Utiliser le DNS Bind9 avec Active Directory

Lien :

- https://www.it-connect.fr/dns-avec-bind-9%ef%bb%bf/
- https://www.it-connect.fr/active-directory-les-enregistrements-dns-indispensables/
- https://www.serverlab.ca/tutorials/linux/network-services/using-linux-bind-dns-servers-for-active-directory-domains/

Enregistrements nécessaires

Un contrôleur de domaine Active Directory a besoin d'enregistrements de ressources du localisateur SRV (Service Location) pour fonctionner.

Un enregistrement SRV doit exister pour les services suivants :

- _kerberos
- _ldap

Les enregistrements de ressources du localisateur SRV sont renseignés dans le fichier **Netlogon.dns** du dossier **%systemroot%\System32\Config**.

Le premier enregistrement dans le fichier est l'enregistrement SRV (Lightweight Directory Access Protocol) du contrôleur de domaine (LDAP) et doit ressembler à ce qui suit :

```
_ldap._tcp. <Domain_Name>
```

Nslookup permet d'afficher des informations utiles pour diagnostiquer l'infrastructure DNS (Domain Name System).

Pour vérifier les enregistrements SRV avec Nslookup :

- Tapez nslookup et appuyez sur Entrée.
- Tapez set type=all et appuyez sur Entrée.
- Tapez *ldap.*tcp.dc.*msdcs.Domain*Name, où <Domain_Name> est le nom de votre domaine, puis appuyez sur Entrée.

Le serveur DNS doit avoir les enregistrements suivant **avant** d'installer le service Active Directory sur le contrôleur de domaine.

Sans ces zones préalablement crées, le contrôleur de domaine ne pourra pas les enregistrements DNS requis pour un fonctionnement normal.

Liste des enregistrements nécessaires :

Rôle	**Enregistrement DNS**	**Type**	**Requis**
PDC	_ldap._tcp.pdc._msdcs.	SRV	Uniquement un par domaine
GC	_ldap._tcp.gc._msdcs.	SRV	Au moins un par forêt
KDC	_kerberos._tcp.dc._msdcs.	SRV	Au moins un par domaine
DC	_ldap._tcp.dc._msdcs.	SRV	Au moins un par domaine
FQDN	<FQDN-Contrôleur-de-domaine>	A	Un enregistrement par contrôleur de domaine
Adresse IP du GC	gc.*msdcs.<Nom-DNS-Forêt>* | *A* |*Au moins un par forêt*| |*GUID via CNAME* |<*DC-GUID*>.msdcs.<Nom-DNS-Forêt>	CNAME	Un enregistrement par contrôleur de domaine

Configuration de Bind9

Il est préférable d'utiliser un fichier de zone séparé pour les enregistrements dynamiques que va faire le contrôleur de domaine Active Directory dans Bind9.

Il est nécessaire de permettre, avec la directive **allow-update**, la création d'enregistrements dns pour :

- le contrôleur de domaine pour le bon fonctionnement d'Active Directory
- les clients Windows pour créer leur propre enregistrement DNS lors de l'adhésion au domaine.

Editez le fichier **/etc/bind/named.conf.local** pour

- ajouter en plus de la zone **agence.cub.fr** la zone **_msdcs.agence.cub.fr**
- ajouter la directive **allow-update** à cette zone en précisant les adresses IP autorisées

```
zone "agence.cub.fr" {
```

```
    type master;
    file "/etc/bind/db.agence.cub.fr";
};

zone "_msdcs.agence.cub.fr" {
   type master;
   file "/var/cache/bind/db._msdcs.agence.cub.fr";
   allow-update { 172.16.x.x; 192.168.x.y/24}
};
```

Création du fichier de zone _msdcs.agence.cub.fr

```
cp /etc/bind/db.empty /etc/bind/_msdcs.agence.cub.fr
```

Le fichier **_msdcs.agence.cub.fr** doit être modifiée pour avoir un contenu de ce type :

Exemple de configuration

```
; enregistrement Active directory du  domaine cub.fr
srv-ad                                      IN  A   172.16.x.y
_ldap._tcp                                  IN  SRV  0 0 389 srv-ad
_ldap._tcp.pdc._msdcs                       IN  SRV  0 0 389 srv-ad
_ldap._tcp.dc._msdcs                        IN  SRV  0 0 389 srv-ad
_ldap._tcp.gc._msdcs                        IN  SRV  0 0 389 srv-ad
_kerberos._tcp                              IN  SRV  0 0 88  srv-ad
_kerberos._tcp.dc._msdcs                    IN  SRV  0 0 88  srv-ad
_ldap._tcp.default-First-Site-Name._sites     IN  SRV  0 0 389 srv-ad
_kerberos._tcp.Default-First-Site-Name._sites IN  SRV  0 0 88  srv-ad
```

Retour Configurer le service DNS

- Configurer le service DNS