Mickael ANGEL

Comment installer le système de gestion d'identité FreeIPA sur Rocky Linux 9

FreeIPA est une solution open source de gestion d'identité pour les systèmes d'exploitation Linux/Unix. Il s'agit d'un projet dérivé du système de gestion d'identité Red Hat, qui fournit des solutions d'authentification et d'autorisation pour les systèmes Linux/Unix.

FreeIPA repose sur plusieurs composants, notamment un serveur d'annuaire, un serveur DNS, Kerberos, une infrastructure à clés publiques (PKI), Certmonger, un serveur NTP et une interface d'administration web. Il centralise la gestion des identifiants et des accès utilisateurs. FreeIPA permet aux administrateurs de gérer facilement les identités dans un environnement centralisé et assure la surveillance, l'authentification et le contrôle d'accès des utilisateurs.

Ce tutoriel vous guidera dans l'installation et la configuration de FreeIPA sur un serveur Rocky Linux 9. Vous installerez les paquets serveur FreeIPA et configurerez son déploiement. Vous créerez ensuite un utilisateur FreeIPA. Enfin, vous apprendrez à installer et configurer le client FreeIPA sur l'hôte Rocky Linux et à l'ajouter au serveur FreeIPA.

Prérequis

Pour suivre ce tutoriel, vous devez disposer des éléments suivants :

Avant de commencer, vous devez vous assurer que vous disposez des éléments suivants :

- Deux serveurs Rocky Linux 9 ou plus - Dans ce tutoriel, vous utiliserez deux hôtes Rocky Linux pour le serveur FreeIPA et le client FreeIPA.
- Un utilisateur non root disposant des privilèges d'administrateur sudo/root.• SELinux fonctionne en mode permissif.

Pour cette démonstration, nous utiliserons deux serveurs Rocky Linux 9 présentant les caractéristiques suivantes :

```
Nom d'hôte  Adresse IP      Utilisé comme
-------------------------------------------
IPA         192.168.5.25    Serveur FreeIPA
client      192.168.5.80    Client FreeIPA
```

Une fois ces prérequis remplis, vous pouvez commencer l'installation de FreeIPA.

Configurer le nom de domaine complet (FQDN) et le fuseau horaire

Pour ce tutoriel, vous allez d'abord configurer le nom de domaine pleinement qualifié (FQDN) et le fuseau horaire par défaut sur votre serveur FreeIPA.

Saisissez la commande « hostnamectl » suivante pour configurer le nom de domaine complet (FQDN) sur votre système. Dans cet exemple, le serveur FreeIPA devrait...avoir le nom de domaine complet 'ipa.mickaelangel.lan'.

```
sudo hostnamectl set-hostname ipa.mickaelangel.lan
```

Ouvrez maintenant le fichier '/etc/hosts' à l'aide de la commande suivante de l'éditeur nano.

```
sudo nano /etc/hosts
```

Ajoutez la ligne suivante au fichier et veillez à remplacer le nom d'hôte détaillé, le nom de domaine complet (FQDN) et l'adresse IP par ceux de votre serveur FreeIPA.

```
# ip - fqdn - nom d'hôte
192.168.5.25     ipa.mickaelangel.lan IPA
```

Enregistrez et fermez le fichier une fois terminé.

Ensuite, saisissez la commande suivante pour vérifier le nom de domaine complet (FQDN) de votre système. Assurez-vous ensuite que ce FQDN correspond bien à votre adresse IP interne.

```
sudo nom_hôte -f
sudo ping -c3 ipa.mickaelangel.lan
```

En cas de succès, votre nom de domaine pleinement qualifié (FQDN) devrait pointer vers l'adresse IP interne de votre serveur. Dans cet exemple, le FQDN « ipa.mickaelangel.lan » pointe vers l'adresse IP « 192.168.5.25 ».

```
[root@ipa ~]#
[root@ipa ~]# sudo hostnamectl set-hostname ipa.[redacted].lan
[root@ipa ~]#
[root@ipa ~]# sudo nano /etc/hosts
[root@ipa ~]#
[root@ipa ~]# sudo hostname -f
ipa.[redacted].lan
[root@ipa ~]#
[root@ipa ~]# sudo ping -c3 ipa.[redacted].lan
PING ipa.[redacted].lan (192.168.5.25) 56(84) bytes of data.
64 bytes from ipa.[redacted].lan (192.168.5.25): icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from ipa.[redacted].lan (192.168.5.25): icmp_seq=2 ttl=64 time=0.107 ms
64 bytes from ipa.[redacted].lan (192.168.5.25): icmp_seq=3 ttl=64 time=0.054 ms
```

Saisissez maintenant la commande « timedatectl » suivante pour définir le fuseau horaire par défaut de votre serveur. Dans cet exemple, le fuseau horaire du serveur FreeIPA sera « Europe/Stockholm ».

```
sudo timedatectl set-timezone Europe/Stockholm
```

Saisissez maintenant la commande suivante pour configurer le fichier « /etc/localtime » de votre serveur avec le fuseau horaire approprié. La liste des fichiers de fuseau horaire se trouve dans le répertoire « /usr/share/timezone/ ». Vous devez créer un lien symbolique du fichier de fuseau horaire souhaité vers « /etc/localtime ».

```
sudo unlink /etc/localtime
sudo ln -s /usr/share/timezone/Europe/Stockholm /etc/localtime
```

```
[root@ipa ~]#
[root@ipa ~]# sudo timedatectl set-timezone Europe/Stockholm
[root@ipa ~]#


[root@ipa ~]#
[root@ipa ~]# sudo unlink /etc/localtime
[root@ipa ~]# sudo ln -s /usr/share/timezone/Europe/Stockholm /etc/localtime
[root@ipa ~]#
```

Une fois le nom de domaine complet (fqdn) et le fuseau horaire configurés, vous configurerez ensuite le serveur firewalld et ouvrirez certains ports que le serveur FreeIPA utilisera.

Configurer le pare-feu

Sur les distributions basées sur RHEL, le pare-feu par défaut est firewalld, qui démarre et s'exécute automatiquement. Dans cette section, vous ajouterez le service FreeIPA ainsi que des services supplémentaires tels que NTP et DNS à firewalld.

Saisissez la commande « firewall-cmd » suivante pour ajouter FreeIPA, DNS et NTP à firewalld. Rechargez ensuite firewalld pour appliquer les modifications. Le message « success » confirme la réussite de l'opération.

```
sudo firewall-cmd --add-service={freeipa-ldap,freeipa-ldaps,dns,ntp,http,https,kerberos} --
permanentsudo firewall-cmd --recharger
```

Ensuite, exécutez la commande suivante pour vérifier l'état de firewalld et la liste des services et ports activés.

```
sudo firewall-cmd --list-all
```

Vous devriez obtenir un résultat similaire à celui-ci : Le service FreeIPA, NTP et DNS ont été ajoutés au firewalld.

```
[root@ipa ~]#
[root@ipa ~]# sudo firewall-cmd --add-service={freeipa-ldap,freeipa-ldaps,dns,ntp} --permanent
success
[root@ipa ~]# sudo firewall-cmd --reload
success
[root@ipa ~]# sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1
  sources:
  services: cockpit dhcpv6-client dns freeipa-ldap freeipa-ldaps ntp ssh
  ports:
```


Maintenant que vous avez configuré le nom de domaine complet (FQDN), le fuseau horaire et firewalld, vous pouvez lancer

l'installation du serveur FreeIPA via le DNF.

