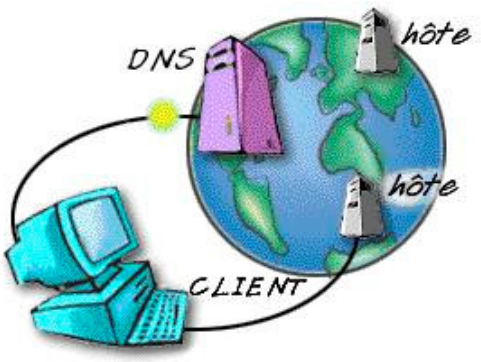
Julien Vehent

BTS Informatique de gestion – Option ARLE

Résolution de noms complètement qualifiés avec Domain Name System (DNS)



Serveur Linux Red Hat 9.0 et Bind 9.2
Clients Windows 2000 Professionnel & Debian

Récapitulatif des compétences mises en œuvres :

- ✓ *C22 Installer et configurer un réseau*
- ✓ *C31 Assurer les fonctions de bases de l'administrateur réseau*
- ✓ *C34 Surveiller et optimiser le trafic sur le réseau*

1. Principe de DNS

Chaque station d'un réseau TCP/IP possède une adresse IP propre. Cependant, il est très difficile de travailler avec des adresses numériques du type 192.168.1.3. C'est pourquoi le protocole DNS à été développé. Ce dernier reprend le principe des noms NETBIOS et y rajoute le domaine d'appartenance en suffixe.

On obtient ainsi une table de correspondance entre des adresses IP et des noms complètement qualifiés (FQDN : Fully Qualified Domain Name).

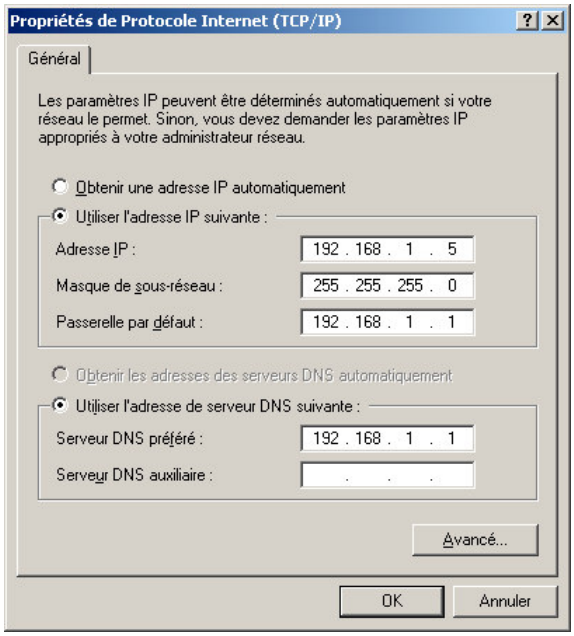
Ex : srvlinux.iscb-corporation.com ↔ 192.168.1.1

La résolution de nom est la corrélation entre les adresses IP et le nom de domaine associé.

Les requêtes DNS sont envoyées via le port 53 en utilisant le protocole de couche 4 UDP.

2. Configuration du client

Que le client soit une machine sous Linux ou sous Windows, la configuration est la même. Dans les paramètres TCP/IP, on spécifie l'adresse du - ou des – serveur DNS par ordre de préférence.



Configuration TCP/IP sur un poste Windows 2000 pro
Le 4éme champ est l'adresse de notre serveur DNS.

L'outil nslookup donne la configuration DNS d'une machine.

Ex : *#nslookup localhost*
Serveur par défaut : srvlinux.iscb-corporation.com
Address : 192.168.1.1

2. Configuration du serveur

Le serveur fonctionne avec la distribution Linux Red Hat 9. Pour déployer la fonctionnalité DNS, on utilise le logiciel Bind 9.2.

