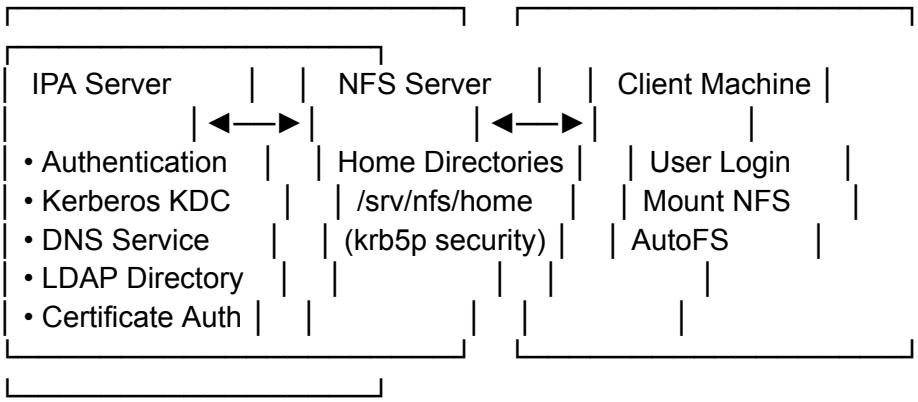
# 📘 FreeIPA Server Setup Documentation

**THIS IS ONLY THE IPA SERVER; NFS SERVER IS COVERED UNDER CLIENT DOCUMENTATIN.**

**Status:** ✅ Production Ready
**Last Updated:** September 16, 2025
**Environment:** Rocky Linux 10 with HOMELAB.LAN realm
**Compatibility:** Matches existing NFS roaming home directories implementation

## 🏗️ Architecture Overview




**Key Components:**

- **Realm:** HOMELAB.LAN
- **Domain:** homelab.lan
- **Primary IPA Server:** ipa.homelab.lan (192.168.1.111)
- **Existing DNS Server:** dns.homelab.lan (192.168.1.200)
- **NFS Server:** server.homelab.lan (can be same as IPA server)
- **Network:** 192.168.1.0/24
- **DNS Integration:** Full DNS management with dynamic updates
- **Security:** Kerberos authentication with krb5p encryption

## 📋 Prerequisites

### Hardware Requirements

- **CPU:** 2+ cores (4 recommended for production)
- **Memory:** 4GB minimum (8GB+ recommended)
- **Storage:** 20GB minimum (more for user data and logs)
- **Network:** Static IP address, proper DNS resolution

### Network Prerequisites

- Static IP configuration (192.168.1.111 for IPA server)
- Resolvable FQDN (ipa.homelab.lan)
- Access to existing DNS server (dns.homelab.lan at 192.168.1.200)
- Required ports accessible (see Security section)
- NTP synchronization capability

### Rocky Linux Requirements

- Rocky Linux 9.0+ (fresh minimal installation preferred)
- Root access or sudo privileges
- SELinux enabled (default Rocky configuration)
- Firewall properly configured

## 🚀 Installation Process

### Step 1: System Preparation

```
# Update the system
sudo dnf update -y
sudo reboot  # If kernel was updated

# Check system version
cat /etc/rocky-release
uname -r
```

### Step 2: Network Configuration

```
# Set the FQDN hostname
sudo hostnamectl set-hostname ipa.homelab.lan

# Configure static IP (adjust interface name as needed)
sudo nmcli connection modify ens160 \
    ipv4.method manual \
    ipv4.address 192.168.1.111/24 \
    ipv4.gateway 192.168.1.1 \
    ipv4.dns "192.168.1.200,192.168.1.111"
```

```
# Apply network changes
sudo nmcli connection down ens160 && nmcli connection up ens160

# Add hostname to /etc/hosts
echo "192.168.1.111 ipa.homelab.lan ipa" | sudo tee -a /etc/hosts

# Verify hostname resolution
ping -c 3 ipa.homelab.lan
```

## Step 3: Time Configuration

```
# Set timezone (adjust as needed)
sudo timedatectl set-timezone America/Denver

# Verify time configuration
timedatectl
```

## Step 4: Package Installation

```
# Install FreeIPA server packages
sudo dnf install -y freeipa-server freeipa-server-dns freeipa-client

# Verify installation
rpm -qa | grep freeipa
```

## Step 5: Firewall Configuration

```
# Configure firewall for FreeIPA
sudo firewall-cmd --permanent --add-service=freeipa-4

# If NFS server is on same host, also add NFS services
sudo firewall-cmd --permanent --add-service=nfs
sudo firewall-cmd --permanent --add-service=mountd
sudo firewall-cmd --permanent --add-service=rpc-bind

# Reload firewall
sudo firewall-cmd --reload

# Verify firewall rules
sudo firewall-cmd --list-services --permanent
```

# ⚙️ FreeIPA Server Configuration

## Interactive Installation (Recommended for first-time setup)

sudo ipa-server-install --setup-dns

**Interactive Prompts:**

- Server host name: `ipa.homelab.lan`
- Domain name: `homelab.lan`
- Realm name: `HOMELAB.LAN`
- Directory Manager password: `[secure_password]`
- IPA admin password: `[secure_password]`
- DNS forwarders: `192.168.1.200` (your existing DNS server)
- Continue with these values: `yes`