Mickael ANGEL

Gestionnaire de paquets.

Mickael ANGEL

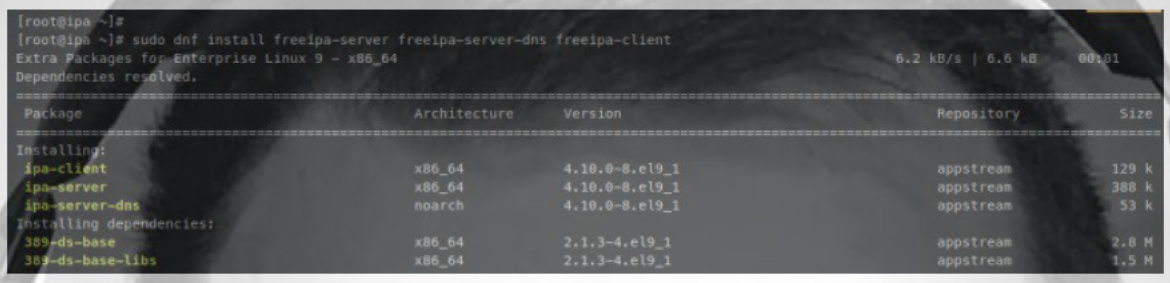
Installation et configuration du serveur FreeIPA

Sur la dernière version de Rocky Linux 9, le serveur FreeIPA est disponible par défaut dans le dépôt « appstream ». Vous n'avez donc pas besoin de...ajouter le dépôt tiers pour installer le paquet serveur FreeIPA.

Dans cette section, vous installerez le serveur FreeIPA, puis configurerez un déploiement interactif de FreeIPA via la ligne de commande.« ipa-server-install », fourni par le paquet FreeIPA.

Saisissez la commande « dnf install » suivante pour installer le serveur FreeIPA, le serveur DNS FreeIPA et le client FreeIPA. À l'invite, saisissez « y » pour confirmer et appuyez sur Entrée pour continuer.

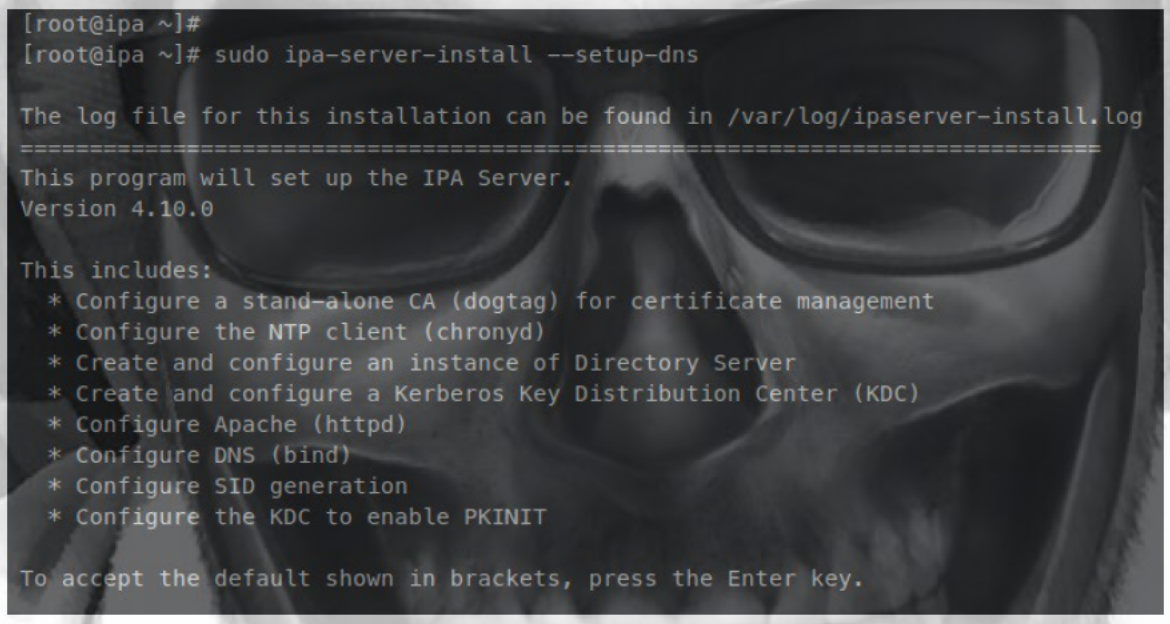
```
sudo dnf install freeipa-server freeipa-server-dns freeipa-client
```



Une fois FreeIPA installé, saisissez la commande « ipa-server-install » suivante pour démarrer le déploiement interactif de votre application.Serveur FreeIPA. Dans cet exemple, vous utiliserez le paramètre « --setup-dns », qui installera également le serveur DNS sur votre serveur FreeIPA.

```
sudo ipa-server-install --setup-dns
```

Dans le résultat suivant, vous devriez voir la liste des tâches que vous devrez effectuer pour installer et configurer le serveur FreeIPA.



Tout d'abord, le programme « ipa-server-install » vérifiera le nom de domaine complet (FQDN) de votre système et s'assurera que le FQDN de votre serveur pointe vers le bon emplacement.Adresse IP (via DNS ou le fichier /etc/hosts). Dans cet exemple, le nom de domaine complet « ipa.mickaelangel.lan » est configuré via le fichier /etc/hosts ; vous pouvez donc commencer.

Le nom de domaine par défaut et le nom de domaine (realm) suivront tous deux le nom de domaine pleinement qualifié (FQDN) de l'hôte. Ainsi, le FQDN « ipa.mickaelangel.lan » vous donnera le nom de domaine par défaut « mickaelangel.lan » et le nom de domaine « MICKAELANGEL.LAN ».

Appuyez sur ENTRÉE pour utiliser la valeur par défaut du nom d'hôte (FQDN), du nom de domaine et du nom de royaume.

```
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 [ipa.[redacted].lan]:

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

Please confirm the domain name [[redacted].lan]:

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

Please provide a realm name [[redacted].LAN]:
Certain directory server operations require an administrative user.
```

Saisissez maintenant un nouveau mot de passe pour le gestionnaire d'annuaire et l'utilisateur administrateur IPA. Veillez à utiliser plus de 8 caractères.et un mot de passe fort.

```
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:
Password (confirm):

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

IPA admin password:
Password (confirm):
```

Vous serez ensuite invité à configurer les serveurs DNS par défaut de votre serveur FreeIPA ainsi que le DNS inverse (rDNS) de son adresse IP. Appuyez sur Entrée pour confirmer la configuration par défaut.