Le principe est le suivant :
Dans le fichier /etc/named.conf, on déclare les zones de résolution de noms. Chaque zone comprend deux déclarations : une pour la résolution de noms, une pour la résolution d'adresses.

Extrait du fichier named.conf : Déclaration de la zone de résolution de noms

```
zone "iscb-corporation.com"{                    #nom de la zone
        type master;                            #le serveur est maître de la zone
        file "iscb-corporation.com.db";         #nom du fichier de zone dans /var/named/
        allow-update {                          #autorisation des MAJ DDNS depuis 127.0.0.1
                127.0.0.1;
                };
};
```

Dans la déclaration de zone, on spécifie un fichier de zone que l'on va créer dans /var/named/ .
Pour chaque déclaration dans le fichier named.conf, on a un fichier dans /var/named/ .
Dans ce dernier, on vas déclarer les résolutions statiques.

FICHIER ISCB-CORPORATION.COM.DB

```
; Serveur primaire DNS - domaine " iscb-corporation.com"
@ IN SOA srvlinux.iscb-corporation.com. julien.srvlinux.iscb-corporation.com. (
        2004060102    ; serial
        21600         ; refresh
        1800          ; retry
        604800        ; expire
        900 )         ; TTL
;
; Definition des serveurs de nom
;
        IN      NS      srvlinux.iscb-corporation.com.
;
; Definition des serveurs de mail
;
        IN      MX      10 srvlinux.iscb-corporation.com.
;
; Definition du localhost
;
localhost       IN      A       127.0.0.1
;
; Definition des hotes de la zone
;
srvlinux        IN      A       192.168.1.1
pcswitcher      IN      A       192.168.1.99
;
```

srvlinux.iscb-corporation.com : serveur DNS primaire de la zone.

julien.srvlinux.iscb-corporation.com : adresse mail de l'administrateur.

serial : numéro de version de la zone du type AAAAMMJJNN.

refresh : temps d'attente en secondes pour qu'un serveur secondaire vérifie si le serveur primaire a fait des modifications.

expire : temps de conservation des données pour un serveur secondaire.

TTL : durée de vie par défaut des enregistrements.

Instructions :
NS → serveur de noms (Name Server)
MX → serveur de messagerie (Mail eXchanger)
On défini une priorité pour le serveur de mail. Plus elle est basse, plus le serveur est prioritaire (ici : 10).
A → hôte

Une fois la zone iscb-corporation.com créée, on configure la zone de recherche inversée : 1.168.192.in-addr.arpa.net

Extrait du fichier named.conf : Déclaration de la zone de résolution d'adresses

```
zone "1.168.192.in-addr.arpa.net"{
        type master;
        file "192.168.1.db";
        allow-update {
                127.0.0.1;
                };
};
```

et le fichier correspondant :

FICHIER 192.168.1.DB

```
;
;       adresses de mapping hostname
;
$TTL 1w
@       IN      SOA     srvlinux. iscb-corporation.com. julien.rnejv.com. (
        1999022702      ; Serial
        21600           ; Refresh
        1800            ; Retry
        604800          ; Expire
        900 )           ; Negative cache TTL
        IN      NS      srvlinux.iscb-corporation.com.
99.1    IN      PTR     pcswitcher.iscb-corporation.com.
1.1     IN      PTR     srvlinux.iscb-corporation.com.
3.1     IN      PTR     portable.iscb-corporation.com.
```

99.1 → adresse IP de pcswitcher. iscb-corporation.com.
PTR → associe l'adresse au nom FQDN (PTR=Point To Record)

Enfin, on édite le fichier /etc/resolv.conf pour y spécifier le domaine et le serveur DNS.

