

Installation on Debian 13

“ This expects a freshly installed Debian 13 (trixie) VM. **Not** an LXC container. Debian 13 ships Samba 4.22, which supports AD functional level 2016.

What you need

Decide on hostname, domain and IP before you start. Changing any of them after provisioning means starting over.

This guide uses:

Item	Value
Hostname	srv-dc01
DNS domain (realm)	samba-test.lan
NetBIOS domain	SAMBA-TEST
IP / prefix	10.0.0.5/20
Gateway	10.0.0.254
Upstream DNS	10.0.0.254

“ NetBIOS domain names are limited to 15 characters. Hyphens are allowed.

1. Preparation

Updates

```
apt update
apt full-upgrade -y
```

Core dependencies

```
apt install -y chrony vim ethtool
```

Hostname

```
hostnamectl set-hostname srv-dc01
```

Configure `/etc/hosts`. Remove the Debian default `127.0.1.1` line — the FQDN must resolve to the real IP:

```
127.0.0.1    localhost
10.0.0.5     srv-dc01.samba-test.lan srv-dc01
```

Verify:

```
hostname -f
```

Must return `srv-dc01.samba-test.lan`. If it does not, provisioning will fail.

Network

Modify `/etc/network/interfaces`.

⚠ Interface `ens18` might be named differently for you.

```
auto ens18
iface ens18 inet static
    address 10.0.0.5/20
    gateway 10.0.0.254
```

Disable the DHCP client

Do not skip this. It is the single most common way to break a Samba DC on Debian 13, and the failure only shows up much later as clients that cannot join the domain.

Since Trixie, `dhcpcd-base` has priority `important` instead of `isc-dhcp-client` on new installations. The Debian installer configures the interface via DHCP, and `ifup@<interface>.service` starts `dhcpcd` at boot. Switching `/etc/network/interfaces` to a static address afterwards does **not** stop the already running daemon — it keeps its lease, adds a second address to the interface and manages the default route.

Samba then registers *both* addresses in DNS. The Windows DC locator tries them in turn, hits the dead one and gives up.

Check:

```
ps aux | grep '[d]hcpcd'
ip -4 addr show ens18
```

If a `dhcpcd` process exists or the interface has a `secondary dynamic` address, find out what holds it:

```
systemctl status <pid-of-dhcpcd>
```

Note that `dhcpcd -x` does **not** work here — `ifupdown` starts the daemon per interface with its own control socket, not in master mode.

The clean fix is a reboot with the static configuration already in place:

```
echo 'denyinterfaces ens18' >> /etc/dhcpcd.conf
reboot
```

“ If you are connected over SSH, do not try to stop the interface manually — you will lock yourself out. Either reboot, or work from the VM console.

After the reboot, verify:

```
ip -4 addr show ens18      # only 10.0.0.5/20
ip route                   # one default route via 10.0.0.254
ps aux | grep '[d]hcpcd'   # empty
```

Also reserve or exclude the DC's address in your DHCP scope, so the pool never hands `10.0.0.5` to another machine.

Time synchronisation

```
systemctl enable --now chrony  
chronyc tracking
```

Kerberos tolerates a clock skew of ± 5 minutes. Aim for an offset well under 5 seconds — anything larger means chrony has not converged yet.

Signed NTP for Windows clients is configured later (section 7), because the socket directory does not exist until after provisioning.

Disable systemd-resolved

Samba's internal DNS server needs port 53.

```
systemctl disable --now systemd-resolved  
rm -f /etc/resolv.conf
```

Create `/etc/resolv.conf`:

“ For provisioning, point `nameserver` at your router or firewall so `apt` keeps working. It is switched to the DC itself in section 5.

```
nameserver 10.0.0.254  
search samba-test.lan
```

“ `/etc/resolv.conf` must never be left absent or empty. `samba_dnsupdate` reads it directly and aborts with `dns.resolver.NoResolverConfiguration: no nameservers` — which silently skips DNS record maintenance.

