TP N°4 - Installation d'un serveur DNS

Un serveur DNS est un serveur qui transforme l'adresse de type http://www.linux.fr en adresse IP valide sur internet. Lorsque vous souhaitez naviguer sur Internet, vous devez obligatoirement avoir configuré le DNS de votre machine, sinon il vous sera impossible d'atteindre le moindre site web, à moins de connaître son adresse IP, ce qui est assez difficile à retenir.

1. Objectif

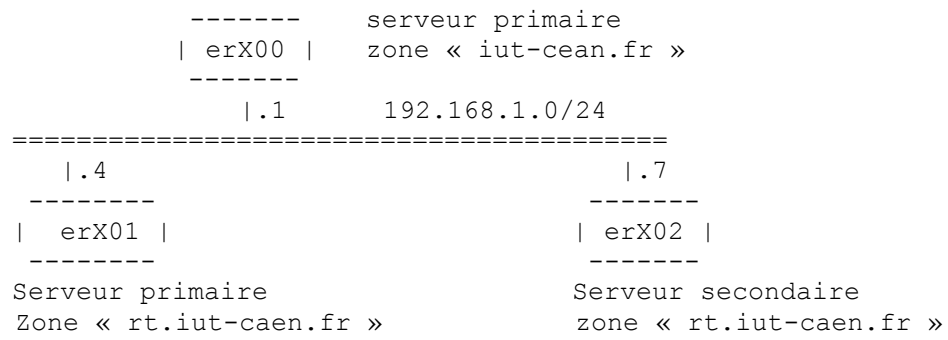
La raison pour laquelle on peut avoir besoin d'un serveur DNS dans un établissement universitaire peut être double :

- La première, disposer d'un serveur cache DNS, afin d'accélérer les requêtes ;
- La seconde, qui n'est pas incompatible avec la première, est de simplifier l'adressage des machines internes à l'établissement.

Ainsi, je veux que les étudiants ne soient pas obligés de taper l'adresse IP de la machine web (intranet), mais puissent y arriver avec www.rt.iut-caen.fr, il faut alors que ce serveur puisse "forwarder" les requêtes vers un serveur DNS officiel.

Il est clair qu'ici **rt.iut-caen.fr** est un sous domaine complètement inventé, il n'a pas de valeur légale sur internet. Ainsi je vous conseille vivement de ne pas utiliser un domaine existant. Un domaine n'existe au sens légal que s'il a été déposé officiellement auprès d'un organisme autorisé. Cela serait la troisième possibilité de configuration d'un serveur DNS, vouloir installer un serveur public (officiel).

Donc pour revenir à ce que nous souhaitons faire, nous allons créer un domaine rien que pour nous, **iut-caen.fr,** puis un sous domaine propre au département RT, **rt.iut-caen.fr**.
Nous souhaitons d'abord configurer un **serveur maître** pour la zone **iut-caen.fr**. Puis déléguer la zone **rt.iut-caen.fr** au poste qui doit devenir maître de ce sous domaine (cf. schéma ci-dessous).



2. Installer le serveur BIND

Chaque groupe disposera de trois machines erX00, erX01 et erX02 (*X étant le numéro du groupe*). Pour la suite du TP, erX00 et erX01 désigneront : *serveur primaire* (NS), serveur web. La machine erX02 sera **cliente** de erX00 (resp. erX01), pour le domaine `iut-caen.fr (resp. rt.iut-caen.fr).`

Voici les noms qui seront assignés :

- Serveur de noms primaire pour la zone `iut-cean.fr` : **ns1**
- Serveur de noms primaire pour la zone rt.`iut-cean.fr` : **ns2**
- Serveur de noms secondaires pour la zone rt.`iut-cean.fr` : **ns3**
- Serveurs web (**www)** comme alias de nom d'hôte.

L'installation de BIND étant déjà faite sur tous les postes.

Mise en garde: l'ensemble des fichiers de configutaion se trouvent cloisonés dans le répertoire **chroot**. Vous devez avoir en particulier les fichiers ci-dessous. les noms et l'emplacement des fichiers peuvent différer d'une distribution à une autre. Pensez à utiliser la commande "Find" en cas de besoin (voir man find).

