Task: Add the following information to the local DNS file and Server

Requirements:

VM server
DNS info:

[sanitized info]
10.1.30.x ipa.procrore.dev
10.1.30.x dev-ansible.procore.prod1 dev-ansible
10.1.30.x stage-bastion.procore.prod1 stage-bastion
10.1.30.x stage-foreman.procore.prod1
10.1.30.x dev-nfs.procore.prod1
10.1.30.x stage.graylog.procore.dev

I updated the /etc/hosts file to add static hostname-to-IP mappings for the FreeIPA server and related environment systems, ensuring reliable name resolution when DNS is unavailable or during initial configuration.

All of these ip addresses are for practice purposes only, they have all been deleted

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1          localhost localhost.localdomain localhost6 localhost6.localdomain6

10.1.15.13   ipa.procore.dev
10.1.30.41   dev-ansible.procore.prod1 dev-ansible
10.1.30.22   stage-bastion.procore.prod stage-bastion
10.1.30.24   stage-foreman.procore.prod
10.1.30.148  dev-nfs.procore.prod1
10.1.30.51   stage.graylog.procore.dev
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

Summary

I configured and validated centralized identity management using FreeIPA by enrolling a Linux client into the IPA domain, configuring required firewall ports, and verifying authentication with Kerberos and SSSD. I created and managed users through the FreeIPA web interface, assigned users to appropriate groups to control access, and confirmed permissions from both the web UI and the command line. I also updated local hostname resolution to ensure reliable connectivity during setup. This ticket demonstrates end-to-end user onboarding, access control, and verification in an enterprise-style FreeIPA environment.