Installation serveur primaire

annuaire, identité, authentification, IPA, serveur, installation

FreeIPA est un système de gestion d'identité. Il vise à fournir une identité, une politique et une vérification (Identity Policy Audit, ou IPA) faciles à gérer. FreeIPA est le projet Open Source en amont (upstream) pour Red Hat Identity Manager (Red Hat IDM).

Source : FreeIPA

Note : un certain nombre de choses ont changé pour l'installation de FreeIPA sur CentOS 8. Yum est déprécié au profit de Dnf, la gestion des canaux logiciels a changé.

Firewall

Les règles de firewall se trouvent à cette page.

Amélioration entropie

Afin d'améliorer l'entropie lors des opérations de chiffrement, nous installons et activons rng-tools, si ce dernier n'est pas déjà installé.

```
sudo dnf install rng-tools
sudo systemctl start rngd
sudo systemctl enable rngd
```

Installation

Nous configurons le nom du serveur :

```
hostnamectl set-hostname ipa01.lab.domain.tld
```

Note : le nom de l'hôte doit être le FQDN de la machine, et non pas juste son hostname.

Nous ajoutons les informations de host :

```
echo '172.16.0.21 ipa01.lab.domain.tld ipa01' | sudo tee -a /etc/hosts >
/dev/null
```

ou

```
sudo sh -c "echo '172.16.0.21 ipa01.lab.domain.tld ipa01' >> /etc/hosts"
```

Nous ajoutons

```
sudo dnf module enable idm:DL1
sudo dnf distro-sync
```

Nous installons les paquets nécessaires :

```
sudo dnf install ipa-server ipa-server-dns
```

Nous configurons le serveur :

```
 sudo ipa-server-install --unattended \
   --setup-dns --domain lab.domain.tld --reverse-zone 16.172.in-addr.arpa \
   --hostname ipa01.lab.domain.tld --ip-address 172.16.0.21 \
   --forwarder 8.8.8.8 --ssh-trust-dns \
   --realm LAB.DOMAIN.TLD \
   --idstart 60000 --idmax 65535 --mkhomedir \
   --ds-password 'secret' --admin-password 'secret'
```

Si vous préférez installer FreeIPA en mode interactif

```
sudo ipa-server-install
```

À la fin de l'installation, il vous est rappelé les ports de communications à ouvrir

```
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
```

Création jeton Kerberos

Pour pouvoir accéder à l'interface graphique, nous devons créer un jeton Kerberos

```
# kinit admin
```

Saisissez le mot de passe défini lors de l'installation. Pour vérifier les jetons actifs

```
# klist
```

Pour ne pas avoir à saisir le mot de passe admin à chaque opération, vous pouvez utiliser un fichier keytab. Pour savoir comment procéder, vous pouvez suivre le mode opératoire disponible à cette adresse.

Intégration du certificat SSL

Les informations pour récupérer le certificat racine se trouvent sur cette page.

Désinstallation

Dans le cas où vous ayez à désinstaller FreeIPA (installation avortée, avec une partie des briques installées qui bloque la relance du processus par exemple), la commande pour procédéder à la purge de la configuration

```
sudo ipa-server-install --uninstall
```

Liens

- documentation FreeIPA
- install and setup FreeIPA server on CentOS 8
- gestion d'identité avec FreeIPA
- installation client FreeIPA
- FreeIPA Partie 1 : Installation du serveur et de son réplica
- FreeIPA Partie 2 : Clients, HBAC, Sudo, Mots de passe
- FreeIPA Partie 3 : Haute-disponibilité, Automount