

Serveurs de noms

Durant cette séance, vous ferez :

1. l'installation, la configuration et le test d'un serveur DNS primaire, et la configuration d'un client,
2. la mise en route d'un serveur secondaire,
3. la définition d'une sous-zone.

Vous utiliserez pour cela un réseau de trois machines virtuelles Unix (distribution Debian). L'une des machines (**serveur1**) jouera le rôle de serveur primaire pour la zone **localdomain**, l'autre (**serveur2**) sera serveur secondaire de cette zone, et la troisième (**client**) sera un simple client (poste de travail).

Dans un second temps, vous configurerez **serveur2** comme serveur primaire pour la sous-zone **appareils.localdomain**.

1 Mise en place des machines

1.1 Création des machines, lancement

Créez les 3 machines virtuelles avec la distribution *Debian* : `uml create debian client serveur1 serveur2` Lancez les en réseau (connectées au même commutateur) : `run client serveur1 serveur2`

1.2 Installation des logiciels

Les commandes exécutées lors de ce TP sont réalisables uniquement par l'administrateur des machines (login : root, passwd : none).

Installez les logiciels nécessaires :

- `apt-get install tcpdump` sur le client,
- `apt-get install tcpdump bind9` sur les serveurs.

L'éditeur de texte `jed` est préinstallé.

1.3 Configuration réseau

Vous donnerez une adresse IP prédéfinie (voir le tableau ci-contre) aux interfaces `eth0` des 3 machines. Pour configurer une interface réseau, il faut ajouter au fichier `/etc/network/interfaces` la configuration de l'interface, par exemple :

machine	adresse IP
client	10.1.5.100
serveur1	10.1.5.1
serveur2	10.1.5.2

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 10.1.5.1
    netmask 255.255.255.0
```

Important : Conservez la déclaration de l'interface `lo` qui est indispensable. Elle porte l'adresse de *loopback* `127.0.0.1` qui sert à la communication entre programmes.

La commande `ifup eth0` démarre l'interface réseau (`ifdown` pour arrêter).

Le nom de la machine (par exemple `client`) peut être mis dans `/etc/hostname`, et sera pris en compte au prochain démarrage. On peut aussi associer le nom de la machine à l'adresse `127.0.0.1` dans `/etc/hosts` (sans enlever `localhost`).

1.4 Redémarrage et vérifications

- Arrêtez les 3 machines proprement (commande `halt`), et relancez ensuite le réseau virtuel :
`uml run client serveur1 serveur2`
- Vérifiez que les interfaces réseau sont bien actives via la commande : `ifconfig` et qu'elles communiquent bien entre elles, avec la commande : `ping adresse-ip -c1`.
- Observez (avec `tcpdump`) les paquets échangés pendant un `ping`.

2 Résolution locale par /etc/hosts

Les applications qui tournent sur les machines ont souvent besoin de *résoudre des noms*, c'est-à-dire déterminer le numéro IP qui correspond à une adresse comme `www.iut.u-bordeaux1.fr`. Elles appellent pour cela le *resolver* qui fait partie de la bibliothèque C.

1. Ce module obtient ses informations de plusieurs sources (fichiers locaux, appel à des serveurs, base de données etc.), selon le paramétrage indiqué dans `/etc/nsswitch.conf` à la ligne de clef `hosts`.
2. Le fichier local qui concerne la résolution est `/etc/hosts`. Modifiez celui de `client` pour qu'il "connaisse" `serveur1`. Testez votre modification avec la commande : `ping serveur1 -c1`.
3. Quel est le résultat de la commande `ping serveur2 -c1` ? Expliquez.

3 Configurer serveur1 en serveur DNS

En cas de problème, voir la fin du fichier `/var/log/syslog` via la commande : `tail /var/sys/log`.

1. Sur `serveur1`, vérifiez que le serveur DNS tourne à l'aide de la commande : `nslookup localhost`. (avec un point après `localhost`).
2. Lisez le fichier `/etc/bind/named.conf`

3.1 Configuration du client

Sur client :

1. Constatez d'abord que la commande :`"nslookup localhost."` échoue.
2. Dans `/etc/resolv.conf`, ajoutez `"nameserver 10.1.5.1"`. Vous avez ainsi configuré le poste de travail pour qu'il utilise le serveur de nom de `10.1.5.1`.
3. Réessayez la commande : `"nslookup localhost."`.

Sur serveur1 :

1. Observez (`tcpdump`) les trames qui circulent lors d'une interrogation par le client. Combien de trames sont échangées ? Quels sont les protocoles et les ports utilisés ?
2. Sur le serveur, quel fichier de configuration du DNS (dans `/etc/bind`) décrit `"localhost."` ?

3.2 Déclaration d'une zone

Sur serveur1, on va maintenant ajouter une zone `"localdomain"`.

1. Copiez le fichier `db.empty` dans `db.localdomain`
2. Modifiez le fichier `db.localdomain` comme suit pour déclarer `dns1` comme serveur de nom primaire (`dns1.localdomain.`) avec l'adresse email de l'administrateur :
`root.dns1.localdomain.`

