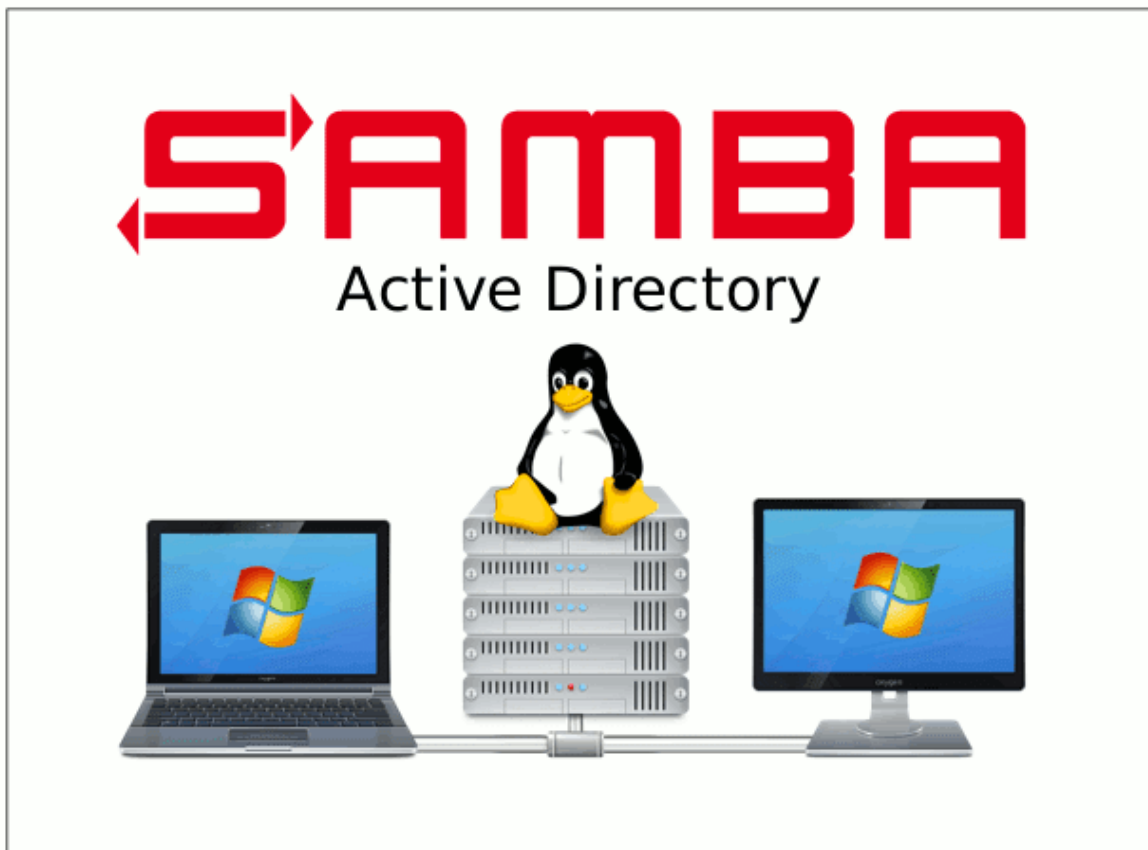


UT4 - PRÁCTICA 5

SAMBA DOMAIN CONTROLLER



INDICE

PASO 1 – Cambio nombre	3
PASO 2 – Backup /etc/hosts.....	3
PASO 3 – Configuración /etc/hosts	3
PASO 4 - Verificación hostname y FQDN	4
PASO 5 - Configuración estática.....	4
PASO 6 – Desactivamos DNS y quitamos enlace resolv.conf	5
PASO 7- Nuevo resolv.conf	5
PASO 8 – Inmutabilidad /etc/resolv.conf	5
PASO 9 - Instalación paquetes necesarios	6
PASO 10 - Configuración instalación	6
PASO 11 - Detención servicios	7
PASO 12 – Desenmascararían e habilitación servicio	7
PASO 13 – Copias seguridad samba	7
PASO 14 - Configuración controlador dominio de Samba	8
PASO 15 - Comprobación smb.conf	8
PASO 16 – Copia seguridad krb5.conf y sobrescribir	9
PASO 17 – Iniciamos servicio samba-ad-dc.....	9
PASO 18 – Permisos chrony	10
PASO 19 - Configuración chrony.....	10
PASO 20 – Reiniamos servicio y comprobación	10
PASO 21 – Comprobaciones	11
PASO 22 – Verificación con login	12
PASO 23 - Creación usuario con samba-tool.....	12

