
NFS Roaming Home Directories – Implementation Documentation

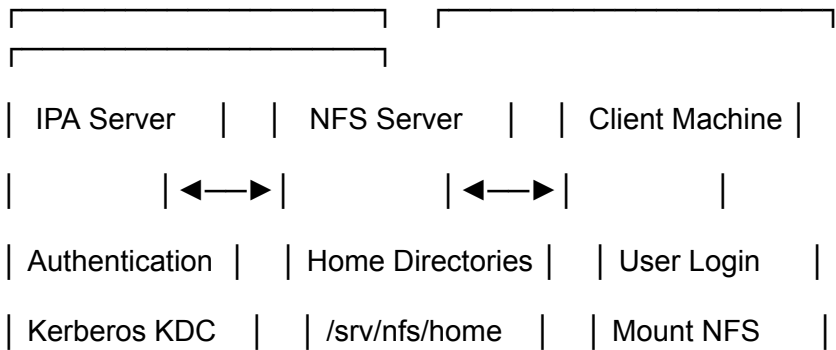
Status:  Working Implementation
Last Updated: September 6, 2025
Environment: `HOMELAB.LAN` Kerberos realm with NFSv4

Architecture

Components

- **Kerberos Realm:** `HOMELAB.LAN`
- **NFS Server:** `server.homelab.lan`
- **Authentication:** Kerberos (`krb5p` security)
- **File System:** NFSv4
- **Client Mounting:** `autofs`

Network Layout



Server Configuration (**server.homelab.lan**)

Directory Structure

/srv/nfs/home/

- |— brett/ (700 permissions, brett:brett ownership)
- |— alice/ (700 permissions, alice:alice ownership)
- |— [users]/ (700 permissions, user:user ownership)

/etc/exports

/srv/nfs/home *.homelab.lan(rw, sync, no_subtree_check, sec=krb5p, fsid=0)

Services

- **nfs-kernel-server**
- **rpcbind**
- Kerberos services via FreeIPA



Client Configuration

Required Packages

Debian/Ubuntu

```
sudo apt update
```

```
sudo apt install freeipa-client sssd-ipa sssd-tools autofs nfs-common oddjob-mkhomedir -y
```

RHEL/Rocky

```
sudo dnf install nfs-utils krb5-workstation autofs
```

Arch/CachyOS

```
sudo pacman -S --needed sssd krb5 nfs-utils autofs
```

```
sudo paru -s autofs cachefilesd
```

```
sudo systemctl enable --now autofs
```

```
sudo systemctl enable --now cachefilesd
```

Kerberos Setup

- Client joined to **HOMELAB.LAN** realm
- Host principal added to IPA
- **/etc/krb5.keytab** installed

```
› cat /etc/krb5.conf
```

```
[libdefaults]
```

```
default_realm = HOMELAB.LAN
```

```
dns_lookup_realm = false
```

```
dns_lookup_kdc = true
```

```
rdns = false
```

```
ticket_lifetime = 24h  
forwardable = true  
default_ccache_name = KEYRING:persistent:%{uid}
```

```
[realms]
```

```
HOMELAB.LAN = {  
    kdc = ipa.homelab.ian  
    admin_server = ipa.homelab.ian  
}
```

```
[domain_realm]
```

```
.homelab.ian = HOMELAB.LAN  
homelab.ian = HOMELAB.LAN
```

User Login Workflow

1. User logs in → PAM calls SSSD → Kerberos TGT issued (**ry@HOMELAB.LAN**)
2. PAM session stack triggers autofs mount of **/home/ry**
3. Autofs consults **/etc/auto.home** → maps to NFS export
 - a. NFS client authenticates with Kerberos (**sec=krb5p**)

4. User lands in `/home/ry` backed by NFS server

AutoFS Implementation

Install autofs

Debian/Ubuntu

```
sudo apt install autofs
```

RHEL/Rocky

```
sudo dnf install autofs
```

`/etc/auto.master`

```
/home /etc/auto.home --timeout=60 --ghost
```

`/etc/auto.home`

```
* -fstype=nfs4,rw,hard,intr,sec=krb5p server.homelab.lan:/srv/nfs/home/&
```

Local Caching (FS-Cache + cachefilesd)

Purpose

Enables **local disk caching** of NFS homes, improving performance especially on Wi-Fi/Tailscale clients.

- Faster desktop logins and app launches (Firefox, IDEs)

- Reduced latency for small config reads/writes
- Resilience during short Wi-Fi drops

Configuration

Enable kernel module

```
sudo modprobe cachefiles
```

Install & start cachefilesd

```
sudo apt install cachefilesd
```

```
sudo systemctl enable --now cachefilesd
```

Update `/etc/auto.home`

```
* -fstype=nfs4,rw,sec=krb5p,fsc,rsiz=131072,wsiz=131072,hard,timeo=600,retrans=2
server.homelab.lan:/srv/nfs/home/&
```

(`fsc` enables FS-Cache.)

PAM Integration

In both `/etc/pam.d/common-session` and `/etc/pam.d/common-session-noninteractive`, before `pam_mkhomedir.so`:

```
# Trigger autofs for real users (skip root/sudo); run as user
```

```
session optional pam_exec.so quiet setuid /bin/sh -c '[ "$PAM_USER" = "root" ] || [
"$PAM_SERVICE" = "sudo" ] || ls -d "/home/$PAM_USER" >/dev/null 2>&1 || true'
```

```
# Create home if missing
```

```
session optional pam_mkhomedir.so
```

Verification

Check mount

```
findmnt /home/ry -o TARGET,SOURCE,FSTYPE,OPTIONS
```

```
# Look for ",fsc," in OPTIONS
```

Check cache stats

```
cat /proc/fs/fscache/stats | head -n 20
```

Offline Behavior

-  Reads from cached files still work if Wi-Fi drops
-  Writes fail if the server is unavailable
-  Uncached files cannot be opened offline
-  Designed for performance + resilience, not true offline work

Tuning (Optional)

Edit `/etc/cache/filesd.conf`:

```
dir /var/cache/fscache
```

```
tag nfs-cache
```

```
brun 10%
```

```
bcull 7%
```

```
bstop 3%
```

Restart:

```
sudo systemctl restart cachefilesd
```

Deployment Guidance

- **Enable FS-Cache** on laptops and Wi-Fi clients
 - **Optional** on wired desktops (LAN latency already low)
 - **Not required** on NFS servers
-

Troubleshooting

Common Issues

Mount Permission Denied

→ Check Kerberos tickets with `klist`, renew with `kinit`.

Directory Not Found

→ Verify directory exists under `/srv/nfs/home/username`.

Permission Denied Inside Home

→ Fix ownership with `chown -R user:user /srv/nfs/home/user`.

Stale NFS Handles

→ `umount -f` then remount.

Local User Conflict

→ Remove or migrate old local user before using IPA accounts.

Client Hostname Issues

→ Must be FQDN: `sudo hostnamectl set-hostname host.homelab.lan`.

Security Considerations

- Kerberos authentication for all NFS mounts (`krb5p`)
 - Encrypted traffic
 - Home dirs set `700`
 - NFS limited to `*.homelab.lan`
 - Rotate Kerberos keys regularly
 - Monitor access logs and patch servers
-