Laissez la configuration du nom de domaine NetBIOS par défaut et appuyez sur ENTRÉE. Pour les paramètres NTP, saisissez le numéro.

```
Checking DNS domain hwdomain.lan., please wait ...
Do you want to configure DNS forwarders? [yes]:
Following DNS servers are configured in /etc/resolv.conf: 192.168.121.1
Do you want to configure these servers as DNS forwarders? [yes]:
All detected DNS servers were added. You can enter additional addresses now:
Enter an IP address for a DNS forwarder, or press Enter to skip:
DNS forwarders: 192.168.121.1
Checking DNS forwarders, please wait ...
Do you want to search for missing reverse zones? [yes]:
Reverse record for IP address 192.168.5.25 already exists
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 [[redacted]]:

Do you want to configure chrony with NTP server or pool address? [no]:
```

Vérifiez maintenant les paramètres de base de votre serveur FreeIPA, puis saisissez « oui » pour confirmer et appuyez sur ENTRÉE pour procéder à l'installation.

```
The IPA Master Server will be configured with:
Hostname:       ipa.[redacted].lan
IP address(es): 192.168.5.25
Domain name:    [redacted].lan
Realm name:     [redacted].LAN

The CA will be configured with:
Subject DN:   CN=Certificate Authority,O=[redacted].LAN
Subject base: O=[redacted].LAN
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       192.168.121.1
Forward policy:   only
Reverse zone(s):  No reverse zone

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

The following operations may take some minutes to complete.
Please wait until the prompt is returned.
```

Une fois l'installation du serveur FreeIPA terminée, vous devriez obtenir un message du type « Installation terminée - La commande ipa-server-install a fonctionné ». Vous verrez également les instructions pour les étapes suivantes : configurer un pare-feu pour ouvrir certains ports et obtenir un ticket Kerberos pour un administrateur.

```
==============================================================================
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@ipa ~]#
```

Vous avez ainsi terminé la configuration de base du serveur FreeIPA via « ipa-server-install ». L'étape suivante consiste à...Vous vous authentifierez auprès de Kerberos et obtiendrez un ticket d'administrateur qui vous permettra de configurer FreeIPA depuis votre terminal.

Authentification d'administrateur Kerberos et tableau de bord de l'interface utilisateur Web FreeIPA

Après avoir configuré le serveur FreeIPA via 'ipa-server-install', vous allez maintenant vérifier l'installation de FreeIPA en obtenant un ticket d'administrateur auprès de Kerberos et en vous connectant au tableau de bord d'administration Web de FreeIPA.

Saisissez la commande « kinit » suivante pour vous authentifier auprès du serveur Kerberos via l'utilisateur « admin ». Lorsque le mot de passe vous est demandé, saisissez votre mot de passe d'administrateur IPA.

```
administrateur de kinit
```

Vérifiez maintenant l'authentification et la liste des tickets Kerberos obtenus en saisissant la commande 'klist' suivante.


```
klist
```

Si l'authentification Kerberos réussit, vous devriez recevoir le ticket mis en cache pour le principal par défaut.' admin@MICKAELANGEL.LAN 'comme indiqué dans la capture d'écran suivante.

```
[root@ipa ~]#
[root@ipa ~]# kinit admin
Password for admin@[redacted].LAN:
[root@ipa ~]#
[root@ipa ~]# klist
Ticket cache: KCM:0
Default principal: admin@[redacted].LAN

Valid starting       Expires              Service principal
02/13/2023 23:27:56  02/14/2023 22:39:36  krbtgt/[redacted].LAN@[redacted].LAN
[root@ipa ~]#
[root@ipa ~]#
```

Ensuite, vous vérifierez le serveur FreeIPA en accédant au tableau de bord d'administration depuis votre ordinateur. Avant de commencer, ouvrez le fichier « /etc/hosts » sur votre ordinateur à l'aide de la commande suivante dans l'éditeur nano.

```
sudo nano /etc/hosts
```

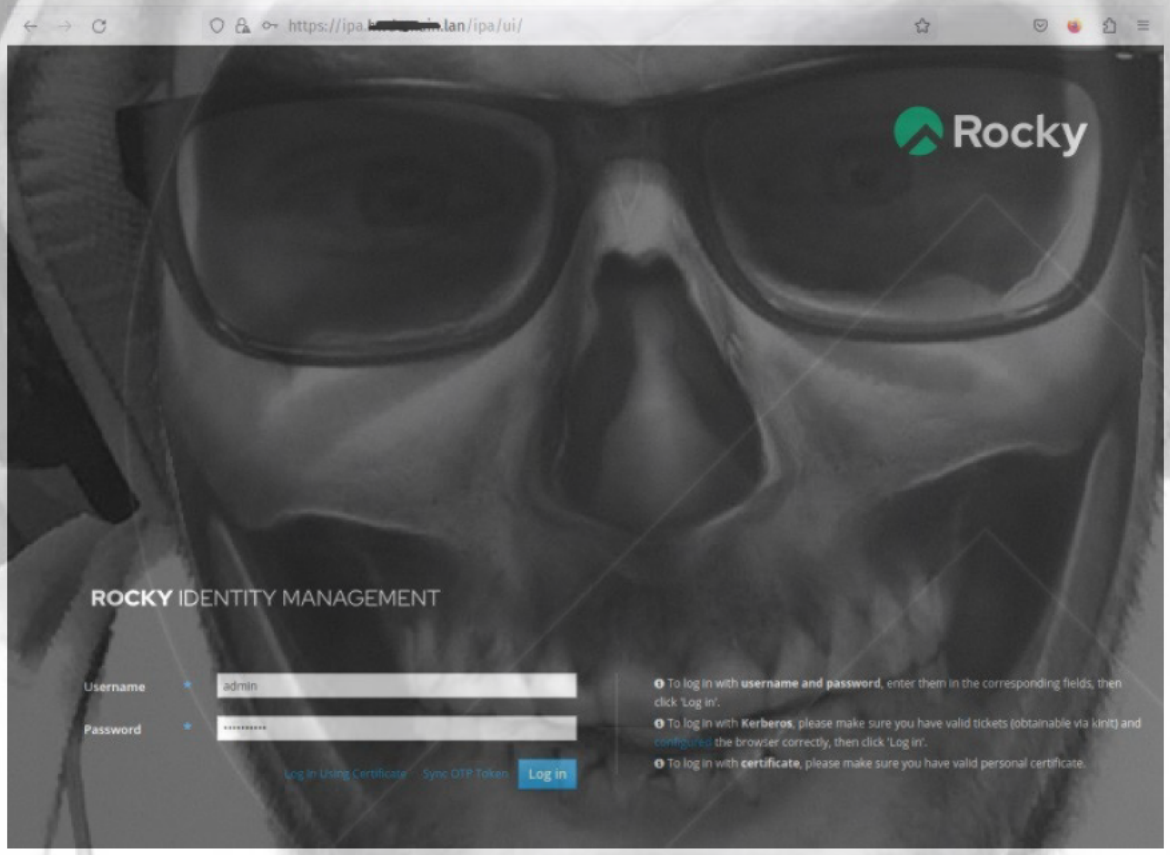
Ajoutez la ligne suivante au fichier et veillez à remplacer l'adresse IP du nom de domaine par les informations de votre serveur FreeIPA.

```
# domaine IP
192.168.5.25 ipa.mickaelangel.lan ipa
```

Enregistrez et fermez le fichier une fois terminé.

