

```
usuario@ubuntu-2404:~$ sudo hostnamectl set-hostname dc
[sudo] password for usuario:
usuario@ubuntu-2404:~$ bash
usuario@dc:~$
```

Cambiaremos el hostname a dc con el siguiente comando:
sudo hostnamectl set-hostname dc

```
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 ubuntu-2404
192.168.1.8 dc.hjm.local dc
```

Modificaremos el archivo de /etc/hosts añadiendo nuestra ip

Para entrar al archivo usaremos el siguiente comando:
sudo nano /etc/hosts

Verificaremos que se haya puesto bien con el siguiente comando:
hostname -f

```
usuario@dc:~$ hostname -f
dc.hjm.local
usuario@dc:~$ _
```

le hacemos ping para verificar que funciona

```
usuario@dc:~$ ping -c2 dc.hjm.local
PING dc.hjm.local (192.168.1.8) 56(84) bytes of data.
64 bytes from dc.hjm.local (192.168.1.8): icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from dc.hjm.local (192.168.1.8): icmp_seq=2 ttl=64 time=0.035 ms

--- dc.hjm.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rtt min/avg/max/mdev = 0.030/0.032/0.035/0.002 ms
usuario@dc:~$ _
```

ping -c2 dc.hjm.local

Desactivar servicio systemd-resolved

```
usuario@dc:~$ sudo systemctl disable --now systemd-resolved
[sudo] password for usuario:
Removed "/etc/systemd/system/sysinit.target.wants/systemd-resolved.service".
Removed "/etc/systemd/system/dbus-org.freedesktop.resolve1.service".
usuario@dc:~$
```

sudo systemctl disable --now systemd-resolved

Eliminar enlace simbólico al archivo /etc/resolv.conf
sudo unlink /etc/resolv.conf

```
usuario@dc:~$ sudo unlink /etc/resolv.conf
```

Creamos de nuevo el archivo /etc/resolv.conf
sudo nano /etc/resolv.conf

```
GNU nano 7.2 /etc/resolv.conf *
nameserver 192.168.1.8
nameserver 8.8.8.8
search hjm.local
```

Añadimos las siguientes líneas:

```
nameserver 192.168.1.8
nameserver 8.8.8.8
search hjm.local
```

Hacemos inmutable al archivo /etc/resolv.conf para que no pueda cambiar
sudo chattr +i /etc/resolv.conf

```
usuario@dc:~$ sudo chattr +i /etc/resolv.conf
usuario@dc:~$
```

Actualizar el índice de paquetes
sudo apt update

```
usuario@dc:~$ sudo apt update
```

Instalar samba con sus paquetes y dependencias

```
sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient
winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony
net-tools
```

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:

```
HJM.LOCAL
```

<Ok>

Configurando la autenticación de Kerberos

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

Servidores de Kerberos para su reino:

dc.hjm.local

<Ok>

Configurando la autenticación de Kerberos

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

Servidor administrativo para su reino de Kerberos:

dc.hjm.local

<Ok>

Detener y deshabilitar los servicios que el servidor de Active Directory de Samba no requiere (smbd, nmbd y winbind)

`sudo systemctl disable --now smbd nmbd winbind`

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

El servidor solo necesita samba-ad-dc para funcionar como Active Directory y controlador de dominio.

`sudo systemctl unmask samba-ad-dc`

```
usuario@dc:~$ sudo systemctl unmask samba-ad-dc
usuario@dc:~$
```

sudo systemctl enable samba-ad-dc

```
usuario@dc:~$ sudo systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /usr/lib/systemd/s
ystemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable samba-ad-dc
usuario@dc:~$
```

Crear una copia de seguridad del archivo /etc/samba/smb.conf
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.orig

```
usuario@dc:~$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
usuario@dc:~$
```

