Chéridanh TSIELA

FreeIPA

I – Introduction

FreeIPA est une solution open source de gestion des identités pour les systèmes d'exploitation Linux/Unix. Il s'agit d'un projet en amont du RedHat Identity Management System, qui fournit des solutions d'authentification et d'autorisation pour les systèmes Linux/Unix.

FreeIPA est construit sur plusieurs composants, notamment le serveur d'annuaire, DNS, Kerberos, PKI, Certmonger, le serveur NTP, l'interface utilisateur d'administration Web, etc. Il fournit une source centralisée d'informations d'identification utilisateur et de contrôle d'accès. L'utilisation de FreeIPA permet aux administrateurs de gérer facilement l'identité dans un environnement centralisé et fournit également la surveillance, l'authentification et le contrôle d'accès des utilisateurs.

II – Prérequis

- Un serveur linux (Rocky Linux)
- Mot de passe utilisateur root

II – Installation de FreeIPA

Commencez par configurer le nom de domaine complet du serveur

sudo hostnamectl set-hostname ipa.hwdomain.lan

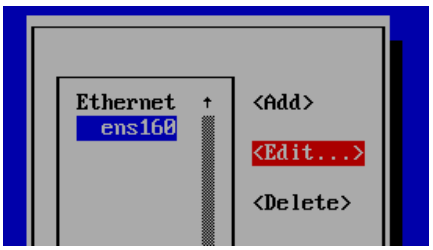
Mettez une adresse IP fixe

nmtui

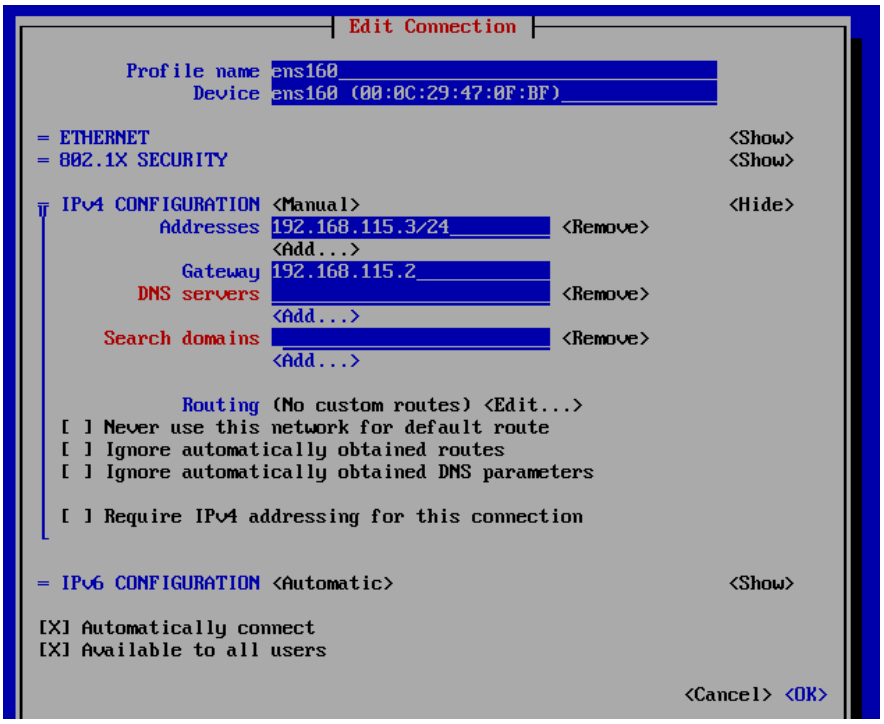
L'assistant graphique s'affiche

Cliquez sur **« Edit a conection »**

Cliquez sur **« Edit »**



Saisissez l'adresse IP adapté à votre topologie et la passerelle correspondante



Modifiez le fichier hosts

```
192.168.115.3    free-ipa.cheridanh.cg    free-ipa
```

Installer les paquets de FreeIPA et lancez la configuration

sudo dnf install ipa-server ipa-server-dns -y
sudo ipa-server-install --setup-dns --allow-zone-overlap

To accept the default shown in brackets, press the Enter key.