Ensuite, ouvrez votre navigateur Web et accédez au nom de domaine du serveur FreeIPA (c.-à-d. :https://ipa.mickaelangel.lanVous devriez voir la page de connexion FreeIPA.

Saisissez le nom d'utilisateur par défaut « admin » et votre mot de passe FreeIPA, puis cliquez sur « Se connecter ».



En cas de succès, vous devriez obtenir le tableau de bord d'administration web de FreeIPA, comme sur la capture d'écran suivante.


https://ipa.[redacted].lan/ipa/ui/#/e/user/search
ROCKY IDENTITY MANAGEMENT
Administrator
Identity
Policy
Authentication
Network Services
IPA Server
Users
Hosts
Services
Groups
ID Views
Automember
Subordinate IDs
User categories
Active users
Stage users
Preserved users
Active users
Search
Refresh
Delete
Add
Disable
Enable
Actions
User login
First name
Last name
Status
UID
Email address
Telephone Number
Job Title
admin
Administrator
Enabled
1783400000
Showing 1 to 1 of 1 entries.

Vous avez donc installé et configuré avec succès le serveur FreeIPA sur Rocky Linux 9. L'étape suivante vous apprendra à gérer le serveur FreeIPA en ajoutant un nouvel utilisateur et un groupe via le terminal, puis en ajoutant une nouvelle machine hôte Linux à l'aide du client FreeIPA.

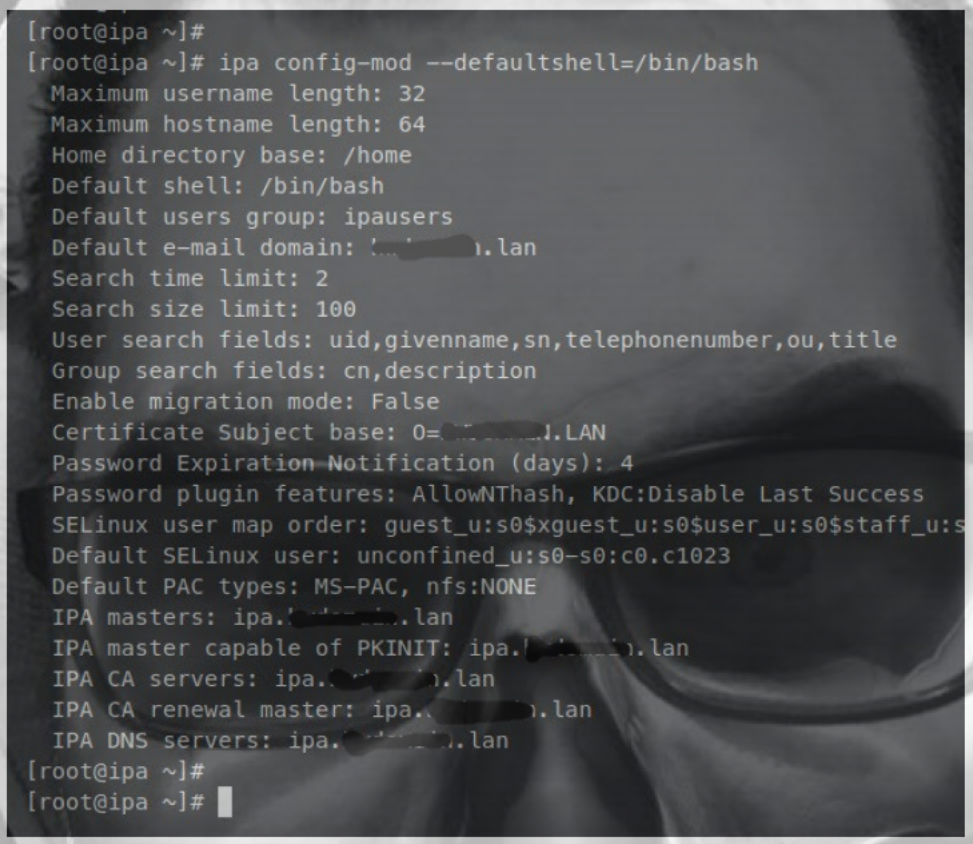
Configurer le premier utilisateur et groupe FreeIPA

Dans cette section, vous apprendrez à utiliser la commande « ipa » pour gérer les utilisateurs et les groupes. Vous utiliserez cette commande avec différents paramètres pour créer un utilisateur, consulter la liste des utilisateurs, créer un groupe, consulter la liste des groupes et ajouter un utilisateur FreeIP à un groupe spécifique. Enfin, vous vérifierez la liste des utilisateurs et des groupes via le tableau de bord d'administration de FreeIPA.

Saisissez la commande « ipa config-mod » suivante pour modifier l'interpréteur de commandes par défaut des utilisateurs de FreeIPA et le définir sur « /bin/bash ». Cette commande affichera également les autres paramètres utilisateur par défaut de FreeIPA.

```
ipa config-mod --defaultshell=/bin/bash
```

Vous trouverez ci-dessous un résultat similaire qui sera affiché dans votre terminal.



