

Joindre un domaine en tant que Contrôleur de domaine

Prérequis

Comme pour tout contrôleur de domaine, il faut :

- Une IP FIXE (ici 172.16.4.2)
- Un contrôleur de domaine à joindre (ici 192.168.4.2)
- Un nom de domaine unique (ici SAMBA)
- un domaine défini (ici domain.tld)

Configuration DNS

Pour pouvoir joindre un contrôleur de domaine, il faut configurer le serveur de DNS de la machine. Par exemple, avec `/etc/resolv.conf`

[/etc/resolv.conf](#)

```
search domain.tld
nameserver 192.168.4.2
```

Initialisation

Pour commencer, on va installer les paquets nécessaires (ignorez les configurations demandées):

```
# apt install acl attr samba krb5-user krb5-config winbind
```

(Vous pouvez aussi [compiler depuis les sources](#))

Il vous faudra commencer par arrêter et désactiver samba :

```
# systemctl disable --now nmbd smb� winbind
```

Il vous faudra supprimer la configuration de samba :

```
# rm /etc/samba/smb.conf
```

Il vous faudra configurer Kerberos ¹⁾:

[/etc/krb5.conf](#)

```
[libdefaults]
```

```
dns_lookup_realm = false
dns_lookup_kdc = true
default_realm = DOMAIN.TLD
```

Pour vérifier que la configuration est bonne, vous pouvez lancer :

```
# kinit administrateur
```

Puis lancez *klist*, vous devriez obtenir quelque chose ressemblant à ça:

```
# klist
```

```
Ticket cache: FILE:/tmp/krb5cc_0
```

```
Default principal: administrateur@DOMAIN.TLD
```

Valid starting	Expires	Service principal
24.09.2015 19:56:55	25.09.2015 05:56:55	krbtgt/DOMAIN.TLD@DOMAIN.TLD
renew until 25.09.2015 19:56:53		

Joindre l'Active Directory en tant que Contrôleur de Domaine

Pour joindre un AD, il faut lancer la commande :

```
# samba-tool domain join domain.tld DC --use-rfc2307 -  
U"administrateur@domain.tld" --dns-backend=SAMBA_INTERNAL
```

```
Finding a writeable DC for domain 'domain.tld'  
Found DC ad.domain.tld  
Password for [DOMAIN\administrateur]:  
workgroup is DOMAIN  
realm is domain.tld  
Adding CN=SAMBA,OU=Domain Controllers,DC=domain,DC=tld  
Adding  
CN=SAMBA,CN=Servers,CN=SITE,CN=Sites,CN=Configuration,DC=domain,DC=tld  
Adding CN=NTDS  
Settings,CN=SAMBA,CN=Servers,CN=SITE,CN=Sites,CN=Configuration,DC=domain,DC=  
tld  
Adding SPNs to CN=SAMBA,OU=Domain Controllers,DC=domain,DC=tld  
Setting account password for SAMBA$  
Enabling account  
Calling bare provision  
Looking up IPv4 addresses  
Looking up IPv6 addresses  
No IPv6 address will be assigned  
Setting up share.ldb  
Setting up secrets.ldb  
Setting up the registry  
Setting up the privileges database
```

```
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
A Kerberos configuration suitable for Samba 4 has been generated at
/usr/local/samba/private/krb5.conf
Provision OK for domain DN,DC=domain,DC=tld
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=domain,DC=tld] objects[402/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=domain,DC=tld] objects[804/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=domain,DC=tld] objects[1206/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=domain,DC=tld] objects[1550/1550]
linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=domain,DC=tld] objects[402/1618]
linked_values[0/0]
Partition[CN=Configuration,DC=domain,DC=tld] objects[804/1618]
linked_values[0/0]
Partition[CN=Configuration,DC=domain,DC=tld] objects[1206/1618]
linked_values[0/0]
Partition[CN=Configuration,DC=domain,DC=tld] objects[1608/1618]
linked_values[0/0]
Partition[CN=Configuration,DC=domain,DC=tld] objects[1618/1618]
linked_values[42/0]
Replicating critical objects from the base DN of the domain
Partition[DC=domain,DC=tld] objects[100/100] linked_values[23/0]
Partition[DC=domain,DC=tld] objects[386/286] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=domain,DC=tld
Partition[DC=DomainDnsZones,DC=domain,DC=tld] objects[44/44]
linked_values[0/0]
Replicating DC=ForestDnsZones,DC=domain,DC=tld
Partition[DC=ForestDnsZones,DC=domain,DC=tld] objects[19/19]
linked_values[0/0]
Committing SAM database
Sending DsReplicaUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database
Joined domain DOMAIN (SID S-1-5-21-469703510-2364959079-1506205053) as a DC
```