Enter the fully qualified domain name of the computer on which you're setting up server software. Using the form <hostname>.<domainname> Example: master.example.com.

Server host name [free-ipa.cheridanh.cg]: <== Tapez Entrer

Warning: skipping DNS resolution of host ipa.hwdomain.io The domain name has been determined based on the host name.

Please confirm the domain name [cheridanh.cg]: <== Tapez Entrer

The kerberos protocol requires a Realm name to be defined. This is typically the domain name converted to uppercase.

Please provide a realm name [CHERIDANH.CG]: <== Tapez Entrer

Certain directory server operations require an administrative user. This user is referred to as the Directory Manager and has full access to the Directory for system management tasks and will be added to the instance of directory server created for IPA. The password must be at least 8 characters long.

Directory Manager password: <== Saisir le mot de passe
Password (confirm): <== Ressaisir le mot de passe

The IPA server requires an administrative user, named 'admin'. This user is a regular system account used for IPA server administration.

IPA admin password: <== Saisir le mot de passe
Password (confirm): <== Ressaisir le mot de passe

Checking DNS domain hwdomain.io., please wait ...
Do you want to configure DNS forwarders? [yes]: <== Tapez Entrer
Following DNS servers are configured in /etc/resolv.conf: 192.168.115.2
Do you want to configure these servers as DNS forwarders? [yes]: <== Tapez Entrer

Do you want to search for missing reverse zones? [yes]: <== Tapez Entrer
Do you want to create reverse zone for IP 192.168.115.3 [yes]: <== Tapez Entrer
Please specify the reverse zone name [115.168.192.in-addr.arpa.]: <== Tapez Entrer
Using reverse zone(s) 115.168.192.in-addr.arpa. Trust is configured but no NetBIOS domain name found, setting it now Enter the NetBIOS name for the IPA domain. Only up to 15 uppercase ASCII letters, digits and dashes are allowed. Example: EXAMPLE.

NetBIOS domain name [CHERIDANH]: <== Tapez Entrer

Do you want to configure chrony with NTP server or pool address? [no]: <== Tapez « no » puis appuyez sur Entrer

Un résumé s'affiche selon les configurations qui ont été saisies en amont :

```
The IPA Master Server will be configured with:
Hostname:       free-ipa.cheridanh.cg
IP address(es): 192.168.115.3
Domain name:    cheridanh.cg
Realm name:     CHERIDANH.CG

The CA will be configured with:
Subject DN:   CN=Certificate Authority,O=CHERIDANH.CG
Subject base: O=CHERIDANH.CG
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       192.168.115.2
Forward policy:   only
Reverse zone(s):  115.168.192.in-addr.arpa.

Continue to configure the system with these values? [no]: yes
```

Une fois l'installation terminée, un message concernant l'ouverture des ports sera affiché

```
==============================================================================
Setup complete

Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 389, 636: LDAP/LDAPS
                  * 88, 464: kerberos
                  * 53: bind
                UDP Ports:
                  * 88, 464: kerberos
                  * 53: bind
                  * 123: ntp

        2. You can now obtain a kerberos ticket using the command: 'kinit admin'
           This ticket will allow you to use the IPA tools (e.g., ipa user-add)
           and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
The ipa-server-install command was successful
[root@free-ipa ~]#
```

Pour ouvrir ces ports, saisissez :

sudo firewall-cmd --add-service={http,https,dns,ntp,freeipa-ldap,freeipa-ldaps} --permanent

Actualisez le pare-feu

sudo firewall-cmd --add-service={http,https,dns,ntp,freeipa-ldap,freeipa-ldaps} --permanent