Ensuite, saisissez la commande « ipa user-add » pour ajouter un nouvel utilisateur FreeIPA. Dans cet exemple, vous allez créer un utilisateur nommé « rocky ». Lorsque le système vous demande un mot de passe, saisissez et confirmez un nouveau mot de passe pour cet utilisateur.

```
ipa user-add rocky --first=Rocky --last=Linux --password
```

```
[root@ipa ~]#
[root@ipa ~]# ipa user-add rocky --first=Rocky --last=Linux --password
Password:
Enter Password again to verify:
----------------------
Added user "rocky"
----------------------
  User login: rocky
  First name: Rocky
  Last name: Linux
  Full name: Rocky Linux
  Display name: Rocky Linux
  Initials: RL
  Home directory: /home/rocky
  GECOS: Rocky Linux
  Login shell: /bin/bash
  Principal name: rocky@[redacted].LAN
  Principal alias: rocky@[redacted].LAN
  User password expiration: 20230213233338Z
  Email address: rocky@[redacted].lan
  UID: 1783400003
  GID: 1783400003
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
[root@ipa ~]#
[root@ipa ~]#
```

Vérifiez maintenant les informations de l'utilisateur « rocky » en saisissant la commande « ipa user-find » ci-dessous. Si les informations détaillées concernant l'utilisateur « rocky » s'affichent, cela signifie que vous avez créé un utilisateur FreeIPA avec succès.

```
utilisateur ipa trouver rocky
```

```
[root@ipa ~]#
[root@ipa ~]# ipa user-find rocky
---------------
1 user matched
---------------
  User login: rocky
  First name: Rocky
  Last name: Linux
  Home directory: /home/rocky
  Login shell: /bin/bash
  Principal name: rocky@[redacted].LAN
  Principal alias: rocky@[redacted].LAN
  Email address: rocky@[redacted].lan
  UID: 1783400003
  GID: 1783400003
  Account disabled: False
----------------------------
Number of entries returned 1
----------------------------
[root@ipa ~]#
```

Vous pouvez également utiliser la commande « ipa user-show » pour afficher les détails des utilisateurs de FreeIPA.

```
ipa user-show --raw rocky
```

Sortir:

```
[root@ipa ~]#
[root@ipa ~]# ipa user-show --raw rocky
  uid: rocky
  givenname: Rocky
  sn: Linux
  homedirectory: /home/rocky
  loginshell: /bin/bash
  krbcanonicalname: rocky@[redacted].LAN
  krbprincipalname: rocky@[redacted].LAN
  mail: rocky@[redacted].lan
  uidnumber: 1783400003
  gidnumber: 1783400003
  nsaccountlock: FALSE
  has_password: TRUE
  has_keytab: TRUE
[root@ipa ~]#
[root@ipa ~]#
```

Ensuite, saisissez la commande « ipa group-add » pour créer un nouveau groupe nommé « development ». Enfin, vérifiez l'existence du groupe « development » en saisissant la commande « ipa group-find ».

```
ipa group-add --desc='Équipe de développement'
développement ipa group-find développement
```

Le message « 1 groupe correspondant » confirme que le groupe « développement » a été ajouté et est disponible sur le serveur FreeIPA.

```
[root@ipa ~]#
[root@ipa ~]# ipa group-add --desc='Development Team' development
-------------------------
Added group "development"
-------------------------
  Group name: development
  Description: Development Team
  GID: 1783400004
[root@ipa ~]#


[root@ipa ~]#
[root@ipa ~]# ipa group-find development
---------------
1 group matched
---------------
  Group name: development
  Description: Development Team
  GID: 1783400004
----------------------------
Number of entries returned 1
----------------------------
[root@ipa ~]#
[root@ipa ~]#
```

Saisissez maintenant la commande suivante « ipa group-add-member » pour ajouter l'utilisateur FreeIPA « rocky » au groupe « development ».

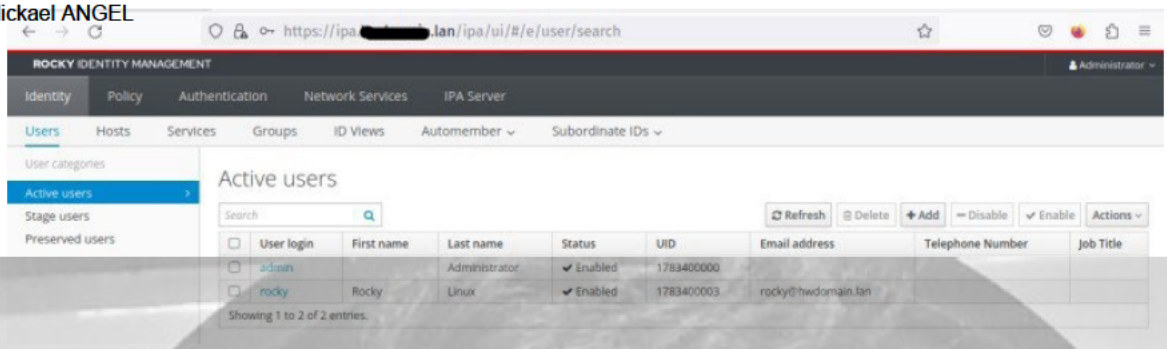
```
ipa group-add-member --user=rocky development
```

Le message « Nombre de membres ajoutés : 1 » confirme que l'utilisateur « rocky » a été ajouté au groupe « development ».

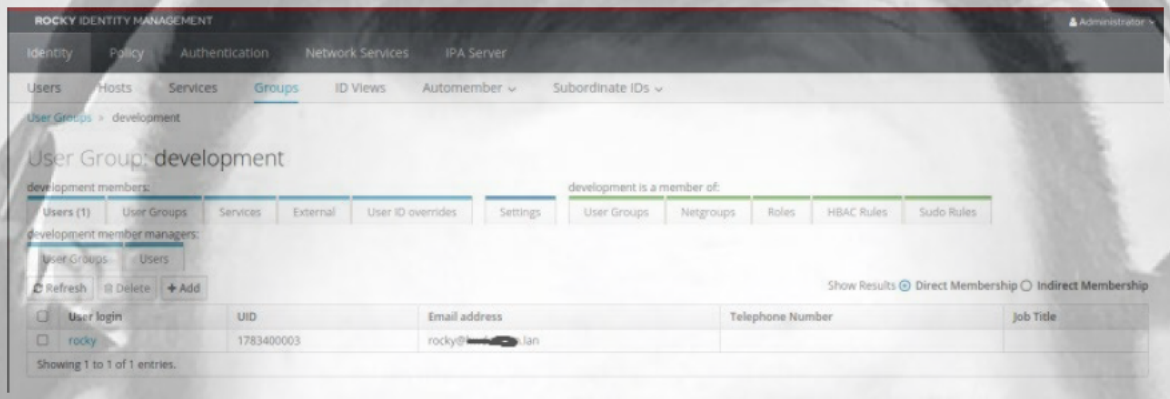
```
[root@ipa ~]#
[root@ipa ~]# ipa group-add-member --user=rocky development
  Group name: development
  Description: Development Team
  GID: 1783400004
  Member users: rocky
-------------------------
Number of members added 1
-------------------------
[root@ipa ~]#
```

Retournez maintenant au tableau de bord d'administration de FreeIPA, cliquez sur le menu « Identité », puis sur l'onglet « Utilisateurs ».

Vous devriez maintenant voir le nouvel utilisateur FreeIPA « rocky » créé et disponible sur le serveur FreeIPA.



Enfin, cliquez sur l'onglet « Groupes » pour consulter la liste des groupes sur FreeIPA. Le nouveau groupe « development » est disponible sur le serveur FreeIPA. Cliquez sur ce groupe pour obtenir des informations détaillées ; vous devriez y voir l'utilisateur « rocky » ajouté et disponible.



