Travaux Pratiques

RSX102 – DNS - 3 heures

SOMMAIRE :

1. Objectifs

A l'issue de cette séance de travaux pratiques, les auditeurs seront capables de :

- Citer les fichiers de configuration d'un serveur de noms : Bind
- Configurer un fichier de zone
- Tester votre installation DNS

L'outil utilisé pour les TP sera le logiciel VMWare Workstation.

2. Rappels

2.1. Pré-requis :

Pour réaliser ce TP, il est nécessaire de :

- Savoir ce qu'est le système DNS : Consultez Définition wikipedia ou http://www.afnic.fr/ext/dns/index.html

  « Le fonctionnement du DNS requiert l'existence d'un certain nombre de fichiers au niveau de chaque serveur autoritaire. Il faut notamment :

  un fichier de configuration du serveur (named.conf ou autres) ;
  un fichier des serveurs racines (named.root, db.root ou autres) ;
  un fichier par zone pour toutes les zones pour lesquelles le serveur est autoritaire. »

- Avoir certaines bases de l'utilisation d'un système Linux
- Avoir quelques bases TCP/IP
- Avoir votre gestionnaire de paquet configuré et à jour. (site de ubuntu-fr.org :http://doc.ubuntu-fr.org/gestionnaire_de_paquets)

2.2. Présentation de BIND

Bind fournit un service de résolution de nom. C'est le serveur DNS le plus utilisé sur INTERNET.

Il utilise comme fichiers de configuration :

/etc/bind/: le répertoire où sont stockés les fichiers de configuration du service Bind : **named.conf, named.conf.local, named.conf.option**

/var/lib/bind/ ou /etc/bind/: le répertoire de travail de Bind où sont stockés les **fichiers de zones et de zones inverses**.

Consultez : http://doc.ubuntu-fr.org/bind9 pour plus d'informations sur le sujet.

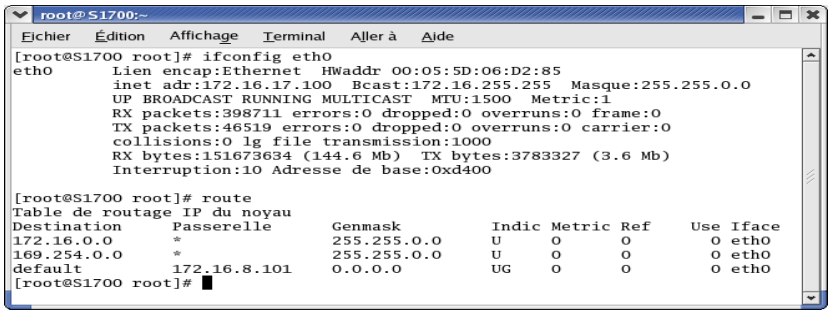
3. TP Installation de BIND9 sous UBUNTU 11

3.1. Pré-requis : contexte du TP

- Copiez la machine Ubuntu-11-04-vsftpd sur votre disque,
- Lancez VMwareWorkstation,
- Ouvrez et démarrez Ubuntu-11-04-vsftpd,
- Connectez-vous avec le compte olivier (mp olivier),
- Lancez le terminal,
- Tapez su (mp :rootpw).

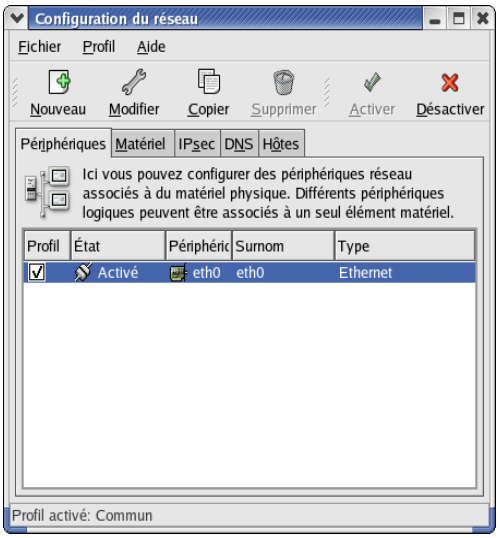
3.2. Vérification de la connexion Réseau

- Vérifier la configuration réseau de votre poste Linux à l'aide de la commande : **ifconfig eth0**
- Vérifier également la configuration de la passerelle :
  commande **: route**



- faire un ping de la passerelle

Si la configuration Réseau n'est pas correcte, vérifier la connectique et modifiez les paramètres à l'aide de l'outil graphique : menu système/Administration/outils réseau.