On peut voir la liste des ports ouverts avec la commande

firewall-cmd –list-all

```
[root@free-ipa ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client dns freeipa-ldap freeipa-ldaps http https ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@free-ipa ~]# _
```

Pour vérifier l'authentification tapez

kinit admin

Après avoir mis le mot de passe de l'Administrateur, tapez :

klist

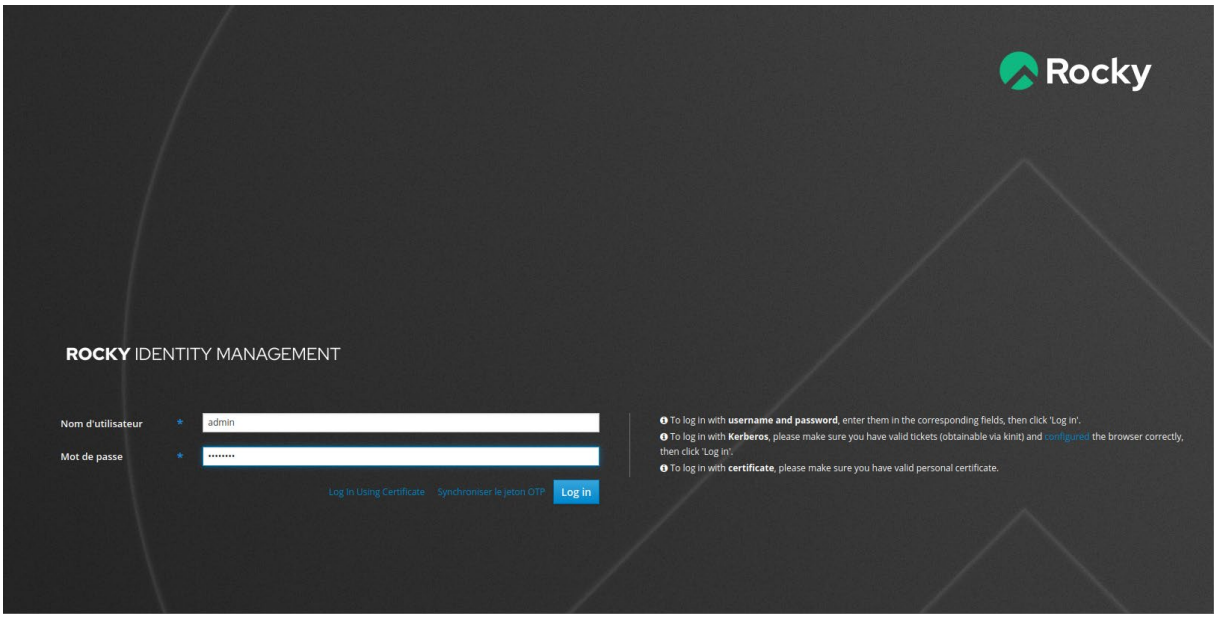
```
[root@free-ipa ~]# klist
Ticket cache: KCM:0
Default principal: root@CHERIDANH.CG

Valid starting     Expires            Service principal
05/13/24 15:54:19  05/14/24 15:11:22  krbtgt/CHERIDANH.CG@CHERIDANH.CG
[root@free-ipa ~]# _
```

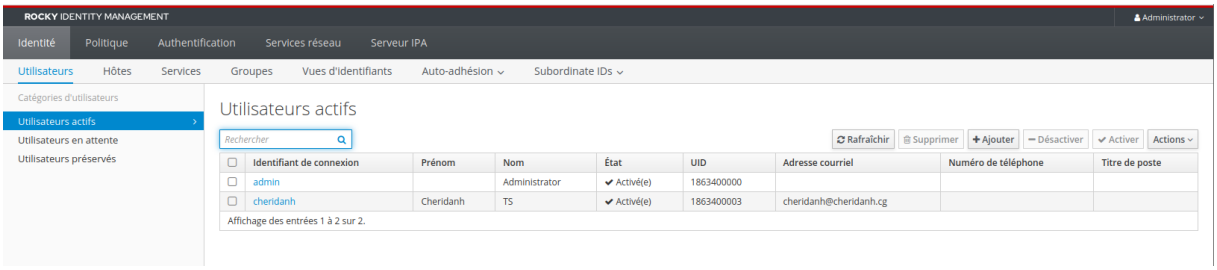
Pour se connecter à l'interface de FreeIPA, saisissez