PASO 1 – Cambio nombre

Cambiamos el nombre de nuestro servidor. Para ello utilizaremos el siguiente comando.

```
admin01@server:~$ hostnamectl set-hostname dani
==== AUTHENTICATING FOR org.freedesktop.hostname1.set-static-hostname ====
Authentication is required to set the statically configured local hostname, as well as the pretty hostname.
Authenticating as: admin01
Password:
==== AUTHENTICATION COMPLETE ====
```

PASO 2 – Backup /etc/hosts

Haremos un backup del fichero /etc/hosts

```
admin01@server:~$ sudo cp /etc/hosts /etc/hosts.old
```

PASO 3 – Configuración /etc/hosts

Modificaremos el fichero original (/etc/hosts) para que resuelva nuestro nombre (nuestro servidor) y nuestro FQDN en este caso dani.aso.local

```
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
192.168.0.5 dani.aso.local dani

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

PASO 4 - Verificación hostname y FQDN

Comprobaremos nuestro hostname modificado con anterioridad y verificamos si nos resuelve nuestro FQDN.

```
admin01@dani:~$ hostname -f
dani.aso.local
admin01@dani:~$ ping dani.aso.local
PING dani.aso.local (192.168.0.5) 56(84) bytes of data.
64 bytes from dani.aso.local (192.168.0.5): icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from dani.aso.local (192.168.0.5): icmp_seq=2 ttl=64 time=0.035 ms
^C
--- dani.aso.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.015/0.025/0.035/0.010 ms
admin01@dani:~$
```

PASO 5 - Configuración estática

Configuraremos una ip estática desde el fichero .yaml de netplan. Una vez configurado, aplicaremos los cambios con netplan apply.

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.0.5/24
      routes:
        - to: default
          via: 192.168.0.1
      nameservers:
        addresses:
          - 10.239.3.7
          - 192.168.0.5
```

PASO 6 – Desactivamos DNS y quitamos enlace resolv.conf

Desactivamos el servicio DNS. También eliminaríamos el enlace simbólico de resolv.conf.

```
root@dani:/etc/netplan# sudo systemctl disable --now systemd-resolved
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
root@dani:/etc/netplan# sudo unlink /etc/resolv.conf
root@dani:/etc/netplan#
```

PASO 7- Nuevo resolv.conf

Crearíamos un nuevo resolv.conf e introduciríamos como servidores DNS nuestra ip para que se pueda hacer la resolución en el propio servidor. También las de Conselleria para tener acceso a internet y que busque desde nuestro FQDN.

```
GNU nano 6.2 /etc/resolv.conf
nameserver 192.168.0.5
nameserver 10.239.3.7
search aso.local
```

PASO 8 – Inmutabilidad /etc/resolv.conf

Se hace inmutable el archivo para evitar que cualquier instalación de otros servicios lo modifique automáticamente.

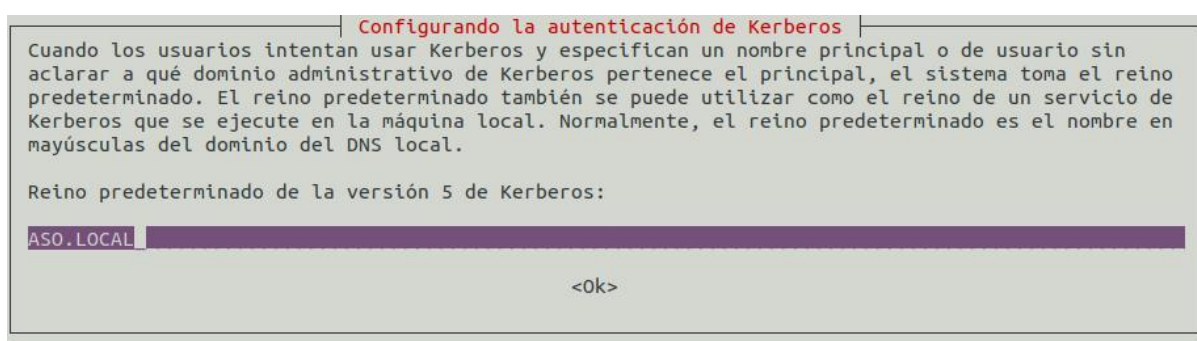
```
root@dani:~# sudo chattr +i /etc/resolv.conf
```