## Unattended Installation (For automation)

```
sudo ipa-server-install \
    --unattended \
    --realm HOMELAB.LAN \
    --domain homelab.lan \
    --ds-password 'SecureP@ssw0rd123!' \
    --admin-password 'AdminP@ssw0rd123!' \
    --setup-dns \
    --auto-reverse \
    --forwarder 192.168.1.200 \
    --no-ntp
```

## Installation Verification

```
# Check IPA server status
sudo ipactl status

# Get Kerberos ticket for admin
kinit admin
# Enter admin password when prompted

# Verify ticket
klist

# Check IPA version
ipa --version
```

```
# Test basic functionality
ipa config-show
```

# 🔧 Post-Installation Configuration

## DNS Configuration

**Important:** You have an existing DNS server at dns.homelab.lan (192.168.1.200). The IPA server will handle DNS for the homelab.lan domain, but you'll need to coordinate with your existing DNS infrastructure.

```
# Allow zone transfers (adjust network as needed)
ipa dnszone-mod homelab.lan --allow-transfer=192.168.1.0/24

# Add mail exchange record (if using email)
ipa dnsrecord-add homelab.lan @ --mx-rec="10 mail.homelab.lan"

# Add additional DNS records as needed
# Example: NFS server record (if separate from IPA)
ipa dnsrecord-add homelab.lan server --a-rec=192.168.1.112

# Verify existing DNS server integration
dig @192.168.1.200 ipa.homelab.lan
dig @192.168.1.111 ipa.homelab.lan
```

**DNS Integration Notes:**

- IPA server at 192.168.1.111 will be authoritative for homelab.lan domain
- Existing DNS server at 192.168.1.200 should delegate homelab.lan to IPA server

Update your existing DNS server to add delegation:

```
homelab.lan.  IN  NS  ipa.homelab.lan.ipa          IN  A   192.168.1.111
```

-

## NFS Service Configuration (if IPA server hosts NFS)

```
# Install NFS packages (if not already installed)
sudo dnf install -y nfs-utils

# Enable NFS services
sudo systemctl enable --now nfs-server rpcbind
```

```
# Create NFS export directory
sudo mkdir -p /srv/nfs/home

# Configure NFS exports
echo '/srv/nfs/home    *.homelab.lan(rw,sync,no_subtree_check,sec=krb5p,fsid=0)' | sudo tee -a
/etc/exports

# Export the share
sudo exportfs -rav

# Add NFS service principal to IPA
ipa service-add nfs/ipa.homelab.lan

# Add NFS principal to keytab
sudo kadmin.local -q "ktadd nfs/ipa.homelab.lan"
```

### User Home Directory Configuration

```
# Configure default home directory and shell for new users
ipa config-mod --homedirectory=/srv/nfs/home --defaultshell=/bin/bash

# Verify configuration
ipa config-show | grep -E "(Home directory|Default shell)"
```

### SSL Certificate Configuration

```
# Backup CA certificates (CRITICAL for replicas)
sudo cp /root/cacert.p12 /root/cacert.p12.backup

# Verify web interface certificate
openssl s_client -connect ipa.homelab.lan:443 -servername ipa.homelab.lan < /dev/null
```

## 👥 User Management

**WebUI is almost always the answer for User Managerment!!!!**
**Follow below for super nerd points.**

### Creating Users

```
# Create a new user with home directory
ipa user-add brett \
```

```
    --first=Brett \
    --last=Doe \
    --password \
    --homedir=/srv/nfs/home/brett

# Create the home directory with proper permissions
sudo mkdir -p /srv/nfs/home/brett
sudo chown brett:brett /srv/nfs/home/brett
sudo chmod 700 /srv/nfs/home/brett
```

### Creating Groups

```
# Create user groups
ipa group-add developers --desc="Development team"
ipa group-add admins --desc="System administrators"

# Add users to groups
ipa group-add-member developers --users=brett
ipa group-add-member admins --users=admin
```

### Host Management

```
# Add client hosts to IPA
ipa host-add client1.homelab.lan --ip-address=192.168.1.100
ipa host-add client2.homelab.lan --ip-address=192.168.1.101

# Generate enrollment passwords
ipa host-add client3.homelab.lan --random
```

## 🌐 Web Interface

### Access Methods

- **Primary URL:** https://ipa.homelab.lan/ipa/ui
- **Alternative:** https://192.168.1.111/ipa/ui

### Web Interface Features

- User and group management
- Host and service management
- DNS record management
- Certificate management

- Sudo rules and HBAC policies
- Audit logs and monitoring

### First Login

1. Navigate to https://ipa.homelab.lan/ipa/ui
2. Accept the self-signed certificate (or install CA cert)
3. Login as `admin` with the password set during installation
4. Explore the Identity, Policy, and Authentication tabs