Ensure nothing is listening on port 53:

```
ss -tlnp | grep :53
```

This must return nothing.

2. Install Samba

```
apt install -y acl attr samba winbind libpam-winbind libnss-winbind \
krb5-config krb5-user dnsutils python3-setproctitle samba-ad-dc
```

`krb5-config` prompts during installation:

- **Default Kerberos version 5 realm:** `SAMBA-TEST.LAN` (uppercase)
- **Kerberos servers for your realm:** `srv-dc01.samba-test.lan`
- **Administrative server for your realm:** `srv-dc01.samba-test.lan`

These values are transient — `/etc/krb5.conf` is replaced in section 5.

Verify the AD DC modules are present:

```
dpkg -l samba-dsdb-modules samba-vfs-modules
samba -V
```

Without `samba-dsdb-modules` the DC will not start.

Mask conflicting services

Debian starts `smbd`, `nmbd` and `winbind` as standalone services immediately after installation. On an AD DC these must not run — the `samba` process provides its own internal file server and `winbind`. Leaving them active causes `samba-dcerpcd` to crash-loop and NSS lookups to hang.

```
systemctl disable --now smbd nmbd winbind
systemctl mask smbd nmbd winbind
```

3. Domain provisioning

Remove the packaged configuration file:

```
rm -f /etc/samba/smb.conf
```

Choose **one** of the two variants below.



Building a replacement for an existing domain? Then you do not provision at all — you join the existing domain as an additional DC. Skip to section 12 and come back here only for a standalone lab domain.

Variant A — default functional level (2008 R2)

Conservative, fully supported, matches most existing Samba deployments.

```
samba-tool domain provision --use-rfc2307 --realm=SAMBA-TEST.LAN \  
--domain=SAMBA-TEST --server-role=dc --dns-backend=SAMBA_INTERNAL \  
--adminpass='ChangeMe123!'
```

Variant B — functional level 2016

Required if the domain this DC will eventually replace runs at FL 2012 R2 or 2016, and needed for Kerberos claims, authentication policies and authentication silos.

```
samba-tool domain provision --use-rfc2307 --realm=SAMBA-TEST.LAN \  
--domain=SAMBA-TEST --server-role=dc --dns-backend=SAMBA_INTERNAL \  
--adminpass='ChangeMe123!' \  
--function-level=2016 \  
--option="ad dc functional level = 2016"
```

The `--option` only applies during provisioning. It **must** also be written permanently into `smb.conf` (section 5) — on every DC in the domain.

“ **Caveats for FL 2016.** Samba's implementation is partial and not enabled by default. Samba reads and writes claims and populates them into the PAC, but does not yet use them for access control decisions. Microsoft's PowerShell based AD tools are not expected to work. Functional levels cannot be lowered again.

“ If you omit `--adminpass`, a random password is generated and printed to the console in cleartext, where it lands in your scrollbar and terminal logs.

4. Deploy Kerberos configuration

```
cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Copy the file — do not symlink it.

5. Configure DNS and `smb.conf`

Point the resolver at the DC itself. Rewrite `/etc/resolv.conf`:

```
nameserver 10.0.0.5
search samba-test.lan
```

Add the following to the **existing** `[global]` section of `/etc/samba/smb.conf` — do not create a second `[global]` block:

```
dns forwarder = 10.0.0.254

# Variant B only — must be present on every DC
ad dc functional level = 2016
```

On first startup, `ad dc functional level` updates the server's own AD entry with the configured level.

Check the file parses:

```
testparm -s
```

6. Start Samba

```
systemctl unmask samba-ad-dc
systemctl enable --now samba-ad-dc
systemctl status samba-ad-dc
```

If the service fails to start, the two usual causes are a port 53 conflict (check `ss -tlnp | grep :53`) and `server role` not being set to `active directory domain controller` in `smb.conf`.

7. Post-provisioning tasks

Set the domain administrator password

