

Les « VIEWS » dans Bind9

Par défaut jusqu'à la version 9 de Bind, un serveur de nom qui était interrogé, ne pouvait pas différencier si le client DNS était une machine du réseau local ou externe. De même le comportement du serveur était le même pour toute machine cliente. Le serveur DNS BIND livrait donc la totalité des informations qu'il détenait sur une zone, sans tenir compte de l'origine du client qui le questionnait.

Dans ce contexte, on imagine qu'un serveur Bind pouvait servir de serveur « récursif » pour n'importe quelle machine de l'internet. Il pouvait donc être obligé d'aller résoudre lui même des noms en interrogeant d'autres serveurs, et donc enrichir son cache... avec une possibilité de corruption de cache si toutefois il interrogeait un serveur pirate en recevant des requêtes DNS forgées.

Pour sécuriser cet aspect du DNS et contrôler pour le « compte de qui? » on lance des requêtes récursives, on aimerait en fait pouvoir servir de serveur récursif pour les machines clientes de notre réseau local, et non pas pour les machines extérieures.

Pour les machines extérieures on souhaite se contenter de délivrer des informations sur les zones locales que le serveur gère et dont il est serveur primaire.

Pour cela, BIND9 introduit une nouvelle fonctionnalité appelée les « views » qui permet de délivrer des informations différentes sur les « zones DNS » qu'un serveur gère, en fonction des adresses IP des clients qui interrogent le serveur.

L'idée est de tester l'adresse IP d'un client et de modifier le comportement du serveur BIND en fonction de l'appartenance des clients à certains subnet.

Pour cela BIND introduit une syntaxe spéciale à l'aide des mots clés « *view* » « *match-client* » et « *acl* »:

```
view « nomdelavue » {  
    match-clients { <classe-d'adresse> | <une_acl> | « any » | « localnets » };  
    <un ensemble d'options de Bind9>;  
}
```

Cette syntaxe permet de spécifier que seuls les clients DNS dont l'adresse IP correspond à celle donnée dans la directive « *match-clients* » seront affectés par les options DNS qui suivent.

La directive « *match-clients* » permet de spécifier soit

- des subnets, 139.124.2.0/24 par exemple
- des mots clés tels que « ANY » correspondant à n'importe quelle machine, ou « LOCALNETS » correspondant aux machines du réseau local sur lequel se trouve le serveur.

Exemple:

```
view "internal" {  
    match-clients { 139.124.2.0/24 ; };  
    recursion yes;  
    include "/etc/bind/meszonesdns.txt";  
};
```

L'exemple ci dessus signifie que la « view » appelée « *internal* » s'appliquera aux machines clientes dont les adresses sont dans le subnet 139.124.2.0/24. Pour cet ensemble de machine la directive

« *recursion yes* » sera appliquée. Les informations des zones présentes dans le fichier `/etc/bind/meszonesdns.txt` seront fournies

Avec cette syntaxe notre serveur DNS BIND9 se comportera comme un serveur « récursif » lorsque ce sont des machines clientes appartenant à notre réseau local, qui l'interogent.

Pratiquement si on gère plusieurs subnets, il sera plus souple et efficace de dénombrer un certains nombres de subnets à l'aide de la directive « ACL » de Bind.

Exemple

```
acl "zoneinternes" {
    { 139.124.2/24; };
    { 139.124.16/24; };
    { 139.124.17/24; };
    { 139.124.232/24; };
    { 139.124.128/22; };
    { 139.124.224/24; };
};
```

A l'aide de l'ACL « zoneinterne », notre exemple de view donnera:

```
view "internal" {
    match-clients { zoneinternes ; };
    recursion yes;
    include "/etc/bind/meszonesdns.txt";
};
```

Si on veut alors interdire le mode récursif du serveur pour toute autre machine, on écrira:

```
view "external" {
    match-clients { any; };
    recursion no;
    include "/etc/bind/meszonesdns.txt";
};
```

Grâce à ces lignes, on définit une autre « view » appelée « *external* », qui sera prise en compte pour toute machine cliente (mot clé « *any* »). Dans ce cas de figure, le mode récursif de Bind est désactivé (« *recursion no* »). Le serveur Bind se contente alors de fournir des résolutions de noms pour les zones locales dont il est serveur primaire.

Cet aspect des views de Bind9 est décrit dans l'ouvrage O'Reilly sur Bind9, et sur le WEB sur http://sysadmin.oreilly.com/news/views_0501.html