http://free-ipa.cheridanh.cg/ipa/ui ou http://192.168.115.3/ipa/ui/

- Nom d'utilisateur : **admin**
- Mot de passe : **Celui que vous avez saisi précédemment**



Une fois connecté vous verrez le tableau de bord



Pour ajouter un hôte, tapez la commande suivante :

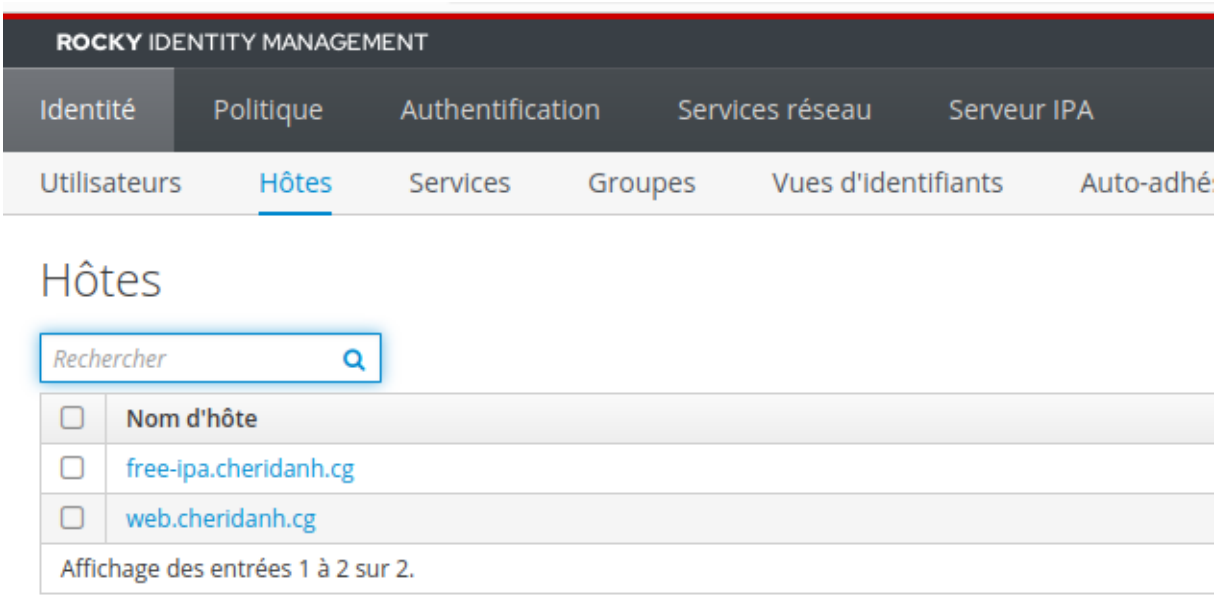
ipa host-add --ip-address 192.168.115.3 web.cheridanh.cg

Ajouter l'hôte au serveur DNS

ipa dnsrecord-add cheridanh.cg web --ttl=3600 --a-ip-address=192.168.115.3

```
[root@free-ipa ~]# ipa host-add --ip-address 192.168.115.5 web.cheridanh.cg
----------------------------
Added host "web.cheridanh.cg"
----------------------------
  Host name: web.cheridanh.cg
  Principal name: host/web.cheridanh.cg@CHERIDANH.CG
  Principal alias: host/web.cheridanh.cg@CHERIDANH.CG
  Password: False
  Keytab: False
  Managed by: web.cheridanh.cg
[root@free-ipa ~]# _
```

