

## Service DDNS dynamique

Pour la reconnaissance du contrôleur de domaine Samba par vos clients Windows, trois choix de service s'offrent à vous:

- Utiliser le fichier *hosts* situé sur chacun des ordinateurs clients (soit se retrouver comme dans les années 70 et faire des dépressions chroniques);
- Monter un serveur WINS (ce qui est complètement désuet et qui n'est plus utilisé depuis Windows NT4);
- Ou simplement monter un serveur DDNS (la meilleure alternative).

Pour obtenir un serveur DDNS, il vous faut combiner un serveur DNS et un serveur DHCP. Le concept en est fort simple, et reste les mêmes processus tant sous Windows que sur Linux.

Le client (*0.0.0.0*) fait une demande de localisation de bail IP (*DHCPDiscover*) en diffusion générale (*255.255.255.255*) sur le réseau pour obtenir une adresse IP d'un serveur DHCP et obtenir des données d'adressage IP.

Ensuite tous les serveurs disponibles sur le réseau envoient une offre au client (*DHCPOffer*), si ce dernier est autorisé par le serveur DHCP.

Le client sélectionne alors une des adresses proposées par l'un des serveurs, puis émet une diffusion générale pour demander un bail relatif à l'adresse retenue par le client (*DHCPRequest*).

Le serveur DHCP a alors deux choix, retenir la demande du client et lui envoyer la confirmation d'acceptation du bail (*DHCPACK*) ou simplement refuser cette demande (*DHCPNACK*).

Lors de l'enregistrement du bail par le serveur DHCP, le service DHCP envoie les données du client au serveur DNS pour qu'il enregistre le client dans sa zone de résolution de nom.

Il est essentiel, sous Linux, que vous utilisiez la version BIND 8.x et supérieure (<http://www.isc.org/products/BIND>) avec le ISC DHCP 3.x et supérieure (<http://www.isc.org/products/DHCP>) pour que cette combinaison supporte la fonctionnalité DDNS.

### NOTES



## Procédures d'installation de BIND 9.x

Les procédures qui suivent, expliquent comment installer BIND et ne concerne en aucun cas la sécurisation de ce service. De toute manière, nous montons un serveur BIND qui doit être accessible que par le réseau interne seulement et qui devrait être moins sujet à des attaques (mais ce n'est pas une raison de ne pas le sécuriser).



**NOTE:** N'oublier pas de changer le *cybiolab.lan* par le nom de domaine que vous désirez utiliser sur votre réseau interne.

### Installation de BIND 9.x

Nous allons maintenant ajouter les USE flags directement dans le fichier */etc/portage/package.use*, cela permettra d'appliquer ces flags à chaque nouvelle installation ou mise à jour.

Par défaut ce fichier est inexistant et devra donc être créé (avec vim par exemple). Ceci vous évitera de devoir les définir pour chaque mise à jour du paquetage Bind. Ajouter l'entrée suivante.

```
vim /etc/portage/package.use
net-dns/bind -ipv6 ssl ldap
```

Pour faire l'installation, saisir la commande suivante:

```
emerge -va bind
```

Dans le fichier */etc/bind/named.conf*, vous devriez obtenir quelque chose qui ressemble à ceci.

```
vim /etc/bind/named.conf
```

```
options {
    directory "/var/bind";

    // Adresse d'ecoute de BIND
    listen-on { 127.0.0.1; 192.168.0.2; };

    //Autorise les requêtes itératives.
    allow-query { localhost; 192.168.0.0/24; };

    //Autorise les requêtes inversées.
    allow-recursion { localhost; 192.168.0.0/24; };

    //Location du fichier du Process ID (PID) de BIND.
```

NOTES















A remarquer que le script ne supprime pas les fichiers **Kdhp\_updater.+\*.key** dans le répertoire `/etc/bind`. Vous devrez donc les supprimer à la main ou modifier ce script. Vérifier aussi que le fichier **named.keys** est bien dans le répertoire `/etc/bind`.

## Démarrage du service DNS

Maintenant que le serveur BIND est configuré pour répondre aux requêtes de notre domaine, démarrons le service et faisons quelques tests pour vérifier son bon fonctionnement.

```
/etc/init.d/named start
```

## Vérification du serveur BIND

Vous pouvez faire la vérification de votre fichier de configuration `named.conf` du service `bind`.

```
named-checkconf -z /etc/bind/named.conf
zone localhost/IN: loaded serial 2008122601
zone 127.in-addr.arpa/IN: loaded serial 2008122601
zone cybiolab.lan/IN: loaded serial 2010022301
zone 0.168.192.in-addr.arpa/IN: loaded serial 2010022301
```

Faites aussi l'installation des outils de vérification de BIND, tel que `dig`, `nslookup` et `host`.

```
emerge -va bind-tools
```

Ensuite procéder à une vérification que vos requêtes directes fonctionnent correctement:

```
dig serveurpdc.cybiolab.lan
```

Si vous désirez faire une *requête directe* sur l'entrée `serveurpdc.cybiolab.lan` sur le serveur DNS `192.168.0.2` sans avoir les `bind-tools`, utiliser la commande.

```
ping serveurpdc.cybiolab.lan
```

```
PING serveurpdc (192.168.0.2) 56(84) bytes of data:
64 bytes from serveurpdc (192.168.0.2): icmp_seq=1 ttl=64 time=0.063 ms
```

Assurez-vous cependant que le fichier `resolv.conf` pointe bien sur votre nouveau serveur DNS.

NOTES







## Problème

Lors d'un **host 192.168.0.2**, vous obtenez l'erreur suivante:

*Host 2.0.168.192.in-addr.arpa not found: 2(SERVFAIL)*

## Solution

Assurez-vous que vos entrées dans les fichiers `named.conf` ainsi que dans le `0.168.192.in-addr.arpa` sont correctes.

## Problème

Lors du **ping serveurpdc.cybiolab.lan**, vous obtenez l'erreur suivante:

*ping: unknown host serveurpdc.cybiolab.lan*

## Solution

Assurez-vous que l'entrée dans le fichier `/etc/hosts` pour votre serveur soit correct.

```
192.168.0.2      serveurpdc.cybiolab.lan serveurpdc
```

NOTES