PASO 9 - Instalación paquetes necesarios

Haremos un apt update para actualizar todos los repositorios de apt e instalaremos los siguientes paquetes: acl attr samba samba-dsdb-modules samba-vfs-modules smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user chrony net-tools

PASO 10 - Configuración instalación

Mientras se realiza la instalación, se nos solicitarán ciertos parámetros. En primer lugar, tendremos que definir nuestro Reino. Será ASO.LOCAL.



Configurando la autenticación de Kerberos

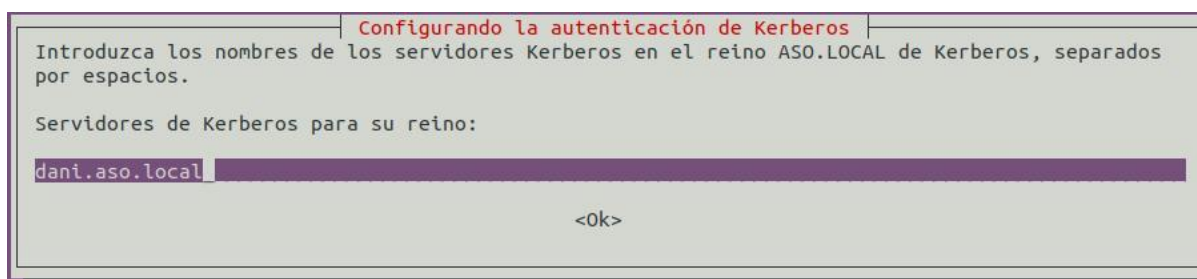
Cuando los usuarios intentan usar Kerberos y especifican un nombre principal o de usuario sin aclarar a qué dominio administrativo de Kerberos pertenece el principal, el sistema toma el reino predeterminado. El reino predeterminado también se puede utilizar como el reino de un servicio de Kerberos que se ejecute en la máquina local. Normalmente, el reino predeterminado es el nombre en mayúsculas del dominio del DNS local.

Reino predeterminado de la versión 5 de Kerberos:

ASO.LOCAL

<Ok>

Luego nos solicitará el nombre del servidor Kerberos de nuestro reino.



Configurando la autenticación de Kerberos

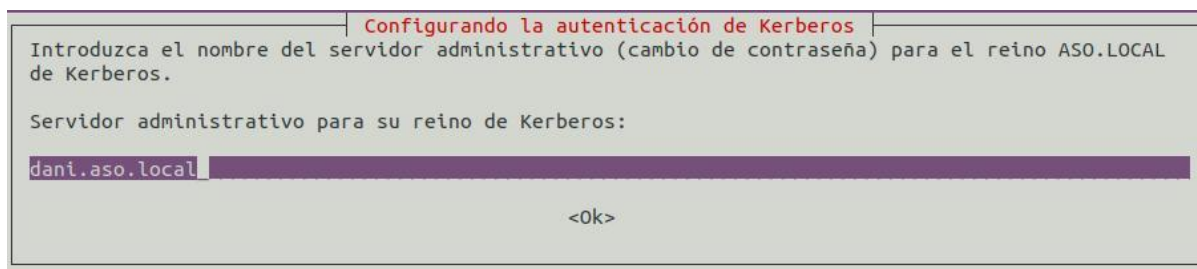
Introduzca los nombres de los servidores Kerberos en el reino ASO.LOCAL de Kerberos, separados por espacios.

Servidores de Kerberos para su reino:

dani.aso.local

<Ok>

Por último, indicamos que nuestro servidor administrativo del reino



Configurando la autenticación de Kerberos

Introduzca el nombre del servidor administrativo (cambio de contraseña) para el reino ASO.LOCAL de Kerberos.