```
samba-tool user setpassword Administrator
```

Review the password policy

```
samba-tool domain passwordsettings show
```

Samba defaults to a maximum password age of 43 days. In a lab this will expire on you at the worst possible moment:

```
samba-tool domain passwordsettings set --max-pwd-age=0
```

Do not do this in production — use the policy your organisation requires.

Verify sysvol ACLs

```
samba-tool ntacl sysvolcheck
```

If it reports errors:

```
samba-tool ntacl sysvolreset
```

Create the reverse DNS zone

Provisioning does not create one.

```
samba-tool dns zonecreate srv-dc01 0.0.10.in-addr.arpa -U Administrator
```



A `/20` network spans `10.0.0.x` through `10.0.15.x`. Either create all 16 zones or use `10.in-addr.arpa` instead.

Signed NTP for Windows clients

Domain members expect authenticated time (MS-SNTP) from a DC. Without this, clients stay on `Local CMOS Clock`, drift out of the ± 5 minute Kerberos window and eventually fail authentication with `KRB_AP_ERR_SKEW`.

The socket directory exists only after provisioning. Samba creates it as `root:root`, but chrony runs as `_chrony` and needs group access:

```
chgrp _chrony /var/lib/samba/ntp_signd
chmod 750 /var/lib/samba/ntp_signd
ls -ld /var/lib/samba/ntp_signd
```

Make the ownership survive — a `samba-ad-dc` restart can recreate the directory and reset the group, after which chrony silently drops back to unsigned operation:

```
echo 'd /var/lib/samba/ntp_signd 0750 root _chrony -' > /etc/tmpfiles.d/samba-ntp-signd.conf
systemd-tmpfiles --create
```

Add to `/etc/chrony/chrony.conf`:

```
ntpsigndsocket /var/lib/samba/ntp_signd
allow 10.0.0.0/20
```

```
systemctl restart chrony
```

Verify — do not skip. Both checks must pass:

```
ss -ulnp | grep :123
journalctl -u chrony -n 20 --no-pager | grep -i 'MS-SNTP'
```

Expected: a listener on `0.0.0.0:123`, and the log line `MS-SNTP authentication enabled`. If that line is missing, chrony started without the signing socket — almost always a permissions problem on `/var/lib/samba/ntp_signd`. Fix it and restart chrony; there is no warning about this in normal operation.

Also confirm chrony itself is synchronised upstream:

```
chronyc tracking
chronyc sources
```

A DC that is not synchronised cannot serve time to anyone.

Take a snapshot

Snapshot the VM here — freshly provisioned, no clients joined. Domain join tests can then be repeated from a known state.

8. Verification

Services and listeners

```
ss -tlnp | grep -E ':(53|88|389|445|464|636)\b'
smbclient -L localhost -N
```

Expected listeners: 53 (DNS), 88 (Kerberos), 389 (LDAP), 445 (SMB), 464 (kpasswd), 636 (LDAPS).
`smbclient` must show the `netlogon` and `sysvol` shares.

DNS records

```
host -t SRV _ldap._tcp.samba-test.1an localhost
host -t SRV _kerberos._udp.samba-test.1an localhost
host -t A srv-dc01.samba-test.1an localhost
```

Repeat from **another host** on the network — this is what clients actually do:

```
host -t SRV _ldap._tcp.samba-test.1an 10.0.0.5
```

Kerberos

```
kinit administrator@SAMBA-TEST.LAN
klist
```

The ticket must show realm `SAMBA-TEST.LAN`.

Directory consistency

```
samba-tool dbcheck --cross-ncs  
getent passwd administrator
```

`getent` proves NSS resolution through the internal winbind works.

Functional level

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

Variant A reports `(Windows) 2008 R2`, Variant B reports `(Windows) 2016`.

9. Raising an existing domain from 2008 R2 to 2016

Only needed if you provisioned with Variant A and now need a higher level.

“ **Functional levels cannot be lowered.** Take a backup and verify it before starting.

Back up first