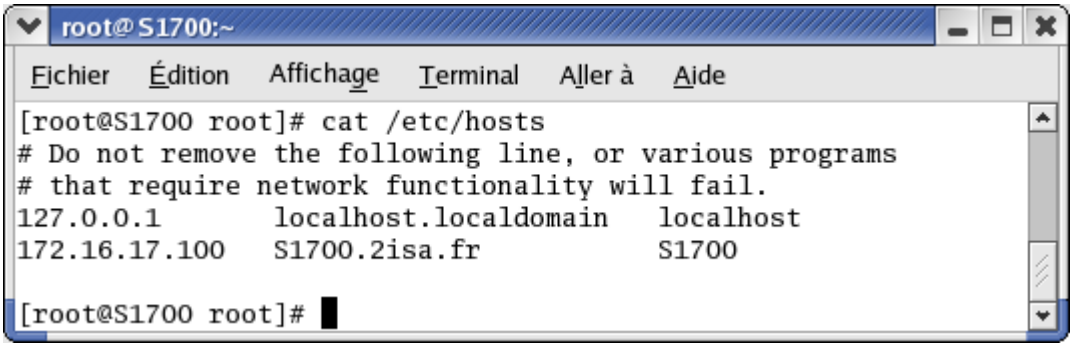


3.3. Vérification du fichier /etc/hosts et du nom du serveur

- Saisissez la commande : **hostname**
  Elle doit afficher le nom de votre machine suivi du nom de votre domaine, exemple :
  # hostname
  M1520
- Ouvrez le fichier /etc/hostname et configurez le nom de l'hôte suivi du nom de domaine
  Pour les besoins de ce TP, on choisira un nom de domaine du style : aislxxxx.local

- Validez et vérifiez à nouveau à l'aide de la commande **hostname**.

- Afficher le contenu du fichier de résolution de nom locale :
  cat /etc/hosts
  Que fait le fichier /etc/hosts ? .....



- Il est fortement recommandé que la syntaxe de votre fichier hosts ressemble à ce qui est affiché ci-dessus, c'est à dire :
  - à l'adresse de boucle locale doit correspondre le nom « localhost »
  - à l'adresse IP doit correspondre le nom de votre machine
  - dans les deux cas, le nom complet (machine.domaine) de la machine doit apparaître avant le nom simple (machine)
- le nom du domaine figurant dans ce fichier doit correspondre au domaine que vous avez choisi de bientôt mettre en œuvre depuis votre serveur DNS.

3.4. Installation

- Le service est-il en cours de fonctionnement ?
  Commandes : #ps –ale | grep named ou
  #/etc/init.d/bind9 status

Sinon, installez le paquet bind sur le serveur :

```
#sudo apt-get install bind9
```

Vous vérifierez ensuite le démarrage du service :

- Le service est-il en cours de fonctionnement ?
  Commandes : #ps –ale | grep named ou
  #/etc/init.d/bind9 status

- Si non procéder à son lancement :
  #/etc/init.d/bind9 start

4. TP Configuration de BIND

4.1. Configuration du serveur

Fichier de configuration général du serveur de nom bind : /etc/bind/named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include « /etc/bind/named.conf.options »;

// prime the server with knowledge of the root servers
zone « . » {
    type hint;
    file « /etc/bind/db.root »;
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone « localhost » {
    type master;
    file « /etc/bind/db.local »;
};

zone « 127.in-addr.arpa » {
    type master;
    file « /etc/bind/db.127″;
};

zone « 0.in-addr.arpa » {
    type master;
    file « /etc/bind/db.0″;
};

zone « 255.in-addr.arpa » {
    type master;
    file « /etc/bind/db.255″;
};

// zone « com » { type delegation-only; };
// zone « net » { type delegation-only; };

// From the release notes:
// Because many of our users are uncomfortable receiving undelegated answers
// from root or top level domains, other than a few for whom that behaviour
// has been trusted and expected for quite some length of time, we have now
// introduced the « root-delegations-only » feature which applies delegation-only
// logic to all top level domains, and to the root domain. An exception list
// should be specified, including « MUSEUM » and « DE », and any other top level
// domains from whom undelegated responses are expected and trusted.
// root-delegation-only exclude { « DE »; « MUSEUM »; };
```