```
@      IN      SOA    dns1.localdomain.  root.dns1.localdomain. (
                                ...
                                ...)
```
3. Ajoutez les déclarations de `dns1 (10.1.5.1)` `dns2 (10.1.5.2)` et poste (`10.1.5.100`).
4. Déclarez `dns2` comme serveur de noms de la zone.
5. Dans `named.conf`, inspirez-vous de `"localhost"` pour déclarer `"localdomain"`.
6. Relancez le serveur de noms (commande `/etc/init.d/bind9 restart`), et vérifiez que les noms définis (`dns1.localdomain`, `poste.localdomain`, etc.) sont bien résolus.
7. Définissez un synonyme `"www.localdomain."` pour `"dns1.localdomain."`. N'oubliez pas d'incrémenter le numéro de série à chaque modification. Relancez et vérifiez.

3.3 Résolution inverse

1. Mettez en place la résolution inverse du sous-réseau `10.1.5.0/24` (nom `5.1.10.in-addr.arpa`).
2. Testez via la commande `nslookup -type=ptr 10.1.5.1`

4 Configurer serveur2 en serveur secondaire

La machine `serveur2` (alias `dns2.localdomain`) va jouer le rôle de serveur secondaire pour la zone `localdomain` et la zone inverse `1.1.10.in-addr.arpa`

1. Vérifiez que `bind9` est installé sur `serveur2`
2. Sur le serveur primaire, déclarez le serveur `dns2.localdomain` dans la liste des serveurs susceptibles de renseigner sur `localdomain` (ajoutez une ligne `IN NS` dans `db.localdomain`).
3. Sur le serveur secondaire, déclarez les zones dont il est esclave, en précisant l'emplacement du fichier de stockage. Format des déclarations :

```
zone "le-nom-de-la-zone" {  
    type slave;  
    file "le-fichier-de-stockage";  
    masters { ip-serveur-maitre ; };  
}
```

Le fichier de stockage est créé et modifié par l'utilisateur `bind` du groupe `bind` qui n'a pas le droit d'écriture sur `/etc/bind`. Utilisez le répertoire `/var/run/bind/run`.

4. Relancez les deux serveurs.
5. Vérifiez que le poste de travail peut les consulter les deux serveurs via la commande suivante :

```
nslookup [ requête [adresse-IP-serveur-DNS] ]
```
6. Configurez le poste de travail pour qu'il utilise les deux serveurs de nom.
7. Sur `serveur1` arrêtez le service DNS (`/etc/init.d/bind9 stop`) vérifiez que le poste de travail peut encore résoudre les adresses. Notez le délai.

5 Délégation d'un sous-domaine

1. Sur le serveur primaire de la zone `localdomain`, pour déclarez un sous-domaine `appareils.localdomain` dont le serveur primaire est `dns2`.
Il suffit d'ajouter dans `db.localdomain`, la ligne : `appareils IN NS dns2`
2. Définissez cette zone sur `dns2`, avec quelques entrées pour télé, magnétoscope, console de jeux...
3. Testez, via les commandes de type `nslookup concole.appareils.localdomain 10.1.5.1`
4. Et pour finir, faites tourner un serveur secondaire de cette zone sur `dns1`.

6 Sur Internet

Sur votre poste de travail (qui est vraiment relié au réseau Internet) :

1. Comparez les résultats des commandes `nslookup`, `host` et `dig`. Aidez vous des manuels.
2. Trouvez l'adresse de "dagobah" et de "dagobah."
3. Trouvez l'adresse IP du serveur "www.lemonde.fr". Qu'observez vous? Expliquez.
4. Trouvez le nom et l'adresse IP du serveur de mails (MX) pour le domaine "laposte.net".
5. Quelle est l'adresse IP du serveur de nom de `iut.u-bordeaux1.fr`? Quels sont ses serveurs de mails?
6. De quoi parle la RFC citée dans `named.conf.local`? (faire recherche sur Internet).