```
samba-tool domain backup offline --targetdir=/srv/backup  
samba-tool dbcheck --cross-ncs
```

Enable the feature

Add to the `[global]` section of `/etc/samba/smb.conf` **on every DC**:

```
ad dc functional level = 2016
```

Restart Samba on every DC:

```
systemctl restart samba-ad-dc
```

Upgrade schema and raise the level

```
samba-tool domain schemaupgrade --schema=2019  
samba-tool domain functionalprep --function-level=2016  
samba-tool domain level raise --domain-level=2016 --forest-level=2016
```

Verify

```
samba-tool domain level show  
samba-tool dbcheck --cross-ncs
```

10. Domain join test

Prepare the client

Set the DC as the **only** DNS server — not the router, not a public resolver, not both. This is the cause of most "domain could not be contacted" errors: if a second resolver answers first, Windows caches its `NXDOMAIN` for the domain and never asks the DC.

```
Get-DnsClientServerAddress -AddressFamily IPv4  
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.5  
Clear-DnsClientCache
```

If the addresses come from DHCP, fix option 6 in the scope — otherwise the router returns on the next lease renewal.

Confirm the client can find a DC before attempting the join:

```
Resolve-DnsName -Name samba-test.lan -Server 10.0.0.5  
Resolve-DnsName -Name _ldap._tcp.dc._msdcs.samba-test.lan -Type SRV -Server 10.0.0.5
```

```
Test-NetConnection -ComputerName 10.0.0.5 -Port 389
```

The A record for the domain must return exactly **one** address. More than one means stale records — see the appendix.

Join and verify

After joining, from the DC:

```
samba-tool computer list  
samba-tool user list
```

The client should have registered itself in DNS via GSS-TSIG:

```
host -t A <client-hostname>.samba-test.lan 127.0.0.1
```

If nothing comes back, dynamic updates are not working — this does not block the join, but breaks name resolution for services later.

Time synchronisation

```
w32tm /query /configuration | findstr /i "Type"  
w32tm /resync /rediscover  
w32tm /query /source  
w32tm /query /status
```

`Type` must be `NT5DS`. `Source` must change to `srv-dc01.samba-test.lan`, `Stratum` must be non-zero, and `Last Successful Sync Time` must show a timestamp. If the source stays `Local CMOS Clock`:

```
Restart-Service w32time  
w32tm /resync /rediscover  
w32tm /stripchart /computer:srv-dc01.samba-test.lan /samples:3 /dataonly
```

On the DC, confirm the request actually arrives:

```
chronyc clients
```

If the client appears here with NTP counters but still refuses to sync, the replies are unsigned — go back to the MS-SNTP check in section 7.

Domain logon

A machine join does not prove that user authentication works.

```
samba-tool user create testuser  
samba-tool group addmembers "Domain Admins" testuser
```

Log on to the client as `SAMBA-TEST\testuser`, then:

```
klist
```

There must be a TGT and service tickets. Also open `\\samba-test.lan\sysvol` in Explorer, and check group policy handling:

```
samba-tool gpo listall
```

11. Before going to production

- **Backups.** `samba-tool domain backup offline` on a schedule, plus a tested restore. A DC without a verified restore path is not a DC you can rely on.
- **Second DC.** Join a second controller and verify replication with `samba-tool drs showrepl`.
- **sysvol replication.** Samba does **not** replicate sysvol between DCs. This has to be built separately with rsync or osync. This surprises people migrating from Windows AD with DFS-R.
- **Monitoring.** Add LDAP, Kerberos and DNS service checks plus `samba-tool drs showrepl` to your monitoring.
- **FSMO roles.** When replacing an existing DC, transfer the roles with `samba-tool fsmo transfer` before demoting the old one.

12. Alternative path: joining an existing domain

Use this **instead of** sections 3 to 5 when the new DC is meant to become part of an existing domain — whether that domain is served by Windows DCs or by Samba. Provisioning would create a *separate* domain that shares nothing with the existing one.

Sections 1 and 2 (preparation, package installation, service masking) apply unchanged. Sections 6 onwards apply after the join, with the differences noted below.

Prerequisites

Check these before starting. A failed join leaves partial objects in the directory that have to be cleaned up manually.

Functional level and schema. Samba must support the level the existing domain runs at. Query it from an existing DC:

