

Ré-enrollement VM dans Free-IPA

Intégrer / ré-enrôler une VM dans le royaume FreeIPA

Procédure d'enrôlement d'un client Linux dans le royaume IdM, et résolution du cas où la liaison des comptes du royaume ne se fait plus.

Paramètre	Valeur
Domaine	example.com
Royaume (realm)	EXAMPLE.COM
Serveur IdM	ipa.example.com
Exemple d'hôte	client01.example.com

Symptôme

La liaison des comptes du royaume ne se fait plus sur une VM (impossible de se connecter avec un compte FreeIPA, `id <user>` ne résout pas les comptes du royaume).

Cause

Supprimer puis recréer l'entrée hôte côté FreeIPA (`ipa host-del` / `ipa host-add`) génère une **nouvelle clé Kerberos**. La VM conserve son ancien `/etc/krb5.keytab`, désormais invalide : SSSD ne peut plus s'authentifier auprès du KDC.

Recréer l'hôte côté serveur ne suffit donc pas — il faut **ré-enrôler le client**.

Piège : `ipa-client-install --force-join` (le vrai « re-enroll ») ne fonctionne que si l'entrée de domaine est restée active. Après un `host-del`, elle ne l'est plus : il faut un enrôlement propre (désinstallation puis réinstallation).

Prérequis

- Nom d'hôte de la VM en **FQDN** (ex. `client01.example.com`), tout en minuscules, uniquement chiffres/lettres/tirets (pas d'underscore).
- FQDN **résolvable via DNS** (résolution directe et inverse). Sinon, fournir l'IP à l'enrôlement avec `--ip-address`, ou utiliser `--force`.
- Horloge synchronisée (Kerberos est sensible au décalage d'heure).
- Identifiants d'un compte autorisé à enrôler : membre du groupe `admins`, ou compte disposant du rôle « Enrollment Administrator ».

Procédure

1. Nettoyer l'ancien enrôlement (si la VM était déjà enrôlée)

```
sudo ipa-client-install --uninstall
```

Retire la configuration SSSD, restaure `/etc/krb5.conf` et nettoie l'ancien keytab.

2. Définir le nom d'hôte en FQDN

```
sudo hostnamectl set-hostname client01.example.com
```

3. Vérifier / corriger `/etc/hosts`

Le FQDN doit précéder le nom court, et le nom d'hôte ne doit pas figurer sur la ligne `localhost` :

```
192.168.x.x    client01.example.com    client01
```

4. Vérifier la résolution

```
hostname -f  
dig +short client01.example.com  
dig +short -x 192.168.x.x
```

`hostname -f` doit renvoyer le FQDN complet.

5. Vérifier l'entrée hôte côté FreeIPA

```
kinit admin-user  
ipa host-show client01.example.com
```

6. Lancer l'enrôlement

```
sudo ipa-client-install \  
  --domain=example.com \  
  --realm=EXAMPLE.COM \  
  --server=ipa.example.com \  
  --principal=admin-user \  
  --mkhomedir
```

`--mkhomedir` : création automatique du répertoire personnel des comptes du royaume à la première connexion.

Tests de validation

```
# Le keytab contient les nouveaux principaux de l'hôte  
sudo klist -kt /etc/krb5.keytab  
  
# Résolution des comptes du royaume (NSS / SSSD)  
getent passwd <user_ipa>  
id <user_ipa>
```

```
# Authentification Kerberos
kinit <user_ipa>
klist

# Test complet de bout en bout
ssh <user_ipa>@client01.example.com
```

Un `kinit` réussi confirme que l'enrôlement est fonctionnel.

Sources officielles

- Installation d'un client IdM — Red Hat :
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/installing_identity_management/assembly_installing-an-idm-client_installing-identity-management
- Ré-enrôlement d'un client IdM — Red Hat :
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/installing_identity_management/re-enrolling-an-idm-client
- Désinstallation d'un client IdM — Red Hat :
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/installing_identity_management/uninstalling-an-ipa-client_installing-identity-management
- FQDN requis par `ipa-client-install` (Solution 200673) — Red Hat :
<https://access.redhat.com/solutions/200673>
- Gestion de `chronyd` par FreeIPA :
https://www.freeipa.org/page/V4/ntpd_deprecation/chronyd_support

Revision #2

Created 2026-09-16 08:54:01 UTC by Florian

Updated 2026-09-16 08:55:16 UTC by Florian