Ejecutar el comando samba-tool para comenzar a aprovisionar Samba Active Directory.
sudo samba-tool domain provision

```
usuario@dc:~$ sudo samba-tool domain provision
Realm [HJM.LOCAL]:
Domain [HJM]:
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: SAMBA_INTE
RNAL
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.1.8]: 8.8.8.8
```

pass: usuario123*

Crear copia de seguridad de la configuración predeterminada de Kerberos.
sudo mv /etc/krb5.conf /etc/krb5.conf.orig

```
usuario@dc:~$ sudo mv /etc/krb5.conf /etc/krb5.conf.orig
usuario@dc:~$
```

Reemplazar con el archivo /var/lib/samba/private/krb5.conf.
sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf

```
usuario@dc:~$ sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
usuario@dc:~$
```

Iniciar servicio Samba Active Directory samba-ad-dc
sudo systemctl start samba-ad-dc

```
usuario@dc:~$ sudo systemctl start samba-ad-dc
usuario@dc:~$
```

Comprobar servicio

sudo systemctl status samba-ad-dc

```
usuario@dc:~$ sudo systemctl status samba-ad-dc
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/usr/lib/systemd/system/samba-ad-dc.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-04-22 16:03:49 CEST; 42s ago
```

Cambiar el permiso y la propiedad predeterminados del directorio

/var/lib/samba/ntp_signd/ntp_signed. El usuario/grupo chrony debe tener permiso de lectura en el directorio ntp_signed.

sudo chown root:_chrony /var/lib/samba/ntp_signd/

sudo chmod 750 /var/lib/samba/ntp_signd/

```
usuario@dc:~$ sudo chown root:_chrony /var/lib/samba/ntp_signd/
usuario@dc:~$ sudo chmod 750 /var/lib/samba/ntp_signd/
usuario@dc:~$
```

Modificar el archivo de configuración /etc/chrony/chrony.conf para habilitar el servidor NTP de chrony y apuntar a la ubicación del socket NTP a /var/lib/samba/ntp_signd.

sudo nano /etc/chrony/chrony.conf

```
GNU nano 7.2 /etc/chrony/chrony.conf *

# Use NTP sources found in /etc/chrony/sources.d.
sourcedir /etc/chrony/sources.d

# This directive specify the location of the file containing ID/key pairs for
# NTP authentication.
keyfile /etc/chrony/chrony.keys

# This directive specify the file into which chronyd will store the rate
# information.
driftfile /var/lib/chrony/chrony.drift

# Save NTS keys and cookies.
ntsdumpdir /var/lib/chrony

# Uncomment the following line to turn logging on.
#log tracking measurements statistics

# Log files location.
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0

# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtcfile' directive
rtcsync

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 1 3

# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smear time.
leapsectz right/UTC

bindcmdaddress 192.168.1.8
allow 192.168.1.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
bindcmdaddress 192.168.1.8
allow 192.168.1.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
```

Reiniciar y verificar el servicio chronyd en el servidor Samba AD.

```
sudo systemctl restart chronyd
sudo systemctl status chronyd
```

```

usuario@dc:~$ sudo systemctl restart chronyd
usuario@dc:~$ sudo systemctl status chronyd
● chrony.service - chrony, an NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chrony.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-04-22 16:09:34 CEST; 6s ago
     Docs: man:chronyd(8)
           man:chronyc(1)
           man:chrony.conf(5)
   Process: 4654 ExecStart=/usr/lib/systemd/scripts/chronyd-starter.sh $DAEMON_OPTS (code>
 Main PID: 4664 (chronyd)
    Tasks: 2 (limit: 9444)
   Memory: 1.3M (peak: 2.2M)
      CPU: 35ms
   CGroup: /system.slice/chrony.service
           └─4664 /usr/sbin/chronyd -F 1
             └─4665 /usr/sbin/chronyd -F 1

abr 22 16:09:34 dc systemd[1]: Starting chrony.service - chrony, an NTP client/server...
abr 22 16:09:34 dc chronyd[4664]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RT>
abr 22 16:09:34 dc chronyd[4664]: Loaded 0 symmetric keys
abr 22 16:09:34 dc chronyd[4664]: Frequency -28.781 +/- 0.332 ppm read from /var/lib/chron>
abr 22 16:09:34 dc chronyd[4664]: Using right/UTC timezone to obtain leap second data
abr 22 16:09:34 dc chronyd[4664]: MS-SNTP authentication enabled
abr 22 16:09:34 dc chronyd[4664]: Loaded seccomp filter (level 1)
abr 22 16:09:34 dc systemd[1]: Started chrony.service - chrony, an NTP client/server.
abr 22 16:09:40 dc chronyd[4664]: Selected source 185.125.190.56 (ntp.ubuntu.com)
abr 22 16:09:40 dc chronyd[4664]: System clock TAI offset set to 37 seconds
lines 1-25/25 (END)

