partición al Fstab, esto montara la carpeta una vez que se inicia el sistema
   Modificar el archivo `/etc/fstab`

```
# Añadir al final del archivo
Node03.srv.nis:/home/ /home               nfs
↪  defaults        0 0
```

Script 10: Modificación del archivo /etc/fstab

5. Añadir el montaje dinámico[1]
   Instalar AutoFS

```
$ dnf -y install autofs
```

Añadir la directiva de automontaje a la configuración maestra de AutoFS en el archivo `/etc/auto.master`

```
# Añadir al final
/-    /etc/auto.mount
```

Crear la configuración de automontaje `/etc/auto.mount`

```
# create new : [mount point] [option] [location]

/home   -fstype=nfs,rw  dlp.srv.world:/home
```

Habilitar el servicio en systemd

```
$ systemctl enable -now autofs
```

[1]En caso de una caída del servidor este volverá a montar cada vez que se quiera acceder al directorio asignado al NFS

VI-C2. Windows:

- Añadir el DNS y asignar una ip estática a la tarjeta de red en el administrador de dispositivos
- En servidor DNS poner la IP del servidor SAMBA AD DC

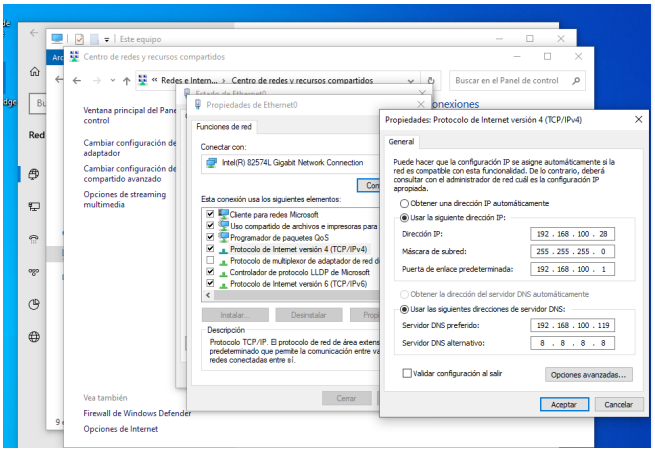

Figura 3. Captura de administrador de dispositivos

VI-C2a. SAMBA AD DC:

Añadir cliente al demonio

- Click derecho a equipo y `propiedades/configuración avanzada/Nombre de equipo/ botón cambiar...`

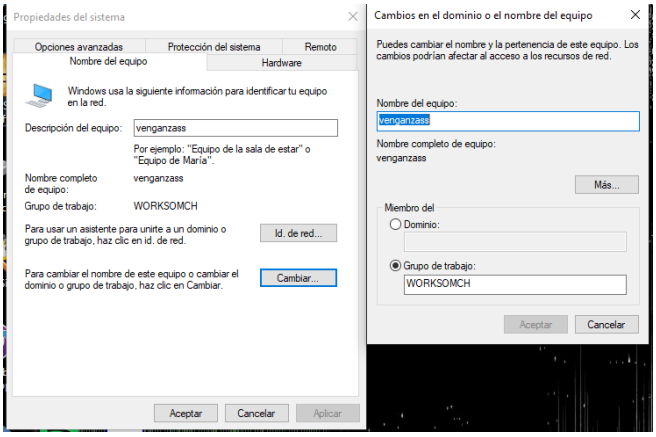

Figura 4. Configuración del nombre del equipo

- En la sección Miembro del seleccionar Dominio poner el dominio del servidor SAMBA que es `srv.nis`

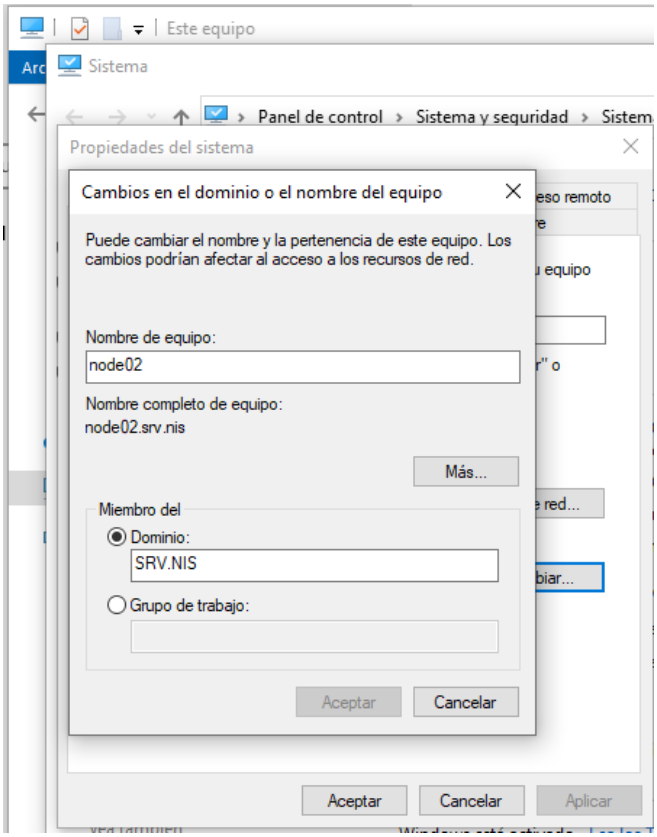

Figura 5. Captura de asignación de dominio

- Si sale un dialogo de inicio de sesión usar el usuario “Administrator” y poner la contraseña proporcionada en la configuración
- Añadir el script `drive.bat` a la carpeta de programas de inicio para automontar la unidad `Z` al inicio de sesión de cada usuario.