Servidor administrativo para su reino de Kerberos:

dani.aso.local

<Ok>

PASO 11 - Detención servicios

Una vez instalado, se deben detener los servicios smbd, nmbd y winbind que vienen activos por defecto al instalar estos recursos.

```
admin01@dani:~$ sudo systemctl disable --now smbd nmbd winbind
Synchronizing state of smbd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable smbd
Synchronizing state of nmbd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable winbind
Removed /etc/systemd/system/multi-user.target.wants/nmbd.service.
admin01@dani:~$
```

PASO 12 – Desenmascararían e habilitación servicio

Activaremos el servicio samba-ad-dc. Este servicio por defecto esta enmascarado porque por defecto no se usa. Se usan los servicios del PASO 11 por lo que desenmascaremos el servicio samba-ad-dc y lo activaremos para que se use.

```
root@dani:~# systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.
root@dani:~# systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
Created symlink /etc/systemd/system/multi-user.target.wants/samba-ad-dc.service → /lib/systemd/system/samba-ad-dc.service.
root@dani:~#
```

PASO 13 – Copias seguridad samba

Ahora vamos a configurar Samba. En primer lugar, se hará una copia de seguridad del fichero /etc/samba/smb.conf

```
admin01@dani:~$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.copia
[sudo] password for admin01:
admin01@dani:~$
```

PASO 14 - Configuración controlador dominio de Samba

Configuraremos el controlador de dominio de Samba mediante el uso de samba-tool. Esto creará un fichero dentro de /etc/samba/

```
root@dani:~# samba-tool domain provision --use-rfc2307 --interactive
```

Dejaremos todos los valores en blanco menos el forwarder

```
root@dani:~# samba-tool domain provision --use-rfc2307 --interactive
Realm [ASO.LOCAL]:
Domain [ASO]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.0.5]: 10.239.3.7
```

Ya, por último, ingresaremos una contraseña. La contraseña que he empleado ha sido AsoAula5

PASO 15 - Comprobación smb.conf

Podemos comprobar que se ha creado el fichero correctamente:

```
root@dani:/etc/samba# cat smb.conf
# Global parameters
[global]
    dns forwarder = 10.239.3.7
    netbios name = DANI
    realm = ASO.LOCAL
    server role = active directory domain controller
    workgroup = ASO
    idmap_ldb:use rfc2307 = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/aso.local/scripts
    read only = No
root@dani:/etc/samba#
```


PASO 16 – Copia seguridad krb5.conf y sobrescribir

Ahora instalaremos Kerberos, antes solo se había asociado la configuración a Samba (reino, dns, password, etc). Para ello se realizaremos una copia de seguridad de la configuración actual y se sobrescribe la realizada por Samba.

Primero renombraremos la configuración por defecto de Kerberos a `krb5.conf.original`

```
root@dani:~# sudo mv /etc/krb5.conf /etc/krb5.conf.original
```

Luego copiamos la configuración generada samba-tool

```
root@dani:~# sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
root@dani:~#
```

PASO 17 – Iniciamos servicio samba-ad-dc

Iniciaremos samba-ad-dc que anteriormente hemos desenmascarado y habilitado

```
root@dani:~# sudo systemctl start samba-ad-dc
root@dani:~# sudo systemctl status samba-ad-dc
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-11-15 11:05:18 UTC; 4s ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
  Main PID: 2093 (samba)
    Status: "samba: ready to serve connections..."
   Tasks: 60 (limit: 4564)
  Memory: 204.6M
    CPU: 2.005s
  CGroup: /system.slice/samba-ad-dc.service
          └─2093 "samba: root process" "
```

PASO 18 – Permisos chrony

Una vez tengamos todos los servicios habilitados, para que no haya una desincronización horaria, configuraremos el servicio chrony que hemos instalado antes también. Daremos los permisos adecuados a chrony.

```
root@dani:~# sudo chown root:_chrony /var/lib/samba/ntp_signd/
root@dani:~# sudo chmod 750 /var/lib/samba/ntp_signd/
```

```
root@dani:~# ls -ld /var/lib/samba/ntp_signd/
drwxr-x-- 2 root _chrony 4096 nov 15 11:05 /var/lib/samba/ntp_signd/
root@dani:~#
```

PASO 19 - Configuración chrony

Una vez asignamos los permisos adecuados, configuraremos chrony.