FICHIER RESOLV.CONF

```
domain iscb-corporation.com
nameserver 192.168.1.1
```

3. La fonction DDNS

Le serveur DNS peut fonctionner de deux manières : soit la table de correspondance est nourrie statiquement comme nous venons de le voir, soit elle est nourrie par le serveur DHCP qui communique au DNS le nom et l'adresse IP d'un poste venant de recevoir un bail DHCP.
La fonction de Dynamic DNS ne nécessite que très peu de configuration au niveau du serveur DNS. Ici, on voit dans le fichier named.conf les lignes :

```
allow-update {
        127.0.0.1;
        };
```

qui autorisent le serveur DNS à recevoir des informations du serveur DHCP local.
Les correspondances ainsi reçues ne seront pas stockées dans les fichiers de zones et de zones inverses mais dans des fichiers qui porteront les mêmes noms suivis de **.jnl** dans /var/named/

//la configuration du DDNS au niveau du serveur DHCP n'est pas abordée ici mais dans le dossier sur le serveur DHCP.

4. Lancement et test

Notre serveur DNS étant correctement configuré, nous allons maintenant nous assurer qu'il se lance au démarrage du serveur Linux. Pour cela, on utilise la commande **chkconfig**.

```
#chkconfig --level 345 named on
#chkconfig --list |grep named
named       0:arrêt  1:arrêt  2:arrêt   3:marche   4:marche   5:marche   6:arrêt
```

On peut maintenant démarrer le service named avec la commande **service**:

```
[root@localhost /]# service named start
Démarrage de named :                        [  OK  ]
```

Et tester le fonctionnement depuis un poste client sur le réseau avec la commande **ping**:

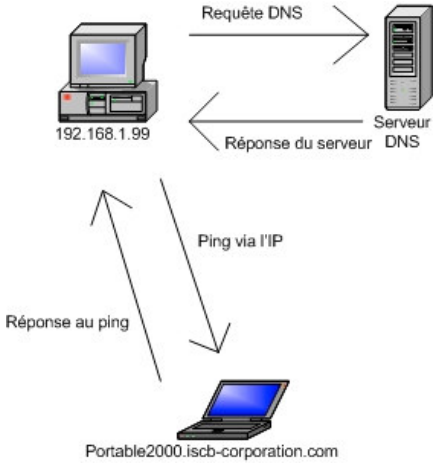
Envoi d'une requête 'ping' sur srvlinux.iscb-corporation.com [192.168.1.1] avec 32 octets de données:
Réponse de 192.168.1.1: octets=32 temps<10 ms TTL=128
Réponse de 192.168.1.1: octets=32 temps<10 ms TTL=128
etc…

Notre serveur DNS est opérationnel.

5. Analyse de requêtes DNS

Voici ce qui se passe sur le réseau lorsque l'on ping un poste en utilisant son nom FQDN.

1	0.000000	192.168.1.99	192.168.1.1	DNS	Standard query A portable2000.iscb-corporation.com
2	0.001038	192.168.1.1	192.168.1.99	DNS	Standard query response A 192.168.1.5
3	0.017202	192.168.1.99	192.168.1.5	ICMP	Echo (ping) request
4	0.017774	192.168.1.5	192.168.1.99	ICMP	Echo (ping) reply
5	1.017737	192.168.1.99	192.168.1.5	ICMP	Echo (ping) request
6	1.018017	192.168.1.5	192.168.1.99	ICMP	Echo (ping) reply



Tout d'abord une requête est envoyée au serveur DNS par le poste qui ping afin de savoir à quelle adresse IP correspond le nom FQDN que l'on ping. Le serveur renvoie sa réponse. L'échange de paquet a lieu via le protocole UDP. Le poste connais désormais l'adresse IP de portable2000.iscb-corporation.com, il n'a plus qu'à le pinger en utilisant le protocole ICMP.

6. Conclusion

La résolution des noms complètement qualifiés est fonctionnelle. Les deux modes de fonctionnement (statique et dynamique) assurent la souplesse de fonctionnement du serveur.

Si l'infrastructure réseau devient importante, le déploiement d'un serveur DNS de cache peut être intéressant, ce dernier se mettant à jour à partir du serveur maître sans pouvoir interagir sur ce dernier.