```

Verificar nombres de dominio

host -t A hjm.local

host -t A dc.hjm.local

```

usuario@dc:~$ host -t A hjm.local
hjm.local has address 192.168.1.8
hjm.local has address 192.168.237.24
usuario@dc:~$ host -t A dc.hjm.local
dc.hjm.local has address 192.168.1.8
dc.hjm.local has address 192.168.237.24
usuario@dc:~$

```

Verificar que los registros de servicio kerberos y ldap apunten al FQDN de su servidor Samba Active Directory.

host -t SRV _kerberos._udp.hjm.local

host -t SRV _ldap._tcp.hjm.local

```

usuario@dc:~$ host -t SRV _kerberos._udp.hjm.local
_kerberos._udp.hjm.local has SRV record 0 100 88 dc.hjm.local.
usuario@dc:~$ host -t SRV _ldap._tcp.hjm.local
_ldap._tcp.hjm.local has SRV record 0 100 389 dc.hjm.local.
usuario@dc:~$

```

Verificar los recursos predeterminados disponibles en Samba Active Directory.

`smbclient -L hjm.local -N`

```
usuario@dc:~$ smbclient -L hjm.local -N
Anonymous login successful

      Sharename      Type      Comment
      -
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC       IPC Service (Samba 4.19.5-Ubuntu)
SMB1 disabled -- no workgroup available
usuario@dc:~$
```

Comprobar autenticación en el servidor de Kerberos mediante el administrador de usuarios

`kinit administrator@hjm.LOCAL`

`klist`

```
usuario@dc:~$ kinit administrator@hjm.LOCAL
Password for administrator@hjm.LOCAL:
kinit: KDC reply did not match expectations while getting initial credentials
usuario@dc:~$ klist
klist: No credentials cache found (filename: /tmp/krb5cc_1000)
usuario@dc:~$
```

Iniciar sesión en el servidor a través de smb

`sudo smbclient //localhost/netlogon -U 'administrator'`

```
usuario@dc:~$ sudo smbclient //localhost/netlogon -U 'administrator'
Password for [HJM\administrator]:
Try "help" to get a list of possible commands.
smb: \>
```

Cambiar contraseña usuario administrador

`sudo samba-tool user setpassword administrator`

```
usuario@dc:~$ sudo samba-tool user setpassword administrator
New Password:
Retype Password:
Changed password OK
usuario@dc:~$
```

pass: usuario123*

Verificar la integridad del archivo de configuración de Samba.

testparm

```
usuario@dc:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions

```

Verificar funcionamiento WINDOWS AD DC 2008

sudo samba-tool domain level show

```
usuario@dc:~$ sudo samba-tool domain level show
Domain and forest function level for domain 'DC=hjm,DC=local'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
usuario@dc:~$ 
```

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)



General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP:

192 . 168 . 1 . 14

Máscara de subred:

255 . 255 . 255 . 0

Puerta de enlace predeterminada:

. . .

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

192 . 168 . 1 . 8

Servidor DNS alternativo:

. . .

☐ Validar configuración al salir

Opciones avanzadas...

Aceptar

Cancelar