Agregaremos las siguientes líneas en el fichero /etc/chrony/chrony.conf

```
bindcmdaddress 192.168.0.5
allow 192.168.0.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
```

PASO 20 – Reiniamos servicio y comprobación

Reiniciaremos el servicio y comprobaremos el estado.

```
root@dani:~# sudo systemctl restart chronyd
root@dani:~# sudo systemctl status chronyd
● chrony.service - chrony, an NTP client/server
   Loaded: loaded (/lib/systemd/system/chrony.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-11-15 11:18:25 UTC; 6s ago
     Docs: man:chronyd(8)
           man:chronyc(1)
           man:chrony.conf(5)
  Process: 2200 ExecStart=/usr/lib/systemd/scripts/chronyd-starter.sh $DAEMON_OPTS (code=exited, status=0/SUCCESS)
 Main PID: 2210 (chronyd)
   Tasks: 2 (limit: 4564)
  Memory: 1.3M
    CPU: 37ms
  CGroup: /system.slice/chrony.service
          └─2210 /usr/sbin/chronyd -F 1
            └─2211 /usr/sbin/chronyd -F 1

nov 15 11:18:25 dani systemd[1]: Starting chrony, an NTP client/server...
nov 15 11:18:25 dani chronyd[2210]: chronyd version 4.2 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SECCOMP +LINUXISA +KASLR +MMIO +RELOC +SCHED)
nov 15 11:18:25 dani chronyd[2210]: Frequency 1.599 +/- 0.203 ppm read from /var/lib/chrony/chrony.drift
nov 15 11:18:25 dani chronyd[2210]: Using right/UTC timezone to obtain leap second data
nov 15 11:18:25 dani chronyd[2210]: MS-SNTP authentication enabled
nov 15 11:18:25 dani chronyd[2210]: Loaded seccomp filter (level 1)
nov 15 11:18:25 dani systemd[1]: Started chrony, an NTP client/server.
lines 1-22/22 (END)
```

PASO 21 – Comprobaciones

Comprobaremos Samba Active Directory

Para ello, en primer lugar, verificaremos el dominio

```
root@dani:~# host -t A aso.local
aso.local has address 192.168.0.5
root@dani:~#
```

Luego, verificaremos el FQDN

```
root@dani:~# host -t A dani.aso.local
dani.aso.local has address 192.168.0.5
root@dani:~#
```

Después de realizar las comprobaciones de dominio y FQDN, verificaremos kerberos y ldap.

Verificaremos el registro SRV para _kerberos

```
root@dani:~# host -t SRV _kerberos._udp.aso.local
_kerberos._udp.aso.local has SRV record 0 100 88 dani.aso.local.
root@dani:~#
```

Posteriormente, verificaremos también el registro SRV para _ldap

```
root@dani:~# host -t SRV _ldap._tcp.aso.local
_ldap._tcp.aso.local has SRV record 0 100 389 dani.aso.local.
root@dani:~#
```

PASO 22 – Verificación con login

Podemos verificar con un login del usuario administrator con kinit. Nos autenticaremos a Kerberos con administrador.

```
root@dani:~# kinit administrator@ASO.LOCAL
Password for administrator@ASO.LOCAL:
Warning: Your password will expire in 41 days on vie 27 dic 2024 10:54:05
root@dani:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@ASO.LOCAL

Valid starting     Expires            Service principal
15/11/24 11:29:48  15/11/24 21:29:48  krbtgt/ASO.LOCAL@ASO.LOCAL
        renew until 16/11/24 11:29:36
root@dani:~#
```

PASO 23 - Creación usuario con samba-tool

Podemos crear usuarios con samba o con RSAT pero también con la herramienta samba-tool.

Creación usuaria dani

```
root@dani:~# sudo samba-tool user create dani
New Password:
Retype Password:
User 'dani' added successfully
```

Comprobación

```
root@dani:~# sudo samba-tool user list
Administrator
krbtgt
Guest
dani
root@dani:~#
```