Vous avez maintenant créé un utilisateur et un groupe FreeIPA depuis le terminal via l'outil de gestion de commandes « ipa ». Vous avez également vérifié que votre utilisateur et votre groupe ont bien été ajoutés via le tableau de bord d'administration web de FreeIPA. L'étape suivante vous montrera comment ajouter un hôte/une machine Linux au serveur FreeIPA.

Ajout d'hôtes au serveur FreeIPA : Rocky Linux

FreeIPA offre la méthode la plus simple pour ajouter un nouvel hôte au serveur FreeIPA : le paquet client FreeIPA, qui inclut l'utilitaire « ipa-client-install ». Dans cette section, vous ajouterez une machine Rocky Linux 9 au serveur FreeIPA « ipa.mickaelangel.lan ».

Voici les étapes à suivre pour ajouter un nouvel hôte au serveur

FreeIPA :• Ajouter les enregistrements DNS de l'hôte depuis le

serveur FreeIPA

- Configurez les fichiers /etc/hosts et /etc/resolv.conf
- Installation du client FreeIPA et ajout de

l'hôte via 'ipa-client-install' Commençons

maintenant par ajouter l'hôte Rocky Linux au serveur FreeIPA. Ajout

des enregistrements DNS

Tout d'abord, vous devez ajouter l'enregistrement DNS de votre machine cliente au serveur FreeIPA. Cela peut se faire via la commande `ipa`.
dnsrecord-add' commande que vous pouvez exécuter depuis le serveur FreeIPA.

Saisissez la commande suivante : « ipa dnsrecord-add » pour ajouter un nouvel enregistrement DNS pour la machine hôte « client » avec l'adresse IP « 192.168.5.80 ». La machine cliente aura alors le nom de domaine « client.mickaelangel.lan ».

Dans cet exemple, vous allez définir l'enregistrement A pour l'hôte nommé « client » avec l'adresse IP « 192.168.5.80 ». Le domaine « mickaelangel.lan » correspond au nom de domaine par défaut de votre serveur FreeIPA.

```
ipa dnsrecord-ajouter le client mickaelangel.lan --a-rec 192.168.5.80
```

Vérifiez maintenant l'enregistrement DNS « client » en saisissant la commande « ipa dnsrecord-find » ci-dessous. Vous devriez voir la machine « client » avec l'enregistrement A résolu en l'adresse IP « 192.168.5.80 ».

```
ipa dnsrecord-trouver le client mickaelangel.lan
```


```
[root@ipa ~]#
[root@ipa ~]# ipa dnsrecord-add [redacted].lan client --a-rec 192.168.5.80
  Record name: client
  A record: 192.168.5.80
[root@ipa ~]#
[root@ipa ~]# ipa dnsrecord-find [redacted].lan client
  Record name: client
  A record: 192.168.5.80
----------------------------
Number of entries returned 1
----------------------------
[root@ipa ~]#
```

Enfin, saisissez la commande « dig » suivante pour vérifier le nom de domaine DNS de la machine cliente : « client.mickaelangel.lan ».

```
client dig.mickaelangel.lan
```

En cas de succès, vous devriez recevoir un résultat comme celui-ci : Le nom de domaine de la machine cliente « client.mickaelangel.lan » pointe vers l'adresse IP du serveur « 192.168.5.80 ».

```
[root@ipa ~]#
[root@ipa ~]# dig client.[redacted].lan

; <<>> DiG 9.16.23-RH <<>> client.[redacted].lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60527
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8709997c2677d1540100000063eada48b38c92afb131ca48 (good)
;; QUESTION SECTION:
;client.[redacted].lan.          IN      A

;; ANSWER SECTION:
client.[redacted].lan.    86400   IN      A       192.168.5.80
```

Vous êtes maintenant prêt à configurer la machine « cliente » et à l'ajouter au serveur FreeIPA.

Configurer le nom de domaine complet (FQDN), le fichier /etc/hosts et le résolveur.

Connectez-vous maintenant à la machine « cliente » pour configurer les paramètres système de base avant d'installer les paquets clients FreeIPA.

Dans cette section, vous allez configurer le fichier « /etc/hosts » et définir le nom de domaine et l'adresse IP du serveur FreeIPA. Ensuite, vous modifierez le fichier « /etc/resolv.conf » afin de configurer le résolveur DNS par défaut de la machine cliente pour qu'il utilise celui du serveur FreeIPA. Ainsi, votre machine cliente pourra accéder au serveur FreeIPA via son nom de domaine.

Saisissez la commande suivante dans l'éditeur nano pour ouvrir le fichier '/etc/hosts'.

```
sudo nano /etc/hosts
```

Ajoutez les lignes suivantes au fichier et veillez à remplacer l'adresse IP et le nom de domaine par ceux de votre serveur FreeIPA.

```
# ip - fqdn/domaine - nom d'hôte
192.168.5.25    ipa.mickaelangel.lan IPA
```

Enregistrez et fermez le fichier une fois terminé.

Ensuite, ouvrez le fichier '/etc/resolv.conf' à l'aide de la commande suivante de l'éditeur nano.

```
sudo nano /etc/resolv.conf
```

Ajoutez la ligne suivante en haut de la ligne et veillez à remplacer l'adresse IP par l'adresse IP de votre serveur FreeIPA.


```
# lister les serveurs de
```

```
noms du résolveur
192.168.5.25
```


Enregistrez et fermez le fichier une fois terminé.

Enfin, saisissez la commande « ping » suivante pour vérifier le nom de domaine du serveur FreeIPA et le nom de domaine de la machine cliente.


```
ping -c3
ipa.mickaelangel.lan ping -
c3 client.mickaelangel.lan
```

Vous devriez obtenir un résultat similaire à celui-ci : le nom de domaine du serveur FreeIPA « ipa.mickaelangel.lan » sera associé à l'adresse IP « 192.168.5.25 » telle que définie dans le fichier « /etc/hosts ».

Et le nom de domaine de la machine cliente « client.mickaelangel.lan » sera redirigé vers l'adresse IP correcte « 192.168.5.80 ».qui est configuré via le serveur DNS FreeIPA et confirme que vos paramètres de résolution DNS sont corrects et appropriés.

```
[root@client ~]#
[root@client ~]# sudo nano /etc/hosts
[root@client ~]#
[root@client ~]# sudo nano /etc/resolv.conf
[root@client ~]#
[root@client ~]# ping -c3 ipa.h       .lan
PING ipa.h       .lan (192.168.5.25) 56(84) bytes of data.
64 bytes from ipa.h       .lan (192.168.5.25): icmp_seq=1 ttl=64 time=2.79 ms
64 bytes from ipa.h       .lan (192.168.5.25): icmp_seq=2 ttl=64 time=0.589 ms
64 bytes from ipa.h       .lan (192.168.5.25): icmp_seq=3 ttl=64 time=0.456 ms

--- ipa.hwdomain.lan ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.456/1.277/2.788/1.069 ms
[root@client ~]#
[root@client ~]# ping -c3 client.h       .lan
PING client.h       .lan (192.168.5.80) 56(84) bytes of data.
64 bytes from client (192.168.5.80): icmp_seq=1 ttl=64 time=0.073 ms
64 bytes from client (192.168.5.80): icmp_seq=2 ttl=64 time=0.073 ms
64 bytes from client (192.168.5.80): icmp_seq=3 ttl=64 time=0.060 ms

--- client.       .lan ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.060/0.068/0.073/0.006 ms
[root@client ~]#
```

Vous êtes maintenant prêt à installer le paquet client FreeIPA et à ajouter votre machine cliente au serveur FreeIPA.