On peut voir l'hôte ainsi ajouté dans notre interface graphique

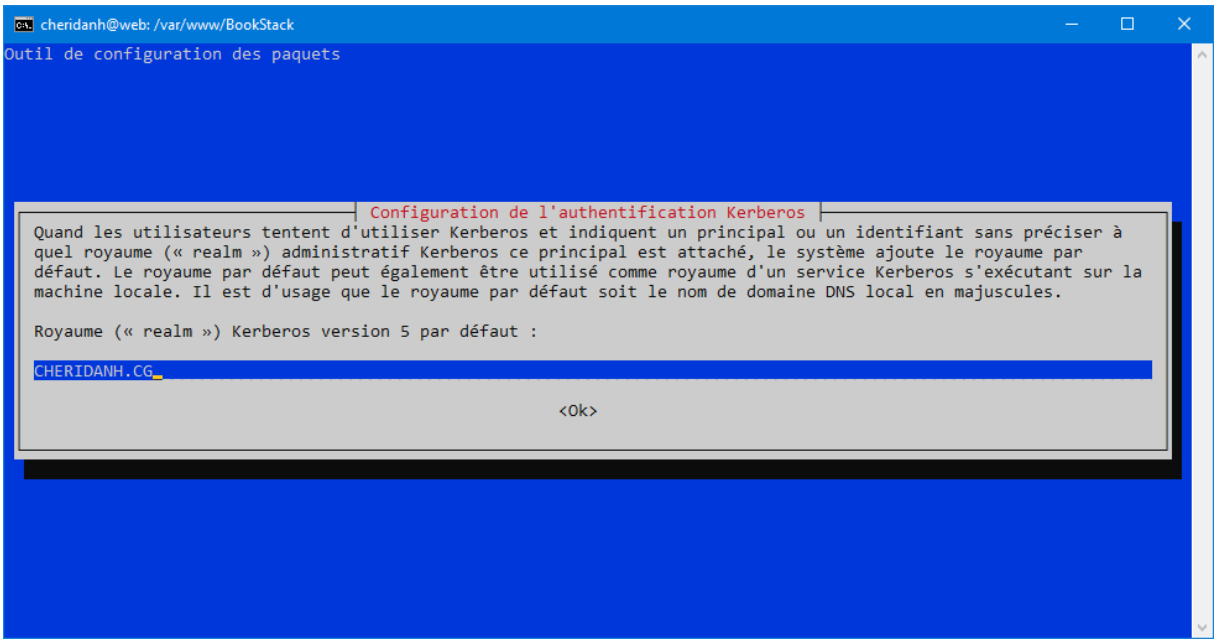


Dans la machine cliente, tapez la commande :