```
include « /etc/bind/named.conf.local »;
```

Votre fichier peut-être plus succinct que celui-ci. Il est alors constitué de plusieurs « include » de fichiers.

Ici, la dernière ligne indique l'inclusion du fichier : **/etc/bind/named.conf.local**, c'est dans ce fichier que nous allons rajouter les informations de la zone (du domaine) que nous souhaitons configurer.

Le fichier **/etc/bind/named.conf.options** peut être comme suit :

```
options {
   directory « /var/cache/bind »;
   // If there is a firewall between you and nameservers you want
   // to talk to, you might need to uncomment the query-source
   // directive below. Previous versions of BIND always asked
   // questions using port 53, but BIND 8.1 and later use an unprivileged
   // port by default.

   //query-source address * port 53;

   // If your ISP provided one or more IP addresses for stable
   // nameservers, you probably want to use them as forwarders.
   // Uncomment the following block, and insert the addresses replacing
   // the all-0's placeholder.

   forwarders {
      172.16.8.99;
   };

auth-nxdomain no; # conform to RFC1035

};
```

Tout ce passe au niveau de forwarders {, : ainsi, si le serveur que nous sommes en train de configurer n'arrive pas à résoudre une adresse donnée, il envoie la requête au serveur dont l'adresse IP est précisée.

Pour chaque domaine, il est nécessaire de configurer deux zones, la zone principale, et la zone de recherche inversée :

- La zone principale permet de faire pointer un nom de domaine pleinement qualifié (FQDN = Full Qualified Domain Name) sur une adresse IP, pour information un nom de domaine pleinement qualifié est de la forme : hote.domaine.extension.
- la zone de recherche inversée, permet de faire, comme son nom l'indique, l'inverse, c'est-à-dire de faire pointer une adresse IP sur un FQDN.

4.1.1. Création de la zone principale

Dans le fichier **/etc/bind/named.conf.local** nous allons rajouter les informations suivantes, où vous remplacerez *mondomaine* par le nom du domaine que vous souhaitez créer (ex : aislxxxx) :

```
//
// Do any local configuration here
//
zone «mondomaine.local» {
        type master;
        file «/var/lib/bind/mondomaine.local.hosts»;
        allow-update { none; };
};
```

Ces informations vont créer le domaine : *mondomaine*.local, la zone est de type master (c'est-à-dire maitre), le fichier qui contiendra les détails des machines de *mon domaine* est **/var/lib/bind/mondomaine.local.hosts**, et les mises à jour ne seront pas autorisées.

4.1.2. Création de la zone de recherche inversée

Toujours dans le fichier **/etc/bind/named.conf.local** nous allons rajouter les informations suivantes :

```
zone «16.172.in-addr.arpa» {
        type master;
        file «/var/lib/bind/16.172.in-addr.arpa.zone»;
        allow-update { none; };
};
```

Il s'agit de l'adresse de votre réseau inversé, si les adresses ip de votre réseau sont de la forme, 172.16.X.X, la zone inverse sera : 16.172.in-addr.arpa,

Pour en savoir plus sur l'extension .arpa : http://fr.wikipedia.org/wiki/.arpa

4.1.3. Configuration de la zone principale

Dans la section principale, on a défini que le fichier **/var/lib/bind/mondomaine.local.hosts** contiendrait la définition des hôtes de notre réseau.

Il faut donc créer ce fichier, et le remplir.