Installation et configuration du client

Commencez par saisir la commande « dnf install » suivante pour installer le paquet client FreeIPA et le paquet supplémentaire.« oddjob-mkhomedir ». Lorsque vous y êtes invité, saisissez « y » pour confirmer et appuyez sur ENTRÉE pour continuer.

```
sudo dnf install freeipa-client oddjob-mkhomedir
```

```
[root@client ~]#
[root@client ~]# sudo dnf install freeipa-client oddjob-mkhomedir
Extra Packages for Enterprise Linux 9 - x86_64                  4.3 kB/s | 6.6 kB     00:01
Package oddjob-mkhomedir-0.34.7-6.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package                Architecture        Version                 Repository      Size
================================================================================
Installing:
 ipa-client             x86_64              4.10.0-8.el9_1          appstream      129 k
Installing dependencies:
 augeas-libs            x86_64              1.13.0-2.el9            appstream      405 k
 autofs                 x86_64              1:5.1.7-31.el9          baseos         364 k
```

Une fois l'installation terminée, saisissez la commande « ipa-client-install » pour ajouter votre machine cliente au serveur FreeIPA. Veillez à remplacer le paramètre « --server=ipa.mickaelangel.lan » par l'adresse de votre serveur FreeIPA, ainsi que les paramètres « --domain mickaelangel.lan » et « --realm MICKAELANGEL.LAN ».

```
ipa-client-install --hostname=`hostname -f` \
--mkhomedir \
--server=ipa.mickaelangel.lan \
--domaine mickaelangel.lan \
--royaume MICKAELANGEL.LAN
```

Saisissez « oui » pour conserver la valeur fixe des détails du serveur FreeIPA et « non » pour les paramètres du serveur NTP.

```
[root@client ~]#
[root@client ~]# ipa-client-install --hostname=`hostname -f` \
--mkhomedir \
--server=ipa.[redacted].lan \
--domain [redacted].lan \
--realm [redacted].LAN
This program will set up IPA client.
Version 4.10.0

Autodiscovery of servers for failover cannot work with this configuration.
If you proceed with the installation, services will be configured to always access t
er to other servers in case of failure.
Proceed with fixed values and no DNS discovery? [no]: yes
Do you want to configure chrony with NTP server or pool address? [no]: no
```

Vérifiez maintenant la configuration du client, puis saisissez « oui » pour confirmer.

```
Client hostname: client.[redacted].lan
Realm: [redacted].LAN
DNS Domain: [redacted].lan
IPA Server: ipa.[redacted].lan
BaseDN: dc=[redacted],dc=lan

Continue to configure the system with these values? [no]: yes
Synchronizing time
No SRV records of NTP servers found and no NTP server or pool address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
```

Vous serez maintenant invité à vous authentifier auprès du serveur Kerberos. Cette étape est nécessaire car le ticket Kerberos doit être mis en cache lors de l'ajout d'un nouvel hôte au serveur FreeIPA.

Saisissez l'utilisateur par défaut « admin » et votre mot de passe. Une fois l'opération réussie, vous devriez obtenir un résultat similaire à celui-ci : le processus devrait maintenant démarrer.

```
User authorized to enroll computers: admin
Password for admin@[redacted].LAN:
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=[redacted].LAN
    Issuer:      CN=Certificate Authority,O=[redacted].LAN
    Valid From:  2023-02-13 23:19:33
    Valid Until: 2043-02-13 23:19:33

Enrolled in IPA realm [redacted].LAN
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Hostname (client.[redacted].lan) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host client.[redacted].lan: 192.168.5.80.
Missing reverse record(s) for address(es): 192.168.5.80.
```

Une fois le processus terminé, vous devriez recevoir un résultat tel que « Configuration du client terminée - La commande ipa-client-install a réussi ».

```
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring [redacted].lan as NIS domain.
Configured /etc/krb5.conf for IPA realm [redacted].LAN
Client configuration complete.
The ipa-client-install command was successful
[root@client ~]#
```

Vous avez ainsi ajouté une machine cliente Rocky Linux au serveur FreeIPA via l'utilitaire « ipa-client-install » fourni par le paquet client FreeIPA. Vous pouvez désormais vous connecter à cette machine cliente avec l'utilisateur FreeIPA que vous avez ajouté.

Connexion au client via l'utilisateur FreeIPA

Mickael ANGEL

Dans cette section, vous vérifierez l'installation du serveur et du client FreeIPA en vous connectant à la machine cliente via l'utilisateur FreeIPA. Vous vous connecterez à la machine hôte « client.mickaelangel.lan » avec l'utilisateur FreeIPA « rocky » via SSH.

Retournez sur votre serveur FreeIPA et exécutez la commande « ssh » ci-dessous pour vous connecter au réseau local « client.mickaelangel » avec l'utilisateur FreeIPA « rocky ». Saisissez « yes » pour accepter l'authentification SSH de la machine hôte.

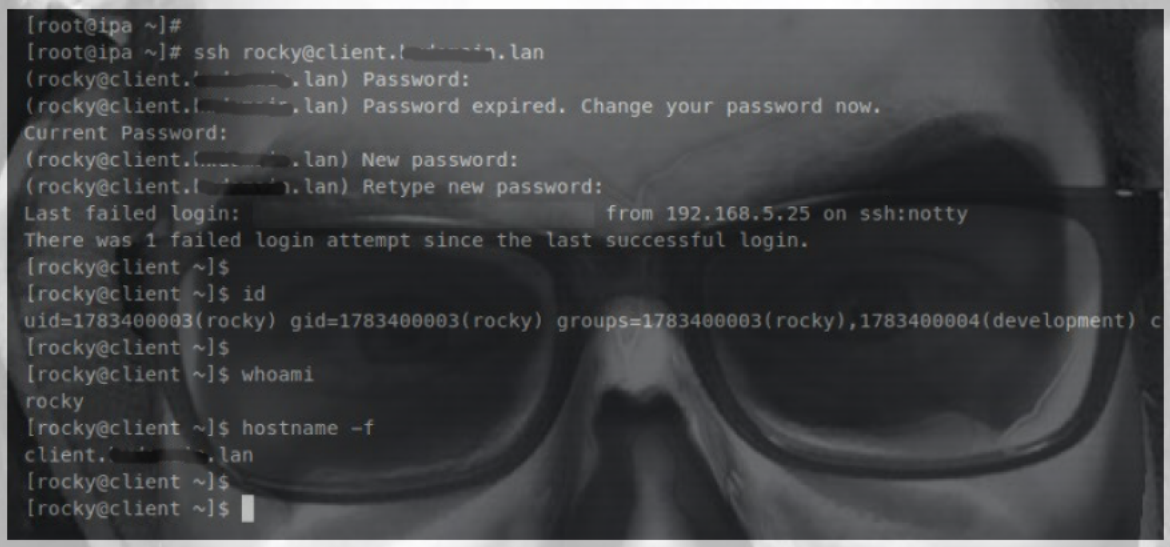
```
sshrocky@client.mickaelangel.lan
```