Il vous faudra ensuite démarrer SAMBA :

```
# systemctl unmask samba-ad-dc
```

puis

```
# systemctl enable --now samba-ad-dc
```

Puis vérifier que la réplication du contrôleur du domaine est faite (cela peut prendre plusieurs minutes)

```
# samba-tool drs showrepl
```

```
SITE\DC2
DSA Options: 0x00000001
DSA object GUID: c14a774f-9732-4ec2-b9fa-2156c95c4e48
DSA invocationId: 7bdb135c-6868-4dd9-9460-33dea4b6b87b

==== INBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ Thu Sep 24 20:08:46 2015 CEST was successful
    0 consecutive failure(s).
    Last success @ Thu Sep 24 20:08:46 2015 CEST

DC=DomainDnsZones,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
    0 consecutive failure(s).
    Last success @ Thu Sep 24 20:08:45 2015 CEST

CN=Configuration,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ Thu Sep 24 20:08:46 2015 CEST was successful
    0 consecutive failure(s).
    Last success @ Thu Sep 24 20:08:46 2015 CEST

DC=ForestDnsZones,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
    0 consecutive failure(s).
    Last success @ Thu Sep 24 20:08:45 2015 CEST

DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
    0 consecutive failure(s).
    Last success @ Thu Sep 24 20:08:45 2015 CEST

==== OUTBOUND NEIGHBORS ====
```

```
CN=Schema,CN=Configuration,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ NTTIME(0) was successful
    0 consecutive failure(s).
    Last success @ NTTIME(0)

DC=DomainDnsZones,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ NTTIME(0) was successful
    0 consecutive failure(s).
    Last success @ NTTIME(0)

CN=Configuration,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ NTTIME(0) was successful
    0 consecutive failure(s).
    Last success @ NTTIME(0)

DC=ForestDnsZones,DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ NTTIME(0) was successful
    0 consecutive failure(s).
    Last success @ NTTIME(0)

DC=domain,DC=tld
  Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
    Last attempt @ NTTIME(0) was successful
    0 consecutive failure(s).
    Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
  Connection name: fb03f58b-1654-4a02-8e11-f0ea120b60cc
  Enabled          : TRUE
  Server DNS name  : DC1.samdom.example.com
  Server DN name   : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=tld
  TransportType: RPC
  options: 0x00000001
Warning: No NC replicated for Connection!
```

Modification DNS

Il faut modifier le DNS de la machine dans /etc/resolv.conf

```
search projet2.local
nameserver 172.16.4.2
nameserver 192.168.4.2      # IP de l'AD joint
```

et aussi dans le fichier `/etc/samba/smb.conf` dans la section global

[/etc/samba/smb.conf](#)

```
dns forwarder = 8.8.8.8      # Évitez de mettre l'IP de L'AD joint
```

Test du Contrôleur de Domaine

Il faut d'abord vérifier si la réplication entre les deux contrôleur de domaine ce fait, en créant un utilisateur, et en vérifiant que l'utilisateur a été créer. Voir commande `samba-tool user`

Attention, il y a un certain délai entre les réplications :

```
SAMBA ----> SAMBA = 15 secondes
SAMBA ---->  AD  = 15 minutes
AD ----> SAMBA = 30 secondes
AD ---->  AD  = 30 secondes
```

La difference s'explique dans le mode de fonctionnement de la réplication qui est différent dans SAMBA. En gros, SAMBA ne sait pas communiquer les modifications aux Windows Server, donc c'est celui-ci qui periodiquement (maximum 4 fois par heure) va chercher les information sur le Contrôleur de domaine SAMBA. Cela devrait ce régler sous peu.

A noté qu'il existe une commande pour lancer la réplication de force.

Il faut ensuite connecter un Poste Windows au domaine, comme pour joindre un Domaine Active Directory.

Un fois connecter on vérifier sur quel contrôleur de domaine il est connecter avec la commande Windows `echo %logonserver%`

```
C:\>echo %logonserver%
\\SAMBA
```

1)

default_realm doit être en majuscule

From:
<https://wiki.virtit.fr/> - VirtIT

Permanent link:
https://wiki.virtit.fr/doku.php/kb:linux:samba:joindre_un_domaine_en_tant_que_controleur_de_domaine?rev=1575043184

Last update: 2019/11/29 15:59