```
$ttl 38400
@    IN   SOA    server.mondomaine.local. webmaster.mondomaine.local. (
     2011102401 ; serial
     21600 ; refresh after 6 hours
     3600 ; retry after 1 hour
     604800 ; expires after 1 week
      38400 ) ; minimum TTL of 1 day
@  IN   NS    server.mondomaine.local.
server   IN   A     172.16.15.120
www    IN    A     172.16.15.121
```

Un fichier de zone DOIT toujours commencer par la définition d'un SOA (Start Of Authority) :

Le « @ » spécifie la zone définie dans le fichier configuration

Ensuite « IN » précise qu'il s'agit d'une zone Internet, il s'agit « presque » de la valeur par défaut (les cas où vous aurez a préciser un autre type de zone sont très rares).

Le mot clé SOA suivi du FQDN du serveur qui héberge la zone (server.mondomaine.local.), puis, sur la même ligne une adresse email de contact (webmaster.mondomaine.local.)

Dans ce dernier cas, le premier « . » est considéré comme un « @ » (il s'agit d'une convention), vous auriez pu mettre aussi : monnom.fai.fr

Attention : Les « . » à la fin de server.mondomaine.local**.** et webmaster.mondomaine.local**.** sont obligatoires !

Ensuite il faut définir les éléments suivant :

- Le numéro de série (serial), généralement la date du jour suivi d'un incrément : YYYYMMDDxx.
- Le temps de rafraichissement (refresh), ici 6 heures.
- Le temps entre deux essais (retry), ici 1 heures.
- Le temps d'expiration (expire) ici 1 semaine.
- La valeur TTL minimum (minimum TTL), ici, 38400 secondes.

Toutes les valeurs de temps sont précisées en secondes

Tout de suite après l'enregistrement SOA, il faut préciser le serveur DNS à consulter :

```
@ IN NS server.mondomaine.local.
```

Cela signifie : la machine server.mondomaine.local est un serveur de nom (NS = Name server) pour la zone.

Ensuite nous avons la définition des machines de notre réseau :

```
server IN A 172.16.15.120
www IN A 172.16.15.121
```

Chaque ligne Précise : le nom du pc – le type de zone – le type d'enregistrement – l'adresse IP de la machine

Le type d'enregistrement A (A pour Alias) permet donc de pointer, par exemple, server sur l'adresse ip 172.16.15.120).

4.1.4. Configuration de la zone de recherche inversée

```
@    IN    SOA    server.mondomaine.local. webmaster.mondomaine.local. (
          2007051401 ; serial
          21600 ; refresh after 6 hours
          3600 ; retry after 1 hour
          604800 ; expires after 1 week
```

```
        86400 ) ; minimum TTL of 1 day
@    IN    NS    server.mondomaine.local
120.15    IN    PTR server.mondomaine.local.
121.15    IN    PTR www.mondomaine.local.
```

Le début du fichier est le même que le précedent

Les lignes d'enregistrements de machine sont un peu différentes, en effet, vous remarquerez que toutes les lignes commencent par un nombre, en fait ce nombre est la fin de l'adresse ip de la machine …
Le type d'enregistrement est PTR.

Votre serveur DNS est configuré.

5. TP Vérification de l'installation

5.1. Test de la configuration

5.1.1. Les outils

Losrque vous avez installé le paquet bind sur votre distribution préférée, certains outils ont été ajoutés :

- named-checkconf : Permet de tester si vos fichiers de configurations sont correctement écrits
- named-checkzone : permet de tester une zone, syntaxe :

```
#sudo named-checkzone mondomaine.local /etc/bind/mondomaine.local.hosts
```

- nslookup : permet d'interroger un serveur de nom.
- dig : permet aussi d'interroger un serveur de nom.

Si les tests de configuration sont correctement passés, redémarrez votre serveur :

```
#sudo /etc/init.d/bind9 restart
```

5.1.2. Interrogation du serveur avec nslookup

```
nrb@M1530:~$ nslookup
> server 172.16.15.120
Default server: 172.16.15.120
Address: 172.16.15.120#53
> M1520.aislxxxx.local
Server: 172.16.15.120
Address: 172.16.15.120#53

Name:M1520.aislxxxx.local
Address: 172.16.15.120
```

Testons la zone de recherche inverse :

```
nrb@M1530:~$ nslookup
```

```
> server 172.16.15.120
Default server: 172.16.15.120
Address: 172.16.15.120#53
> 172.16.15.121
Server: 172.16.15.120
Address: 172.16.15.120#53

121.15.16.172.in-addr.arpa name = www.aislxxxx.local
```

Tout fonctionne.

5.1.1. Interrogation du serveur avec dig

```
nrb@M1530:~$dig
```

5.2. Utilisation des CNAME

Nous allons voir un autre type d'enregistrement : le type : CNAME (pour Canonical Name).

Ce type d'enregistrement permet de faire pointer un nom différent sur une machine précise et sans passer par l'adresse ip …

Le meilleur exemple pour ce type d'enregistrement est le nom d'hôte : www
On va dire par exemple que votre serveur contient aussi un serveur web, alors dans ce cas ce serait bien d'avoir www.mondomaine.local qui pointe sur votre serveur.

Reprenons le fichier de zone principal :