Lorsque le mot de passe vous est demandé, saisissez celui de l'utilisateur FreeIPA « rocky ». Une fois le mot de passe correct saisi, il vous sera demandé de le modifier.

Saisissez le mot de passe actuel, puis le nouveau mot de passe de l'utilisateur « rocky » et confirmez-le. Une fois la connexion établie, vous serez connecté à la machine « client.mickaelangel.lan » via l'utilisateur FreeIPA « rocky ». Le répertoire personnel de l'utilisateur FreeIPA sera également créé automatiquement lors de la connexion.

Saisissez la commande suivante pour vérifier l'état actuel de votre connexion. L'utilisateur utilisé devrait s'appeler « rocky » et appartenir au groupe « development ». Le nom de domaine complet (FQDN) de la machine cliente devrait être « client.mickaelangel.lan ».

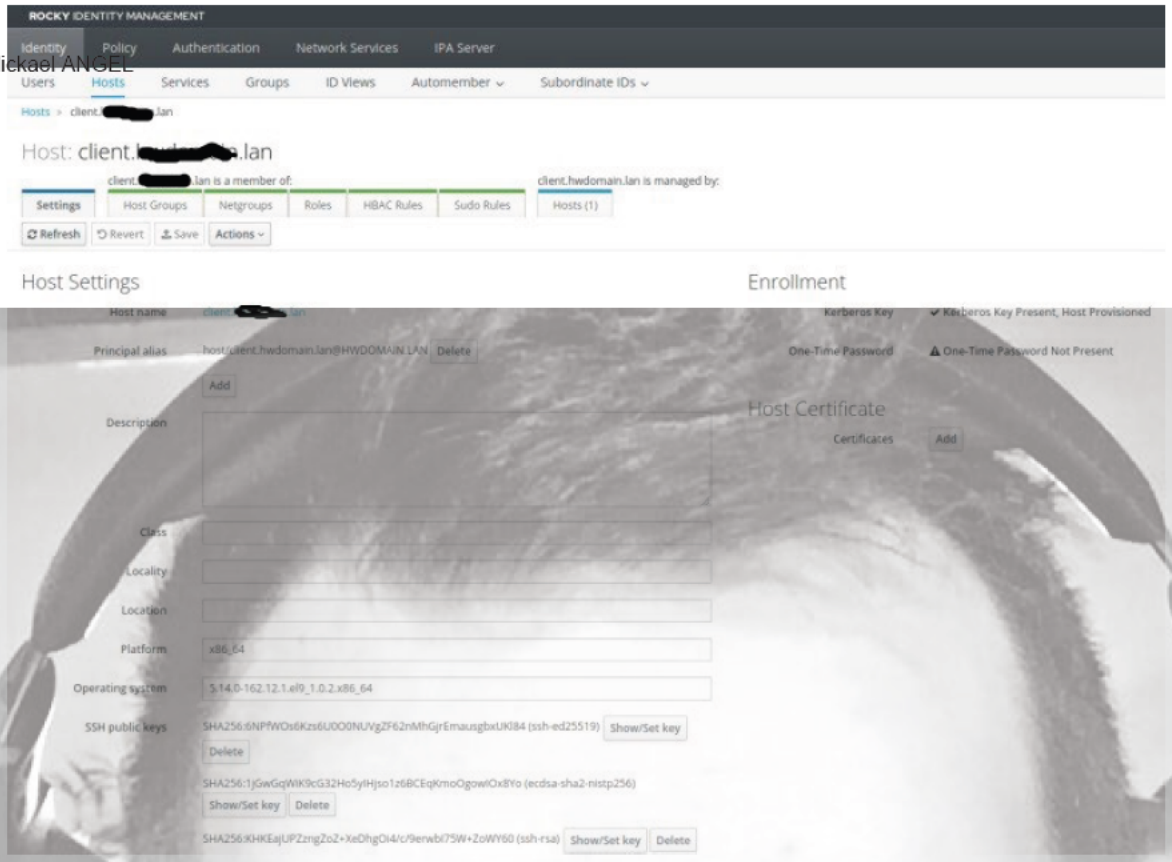
```
je
suis
qui
nom d'hôte -f
```



Enfin, via le tableau de bord d'administration web, vous pourrez vérifier la liste des hôtes/machines disponibles sur le serveur FreeIPA.

Retournez au tableau de bord d'administration de FreeIPA et cliquez sur le menu « Identité », puis sélectionnez l'onglet « Hôtes ». Vous devriez voir « client.mickaelangel.lan » ajouté et disponible sur le serveur FreeIPA.

Cliquez maintenant sur le lien « client.mickaelangel.lan » pour obtenir des informations détaillées sur l'hôte. Vous devriez voir les détails de la machine hôte dans la capture d'écran suivante.



Compte tenu de cela, vous avez maintenant installé avec succès le serveur FreeIPA sur Rocky Linux 9 et ajouté l'hôte client Rocky Linux via le client FreeIPA.

Conclusion

Dans ce tutoriel, vous avez appris à installer et à déployer le serveur FreeIPA sur un serveur Rocky Linux 9. Vous avez configuré le serveur FreeIPA sur Rocky Linux avec le DNS activé via Bind et firewalld également configuré.

En outre, vous avez également appris l'utilisation de base de la commande « ipa » pour créer et gérer les utilisateurs et les groupes FreeIPA, ainsi que la manière d'obtenir un ticket Kerberos via la commande kinit et de vous connecter à l'administration Web de FreeIPA via l'utilisateur et le mot de passe administrateur.

Enfin, vous avez ajouté la machine cliente au serveur FreeIPA via le paquet client FreeIPA. Vous avez appris étape par étape comment procéder et vous avez également vérifié vos paramètres en vous connectant à la machine cliente avec l'utilisateur FreeIPA.

Vous pouvez désormais ajouter des hôtes, des utilisateurs et des groupes à votre serveur FreeIPA. Vous pouvez également intégrer FreeIPA à votre environnement de production. Pour plus d'informations, consultez la documentation officielle de FreeIPA.