## 🔒 Security Configuration

### Required Network Ports

#### TCP Ports:

- 80, 443: HTTP/HTTPS (Web UI and API)
- 389, 636: LDAP/LDAPS (Directory service)
- 88, 464: Kerberos (Authentication)
- 53: DNS (Name resolution)
- 2049: NFS (if hosting home directories)

#### UDP Ports:

- 88, 464: Kerberos
- 53: DNS
- 123: NTP (time synchronization)

### SELinux Configuration

```
# Verify SELinux is enabled and enforcing
getenforce

# Check for any IPA-related SELinux denials
sudo ausearch -m avc -ts recent | grep ipa

# If needed, generate custom SELinux policies
sudo audit2allow -a -M ipa-custom
sudo semodule -i ipa-custom.pp
```

### Kerberos Security

```
# List available Kerberos principals
ipa service-find
```

```
# Set strong password policies
ipa pwpolicy-mod --minlength=12 --minclasses=3

# Configure password expiration
ipa pwpolicy-mod --maxlife=90 --minlife=1
```

# 🔄 Backup and Recovery

## Critical Backup Items

```
#!/bin/bash
# IPA Backup Script
BACKUP_DIR="/backup/ipa/$(date +%Y%m%d-%H%M%S)"
mkdir -p "$BACKUP_DIR"

# IPA-specific backup
ipa-backup --data --logs --online

# Copy backup to secure location
cp -r /var/lib/ipa/backup/* "$BACKUP_DIR/"

# Backup certificates
cp /root/cacert.p12 "$BACKUP_DIR/"
cp /etc/pki/ca-trust/source/anchors/ipa-ca.crt "$BACKUP_DIR/"

# Backup configuration files
cp /etc/ipa/default.conf "$BACKUP_DIR/"
cp /etc/sssd/sssd.conf "$BACKUP_DIR/"
cp /etc/krb5.conf "$BACKUP_DIR/"

echo "Backup completed: $BACKUP_DIR"
```

## Automated Backups

```
# Create backup script
sudo tee /usr/local/bin/ipa-backup.sh << 'EOF'
#!/bin/bash
BACKUP_DIR="/backup/ipa"
DATE=$(date +%Y%m%d-%H%M%S)

mkdir -p "$BACKUP_DIR"
ipa-backup --data --logs --online
```

```
find /var/lib/ipa/backup -name "*$DATE*" -exec cp -r {} "$BACKUP_DIR/" \;

# Keep only last 30 days of backups
find "$BACKUP_DIR" -type d -mtime +30 -exec rm -rf {} \;
EOF

sudo chmod +x /usr/local/bin/ipa-backup.sh

# Create daily backup cron job
echo "0 2 * * * /usr/local/bin/ipa-backup.sh" | sudo crontab -
```

# 🧪 Testing and Validation

## Basic Functionality Tests

```
# Test Kerberos authentication
kinit admin
klist

# Test LDAP connectivity
ldapsearch -x -h ipa.homelab.lan -b "dc=homelab,dc=lan" "(uid=admin)"

# Test DNS resolution
dig @ipa.homelab.lan ipa.homelab.lan
dig @192.168.1.200 ipa.homelab.lan  # Test with existing DNS
dig @ipa.homelab.lan -x 192.168.1.111

# Test web interface
curl -k https://ipa.homelab.lan/ipa/json
```

## Client Connectivity Tests

```
# From a client machine
ipa-client-install --domain=homelab.lan --server=ipa.homelab.lan --unattended
--enable-dns-updates
```

# 🔧 Troubleshooting

## Common Issues and Solutions

### Issue: Installation fails with "DNS resolution error"

```
# Solution: Verify hostname and DNS configuration
hostnamectl
cat /etc/hosts
systemctl status systemd-resolved
```

**Issue: Web interface not accessible**

```
# Check Apache status
sudo systemctl status httpd

# Check certificates
sudo openssl x509 -in /etc/httpd/alias/server.crt -text -noout

# Restart web services
sudo systemctl restart httpd
```

**Issue: Kerberos authentication failures**

```
# Check KDC status
sudo systemctl status krb5kdc

# Verify time synchronization
timedatectl status

# Check Kerberos configuration
sudo ktutil -k /etc/krb5.keytab list
```

**Issue: DNS not working properly**

```
# Check named service
sudo systemctl status named

# Verify zone files
sudo named-checkconf
sudo named-checkzone homelab.lan /var/named/dynamic/homelab.lan.db
```

## Log Locations

- **IPA Installation:** `/var/log/ipaserver-install.log`
- **General IPA logs:** `/var/log/ipa/`
- **Directory Server:** `/var/log/dirsrv/slapd-HOMELAB-LAN/`
- **Kerberos:** `/var/log/krb5kdc.log`
- **Apache:** `/var/log/httpd/`

- **Named/DNS:** `/var/log/named.log`

## Useful Diagnostic Commands

```
# IPA server status
sudo ipactl status

# Check all IPA services
sudo systemctl status ipa

# View recent logs
sudo journalctl -u ipa -f

# Test LDAP connectivity
ldapsearch -Y GSSAPI -H ldap://ipa.homelab.lan -b "dc=homelab,dc=lan"

# Verify DNS zones
ipa dnszone-find
```