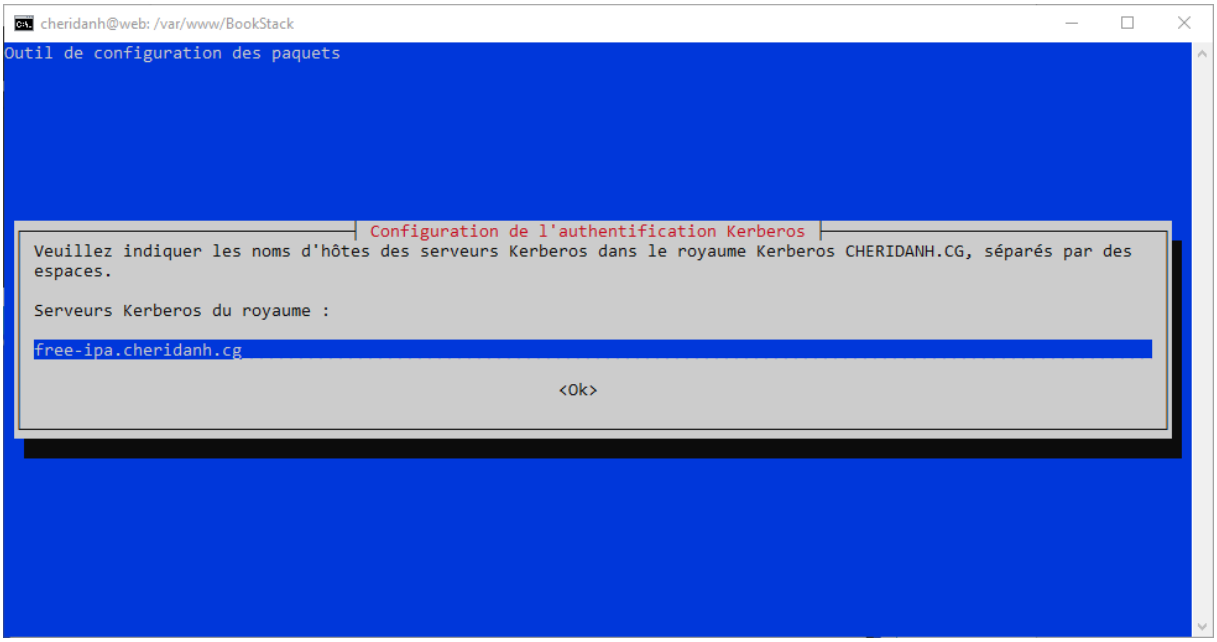
dnf install -y freeipa-client

Pour le Royaume saisissez votre nom de domaine en lettres capitales

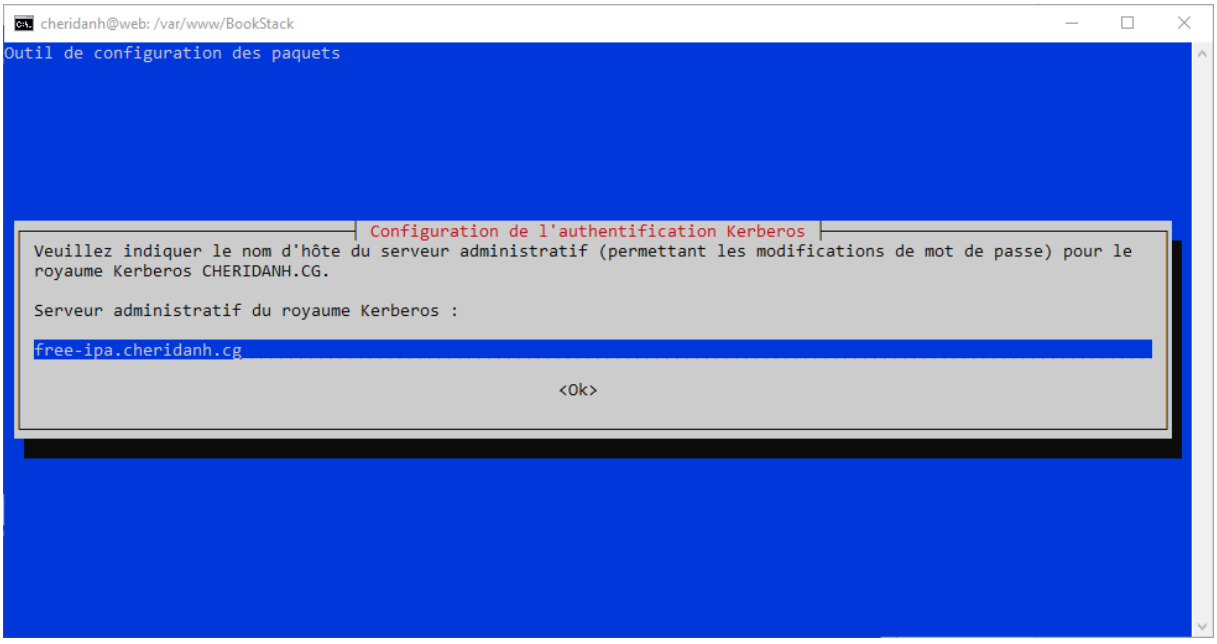
Dans mon cas : **CHERIDANH.CG**



Pour le serveur Kerberos c’est le FQDN du serveur sur lequel est installé FreeIPA