```
samba-tool domain level show -H ldap://<existing-dc> -U Administrator
```

Samba 4.22 handles up to 2016. If the source domain is higher, the join will not work.

Time. The new DC must be within the Kerberos skew of the existing domain. Point chrony at the existing DC rather than a public pool:

```
server <existing-dc-fqdn> iburst
```

```
systemctl restart chrony  
chronyc tracking
```

DNS. `/etc/resolv.conf` on the new machine must point at an existing DC — not the router, not a public resolver:

```
nameserver <existing-dc-ip>  
search samba-test.lan
```

Verify the domain is discoverable:

```
host -t SRV _ldap._tcp.dc._msdcs.samba-test.lan  
host -t SRV _kerberos._tcp.samba-test.lan
```

Kerberos. Create `/etc/krb5.conf` before joining — the generated one from provisioning does not exist yet:

```
[libdefaults]  
    default_realm = SAMBA-TEST.LAN  
    dns_lookup_realm = false  
    dns_lookup_kdc = true
```

Test it:

```
kinit Administrator@SAMBA-TEST.LAN  
klist
```

If this fails, the join will fail too. Fix it here.

Clean slate. If you previously provisioned on this machine, wipe it:

```
systemctl stop samba-ad-dc  
rm -f /etc/samba/smb.conf  
rm -rf /var/lib/samba/private/* /var/cache/samba/* /var/lib/samba/sysvol/*
```

Join

```
samba-tool domain join samba-test.lan DC \  
-U Administrator \  
--dns-backend=SAMBA_INTERNAL \  
--option="ad dc functional level = 2016"
```

Useful additions:

- `--server=<existing-dc-fqdn>` — replicate from a specific DC instead of whichever one DNS returns. Worth setting when the source DCs are in different sites.
- `--site=<site-name>` — place the DC in a specific AD site. Defaults to `Default-First-Site-Name`.

Drop `--option="ad dc functional level = 2016"` if the domain runs below 2016. Where it applies, it must be written permanently into `smb.conf` as well.

The join replicates the full directory. On a domain with many objects this takes a while and produces little output — let it run.

After the join

Point the resolver at the new DC itself and add the forwarder, as in section 5:

```
nameserver 10.0.0.5  
search samba-test.lan
```

```
dns forwarder = 10.0.0.254
```

```
# only where the domain runs at 2016
ad dc functional level = 2016
```

Then start Samba as in section 6:

```
systemctl unmask samba-ad-dc
systemctl enable --now samba-ad-dc
```

Register the new DC's own DNS records:

```
samba_dnsupdate --verbose --all-names
```

Verify replication

This is the check that matters — the join can succeed while replication does not.

```
samba-tool drs showrepl
```

Every partition must show recent successful inbound and outbound replication with zero consecutive failures. Force a run to be sure:

```
samba-tool drs replicate <new-dc> <existing-dc> DC=samba-test,DC=lan
samba-tool drs replicate <existing-dc> <new-dc> DC=samba-test,DC=lan
```

Confirm the new DC is visible domain-wide:

```
samba-tool computer list | grep -i srv-dc01
host -t SRV _ldap._tcp.dc._msdcs.samba-test.lan 127.0.0.1
```

The SRV record must now list both DCs.

sysvol

Samba does not replicate sysvol. The join brings the directory database, not the policy files. Copy them once from an existing DC and repair the ACLs:

```
rsync -aAXv --delete root@<existing-dc>:/var/lib/samba/sysvol/ /var/lib/samba/sysvol/
samba-tool ntacl sysvolreset
samba-tool ntacl sysvolcheck
```

For ongoing operation this has to be automated — rsync on a timer or osync for bidirectional sync. Coming from Windows AD with DFS-R, this is the single biggest operational difference and the most common thing to forget.

Replacing the old DC

Only once replication has been verified and has run cleanly for a while.

Transfer the FSMO roles:

```
samba-tool fsmo show
samba-tool fsmo transfer --role=all -U Administrator
samba-tool fsmo show
```

Then demote the old DC. On a Samba DC:

```
samba-tool domain demote -U Administrator
```

On a Windows DC, use `dcpromo` / Server Manager. Only if the old DC is already gone and cannot be demoted properly:

```
samba-tool domain demote --remove-other-dead-server=<old-dc-name> -U Administrator
```

Afterwards, clean up its DNS records and check the directory:

```
samba-tool dns query localhost samba-test.ian @ A -U Administrator
samba-tool dbcheck --cross-ncs
samba-tool drs showrepl
```

Finally, repoint clients and DHCP option 6 at the new DC.

Appendix: cleaning up stale A records

If the DC ever held a second IP address — a DHCP lease, a temporary interface, a changed address — `samba_dnsupdate` will have registered it, and the record survives after the address is gone.

Symptom: domain joins fail intermittently, `dcdiag` reports `DNS name does not exist` for `_ldap._tcp.dc._msdcs.<domain>`.

Fix the interface first. As long as a DHCP client is running, records are re-registered as fast as you delete them.

```
ip -4 addr show ens18      # must show only the static address
```

Then inspect every name that carries an A record for the DC:

```
samba-tool dns query localhost samba-test.lan @ A -U Administrator
samba-tool dns query localhost samba-test.lan srv-dc01 A -U Administrator
samba-tool dns query localhost samba-test.lan DomainDnsZones A -U Administrator
samba-tool dns query localhost samba-test.lan ForestDnsZones A -U Administrator
samba-tool dns query localhost _msdcs.samba-test.lan gc A -U Administrator
```

The simplest repair is to let Samba do it — with a valid `/etc/resolv.conf` in place, `samba_dnupdate` removes stale entries by itself:

```
printf 'nameserver 127.0.0.1\nsearch samba-test.lan\n' > /etc/resolv.conf
samba_dnupdate --verbose --all-names
```

Watch for `need delete:` lines in the output — those are the stale records. The run must finish without a traceback, otherwise the deletes never happen.

To remove records manually instead, per name and per address:

```
samba-tool dns delete localhost samba-test.lan @ A 10.0.1.108 -U Administrator
samba-tool dns delete localhost samba-test.lan srv-dc01 A 10.0.1.108 -U Administrator
samba-tool dns delete localhost samba-test.lan DomainDnsZones A 10.0.1.108 -U Administrator
samba-tool dns delete localhost samba-test.lan ForestDnsZones A 10.0.1.108 -U Administrator
samba-tool dns delete localhost _msdcs.samba-test.lan gc A 10.0.1.108 -U Administrator
```

`WERR_DNS_ERROR_RECORD_DOES_NOT_EXIST` simply means that name was already clean.

Verify:

```
host -t A samba-test.lan 127.0.0.1
host -t A srv-dc01.samba-test.lan 127.0.0.1
host -t A gc._msdcs.samba-test.lan 127.0.0.1
```

Each must return exactly one address. Finally, flush the client cache — Windows will otherwise keep serving the old answers:

```
Clear-DnsClientCache
Resolve-DnsName -Name samba-test.lan -Server 10.0.0.5
```

Revision #9

Created 25 July 2026 14:22:28 by Oliver Karger

Updated 25 July 2026 16:22:08 by Oliver Karger