

Mettre une machine linux sur un AD windows





Amaury Chasline & Zineddine Hadjab

Table des matières

Pré-requis :	3
Vérification de la connexion à l'AD	3
Synchroniser L'horloge :	3
Installer les paquets nécessaires :	4
Mise à système et installer les dépendances :	4
Configuration de Kerberos :	4
Connexion à l'AD :	5
Modification de « Resolve.conf » et « Resolv.conf » :	5
Joindre la machine au domaine AD :	5
Configurer le fichier Idap :	5
Vérification de l'intégration :	6



Pré-requis:

Vérification de la connexion à l'AD

Vous devez avoir un accès réseau à votre Debian pour joindre le contrôleur de domaine (DC)

« ping 'nom du domaine' »

```
root@SRV-GLPI:~# ping iuto-5.priv
PING iuto-5.priv (10.200.0.1) 56(84) bytes of data.
64 bytes from 10.200.0.1 (10.200.0.1): icmp_seq=1 ttl=128 time=0.569 ms
64 bytes from 10.200.0.1 (10.200.0.1): icmp_seq=2 ttl=128 time=0.781 ms
64 bytes from 10.200.0.1 (10.200.0.1): icmp_seq=3 ttl=128 time=0.899 ms
^C
--- iuto-5.priv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.569/0.749/0.899/0.136 ms
root@SRV-GLPI:~# _
```

Configurer le « nano /etc/hosts » pour inclure le contrôleur de domaine.

```
GNU nano 7.2

/etc/hosts
127.0.0.1 localhost
10.200.0.1 SRV-GLPI.debiancli.debian.loc SRV-GLPI

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Synchroniser L'horloge:

Mettre à jour :

- « apt update & apt upgrade »
- « apt install ntpsec »
- «systemctl start ntp»



Installer les paquets nécessaires :

Mise à système et installer les dépendances :

- « apt update »
- « apt install sssd sssd-tools realmd adcli krb5-user samba-common-bin packagekit »

Configuration de Kerberos :

Vous pouvez laisser par défault car nous allons le configure dans le dossier :

« nano /etc/krb5.conf »

```
GNU nano 7.2

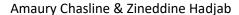
[libdefaults]
    default_realm = SRV-GLPI.IUTO-5.priv

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    rdns = false

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    IUTO-5.priv = {
     kdc = SRV5-AD1.IUTO-5.priv
     admin_server = SRV5-AD1.IUTO-5.priv
}
```

```
[domain_realm]
.iuto-5.priv = IUTO-5.priv
iuto-5.priv = IUTO-5.priv
```





Connexion à l'AD:

Modification de « Resolve.conf » et « Resolv.conf » :

Vous devez écrire « nameserver '@IP de votre srv AD' »

```
GNU nano 7.2 /etc/resolv.conf
nameserver 10.200.0.1
```

Joindre la machine au domaine AD:

« adcli join -D IUTO-5.priv -U administrateur -v »

```
root@SRV-GLPI:~# adcli join -D IUTO-5.priv -U administrateur -v
```

Puis taper votre mot de passe.

Configurer le fichier ldap:

Dans le dossier « nano /etc/ldap/ldap.conf »

Puis écrivez « TLS_REQCERT try »

```
## LDAP Defaults
## See Idap.conf(5) for details
# This file should be world readable but not world writable.

##BASE dc=example,dc=com
#URI Idap://ldap.example.com Idap://ldap-provider.example.com:666

#$SIZELIMIT 12
#TIMELIMIT 15
#DEREF never

## TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
TLS_REQCERT try
```



Amaury Chasline & Zineddine Hadjab

Vérification de l'intégration :

Une fois la machine jointe au domaine, vous pouvez vérifier avec la commande « realm list »

Vous pouvez également vous rendre sur votre AD et vérifier que le poste est bien remonté, taper la commande suivante dans votre cmd : « dsa.msc »

On peut apercevoir que nos deux machines linux sont bien remonté dans notre AD.