De même pour le serveur administratif su royaume Kerberos

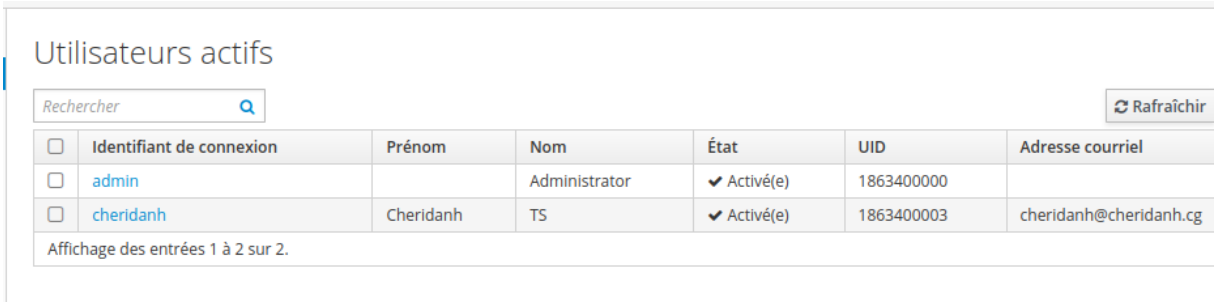


Pour ajouter un utilisateur à notre FreeIPA

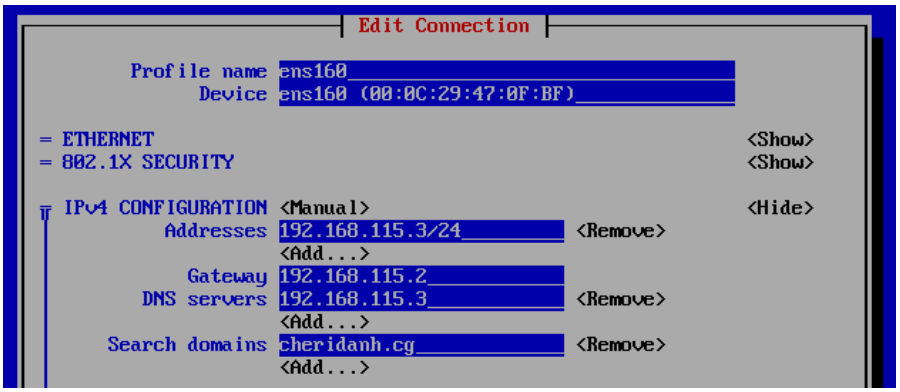
ipa user-add cheridanh --first=Cheridanh --last=TS --password

```
[root@free-ipa ~]# ipa user-add cheridanh --first=Cheridanh --last=TS --password
Password:
Enter Password again to verify:
----------------------
Added user "cheridanh"
----------------------
  User login: cheridanh
  First name: Cheridanh
  Last name: TS
  Full name: Cheridanh TS
  Display name: Cheridanh TS
  Initials: CT
  Home directory: /home/cheridanh
  GECOS: Cheridanh TS
  Login shell: /bin/sh
  Principal name: cheridanh@CHERIDANH.CG
  Principal alias: cheridanh@CHERIDANH.CG
  User password expiration: 20240501224632Z
  Email address: cheridanh@cheridanh.cg
  UID: 1863400003
  GID: 1863400003
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
[root@free-ipa ~]# _
```

On peut voir l'utilisateur ajouté dans l'onglet **« Utilisateurs actifs »**



L'installation est ainsi terminée, pensez à rajouter l'adresse IP du serveur FreeIPA dans la zone DNS des paramètres de la carte réseau.



Chéridanh TSIELA

N'hésitez pas à me laisser un message sur mon site :

https://cheridanh.cg/about