

Utilisation des serveurs DNS Linux BIND pour les domaines Active Directory

Lien : <https://www.serverlab.ca/tutorials/linux/network-services/using-linux-bind-dns-servers-for-active-directory-domains/>

Présentation

Active Directory s'appuie sur le DNS pour fonctionner correctement. Si votre environnement dispose déjà d'un serveur DNS BIND basé sur Linux, il est possible que les zones DNS Active Directory soient hébergées sur le serveur DNS existant.

Les avantages :

- Un serveur Linux BIND est un serveur DNS très léger et rapide.
- Linux peut être plus sûr car il y a moins de vulnérabilités connues.

Les inconvénients :

- perte de certaines fonctionnalités d'Active Directory.
- les zones de domaine BIND ne peuvent avoir qu'un seul maître, contrairement à Windows DNS. Un serveur de noms Windows dans un environnement Active Directory est capable d'être multimaître, ce qui vous donne une disponibilité beaucoup plus élevée.

Configurations nécessaires

Les zones suivantes sont créées pour Active Directory dans le serveur de noms.

Ces zones doivent être **créés avant** la configuration du premier contrôleur de domaine.

Sans ces zones, le contrôleur de domaine ne sera pas en mesure d'enregistrer les enregistrements DNS requis pour qu'Active Directory fonctionne correctement.

Zone de domaine DNS	Exemple	Obligatoire/Optionnel
votre-nom-de-domaine-fqdn	corp.serverlab.intra	Obligatoire
_msdcs.votre-nom-de-domaine-fqdn	_msdcs.corp.serverlab.intra	Optionnel
_Sites.votre-nom-de-domaine-fqdn	_sites.corp.serverlab.intra	Optionnel
_Tcp.votre-nom-de-domaine-fqdn	_tcp.corp.serverlab.intra	Optionnel
_Udp.votre-nom-de-domaine-fqdn	_udp.corp.serverlab.intra	Optionnel

La première zone de domaine est requise. Les zones restantes ne sont nécessaires que si vous souhaitez organiser vos enregistrements dans différentes bases de données, par exemple pour des raisons administratives ou de performances. Si vous ne créez pas ces zones, elles seront automatiquement créées dans la base de données de la première zone.

Création des zones de domaine Active Directory

Complétez le fichier `/etc/bind/named.conf.local`.

- autoriser les mises à jour depuis vos réseaux internes :

```
zone "agence.cub.fr" {
    type master;
    file "/etc/bind/db.agence.cub.fr";
    allow-update { 172.x.y.z/24; 192.x.y.z/24; };
};
```

- ajoutez la zone `_msdcs`

```
zone "_msdcs.agnce.cib.fr" IN {
    type master;
    file "/etc/bind/_msdcs.agence.cub.fr";
    allow-update { 172.x.y.z/24; 192.x.y.z/24; };
};
```

- créez le fichier de zone `/etc/bind/_msdcs.agence.cub.fr` avec le contenu suivant

```
$TTL 1D
agence.cub.fr.      IN      SOA      ns0.agence.cub.fr. root.agence.cub.fr. (
    2006031201      ; serial
    1D              ; refresh
    1H              ; retry
    1W              ; expire
    3H)             ; Negative Cache TTL

agence.cub.fr. IN      NS       ns0.agence.cub.fr.
```

- redémarrer le service Bind9

Exemple de configuration pour l'AD CUB

```
; 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
```

Promouvoir le serveur Windows en contrôleur de domaine

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/systeme/windows/server/bind?rev=1759397461>

Last update: 2025/10/02 11:31