```
@    IN    SOA    server.mondomaine.local. webmaster.mondomaine.local. (
          2007051401 ; serial
          21600 ; refresh after 6 hours
          3600 ; retry after 1 hour
          604800 ; expires after 1 week
          86400 ) ; minimum TTL of 1 day
@    IN    NS    server.mondomaine.local.
server    IN    A    172.16.15.120
www    IN    CNAME    server
```

Testez à l'aide d'un ping.

6. TP : Configuration des clients

6.1. Tests à partir d'un client Linux autre que le serveur.

- Procéder à des tests avec votre binôme en déclarant son poste Linux en tant que client DNS de votre serveur.

Aide : vous devez correctement configurer les fichiers : /etc/resolv.conf et /etc/nsswitch.conf

Editez le fichier **/etc/resolv.conf**, puis renseignez le comme suit :

```
domain mondomaine.local
nameserver 172.16.15.120
```

- Reprendre les tests du paragraphe 5 avec ce nouveau client.

6.2. Tests à partir d'un client Microsoft sur le réseau

- Configurer un poste sous Windows comme client de votre serveur DNS.
  Pour les besoins du TP, ne configurer qu'un seul serveur DNS (retirer les serveurs habituels de 2isa et remplacez les par le vôtre)

- Reprendre les tests comme dans le cas d'un client Linux à l'aide de l'utilitaire nslookup

7. TP : Suivi de l'activité de named et des journaux de log

- Ouvrir un terminal de commandes: positionnez cette console dans la partie haute de votre écran, en permanence. Vous allez vous en servir pour suivre l'activité de votre service DNS.
  Saisir la commande : tail -f /var/log/syslog
  (commande d'affichage en continu des messages journaux)

- Dans une 2ème console arrêter le service named :
  #/etc/init.d/named stop
  ou #service named stop
  Observer les messages dans la 1ère console de log

- Relancer le service named :
  #/etc/init.d/named start
  ou #service named start

  Observer les messages dans la 1ère console de log.
  Y-a-t-il des messages d'erreurs ?
  Si non OK : cette procédure de suivi d'activité sera utilisée par la suite lors de la configuration du service.
  Si oui essayer de diagnostiquer le problème puis faites appel à votre formateur.

8. TP : Dépannage et diagnostics sur le service DNS

- Depuis un poste XP client de votre serveur DNS, faites un ping d'un site Web bien connu :
  exemple : ping www.google.fr
  Notez l'adresse IP du site

- Dans une console, consultez puis videz le cache DNS :
  ipconfig /displaydns

ipconfig /flushdns
ipconfig /displaydns (le cache DNS doit être vide)

- sur votre serveur Linux, arrêter le service bind.

- refaites un ping du même site. Que se passe-t-il ?
  Pouvez-vous joindre ce serveur en utilisant son adresse IP ?
  Expliquez pourquoi ces deux réponses semblent se contredire ?

- Redémarrer le service bind, refaites le ping et consulter le cache DNS

- A VOUS :
  - créez une nouvelle zone principale « aisl.fr ».
    Vous allez y créer les enregistrements :
    smtp correspond à 172.16.15.120
  - sauvegarder, appliquer les changements et tester.

9. Compléments TP DIG

Taper la commande :

```
$ dig eof.eu.org
```

En interprétant les résultats obtenus par la commande **`dig`**, répondre à ces 3 questions :

- Qui est en charge de servir la zone `eof.eu.org` ?
- Se mettre à la place du serveur DNS, et indiquer les requêtes DNS effectuées pour résoudre `eof.eu.org` en utilisant **`dig`**.
- Parmi les serveurs DNS trouvés précédemment, indiquer s'ils gèrent l'IP v6.

10. Bibliographie

http://www.afnic.fr/ext/dns/index.html
Cours cisco CCNA Discovery
http://www.mines.inpl-nancy.fr/~tisseran/cours/reseaux/
http://www.mimiz.fr/linux/installation-et-configuration-dun-serveur-dns-bind9-sur-ubuntu/
Travaux stagiaires 2ISA.
TP DNS rédigé par Olivier Delattre
http://ferry.eof.eu.org/lesjournaux/ll/public_html/ch09s02.html