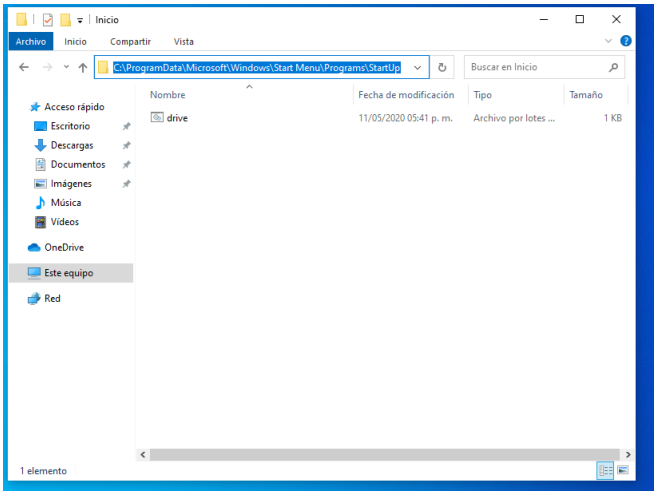

Figura 6. Captura de menú de inicio

el contenido de este `drive.bat` es el siguiente:

```
net use Z: \\SRV.NIS\%USERNAME% /PERSISTENT:YES
```

Script 11: Contenido de drive.bat

- Para adaptar a caso de uso diferente modificar `SRV.NIS` por el nombre de dominio. correspondiente.
- Reiniciar equipo

- Si todo sale bien debe poder iniciar sesión con los usuarios creados en el servidor SAMBA

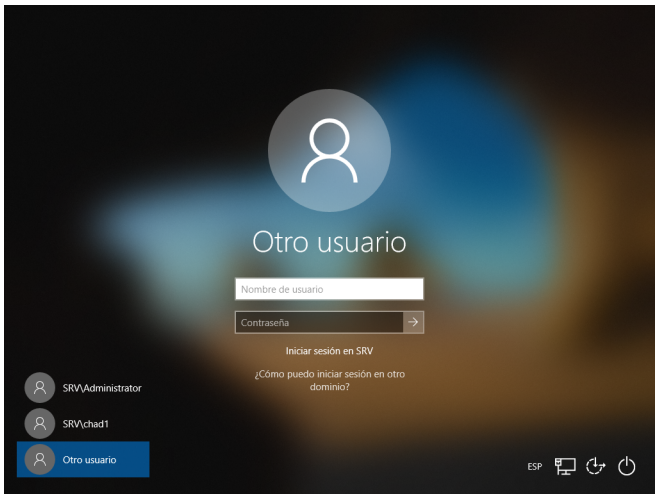

Figura 7. Captura de inicio de sesión

- La unidad `Z:` con la carpeta `home` del usuario debe montarse al inicio de cada sesión

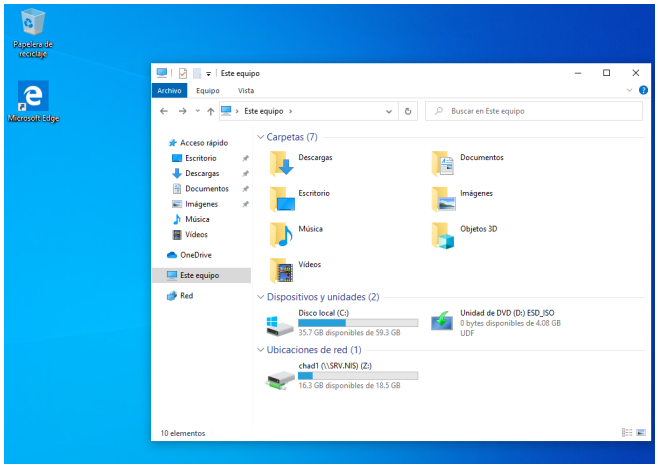

Figura 8. Unidad **Z:** montada

VII. Conclusión

Se utilizaron distintos protocolos para llevar a cabo la distribución de los archivos de los usuarios que se crean en el servidor maestro (IV-C2), también en casos se implemento una manera para volver a reactivar la conexión servidor (para Linux) en caso de que este se encuentre desconectado por factores externos, esta esta descrita en la sección VI-C1.

El uso de los protocolos descritos en el glosario nos ayuda a crear nuestra red de usuarios sin tener que crear uno por uno en cada ordenador, al igual la persistencia de los datos de los usuarios cuando ellos cambian de ordenador, ya que gracias SAMBA, el directorio `/home` del usuario se monta en cada PC donde, para acceder a esta carpeta, debe ser el mismo usuario con su cuenta usando protocolos de autenticación como Active Directory.

Índice de figuras

Índice de Script's

Glosario

AutoFS Es un servicio por parte del cliente que monta automáticamente el sistema de archivos adecuado. 9

fstab Es un fichero que se encuentra comúnmente en sistemas Unix (en el directorio `/etc/`) como parte de la configuración del sistema. Lo más destacado de este fichero es la lista de discos y particiones disponibles. En ella se indica como montar cada dispositivo y qué configuración utilizar. 9

Kerberos Es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura. 2, 4

LDAP El protocolo ligero de acceso a directorios hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. 4

NFS Network File System es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos. 4, 9

NTP Network Time Protocol es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable . 4

SAMBA Es una implementación libre del protocolo de archivos compartidos de Microsoft Windows para sistemas de tipo UNIX. 2, 4, 5, 7, 10–12

systemd Es un conjunto de demonios o daemons de administración de sistema, bibliotecas y herramientas diseñados como una plataforma de administración y configuración central para interactuar con el núcleo del Sistema operativo GNU/Linux. 8, 9

Siglas

NIS Network Information Service. 3–5, 8, 9