/var/named/chroot/etc/named.conf	Contient les paramètres généraux de configuration du serveur et fait appel au fichier **named.rfc912.zones** (commande include)
/var/named/chroot/etc/named.rfc912.zones	C'est le fichier de configuration des zones du serveur
/var/named/chroot//var/named/named.ca	Fichier de configuration de la zone racine '.' contenant les 13 serveurs DNS racines.
/var/named/chroot//var/named/named.local	Fichier de configuration de la résolution inverse des adresses loopback

Tout au long de ce TP, étape par étape, vous allez créer les fichiers de zones suivants:

/var/named/chroot/var/named/iut.zone	*fichier de configuration de la zone* iut-cean.fr, *qui fait correspondre les noms/adresses de toutes les machines de cette zone* (cf. sections 3 & 5.2).
/var/named/chroot//var/named/rt.iut-caen.fr.zone	*fichier de configuration de la zone* rt.iut-cean.fr, *qui fait correspondre les noms/adresses de toutes les machines de cette zone* (cf. sections 3 & 5.2).
/var/named/chroot/var/named/iut.rev	*fichier de configuration de la zone inverse* 1.168.192.in-addr.arpa, *qui fait correspondre une adresse IP avec le nom de machine* (cf. section 3).
/var/named/chroot/var/named/localhost.zone	*ficher de configuration pour la zone locale* (localhost: 127.0.0.1)
/var/named/chroot/etc/resolv.conf	*ficher de configuration pour le client DNS. Il indique le serveurs DNS à contacter pour la résoltion de noms* (cf. section 5.1)

3. Configurer un serveur primaire

Il faut pour cela configurer les différents fichiers que nous venons de voir. On cherche à configurer un serveur de noms primaire pour le domaine **iut-cean.fr** et **rt.iut-cean.fr**. Pour la configuration, vous utiliserez les informations de l'annexe. N'hésitez pas à soliciter votre enseignant en cas de besoin.

- Sur la machine erX00 :
  a) Configurez le fichier /chroot/etc/named.rfc912.zones de votre DNS
  b) Configurez les fichiers de configuration pour les zone iut-caen.fr, 1.168.192.in-addr.arpa et rt.iut-caen.fr

Remarques importantes :

- Pour vérifier la syntaxe de named.rfc912.zones de votre DNS, utilisez **named-checkconf**
- La configuration d'une zone n'a rien de sorcier mais les erreurs sont fréquentes. Pour vérifier la validité de la zone, utilisez **named-checkzone iut-caen.fr /chroot/etc/named/iut.zone**
- Pour consulter les éventuels messages d'erreurs, pensez à visualiser les logs avec la commande : **tail /var/log/syslog | grep named** et/ou **tail /var/log/daemon.log | grep named**
- Pensez à lancer wireshark pour visualiser les messages échangés.

4. Tester son serveur primaire

Une fois les fichiers en place, votre serveur est configuré, il ne reste plus à lancer ce dernier, en utilisant le script **/etc/init.d/named start.** Avant de continuer vérifiez que le service est bien démarré « ***ps aux | grep named*** ».

5.1 Configurer le client - /etc/resolv.conf

Sur la machine erX02, un client DNS doit être configuré pour utiliser le service de résolution de noms des domaines **iut-caen.fr** et **rt.iut-cean.fr**. Modifiez le fichier */chroot/etc/resolv.conf*. Il suffit de renseigner les lignes suivantes :

search *nom-du-domaine*
nameserver *addr-ip (= adresse du serveur DNS faisant autorité sur le domaine)*

Ensuite, relancez le service réseau. Utilisez les commandes suivantes :

/etc/init.d/network stop
/etc/init.d/network start

a) Vérifiez que la résolution de noms fonctionne sur : www.iut-caen.fr, www.rt.iut-caen.fr.

Une machine locale n'est pas obligée d'utiliser le DNS pour résoudre un nom symbolique en adresse IP, on peut aussi utiliser le fichier **/etc/hosts**. Le choix de la méthode à utiliser se fait (pour Linux) dans le fichier **/etc/host.conf**, une ligne commençant par **order** permet de spécifier les méthodes utilisées et l'ordre dans lesquelles elles seront essayées. Exemple de fichier **/etc/host.conf**: **order bind, hosts**

5.2 Configurer la délégation de zone

On veut maintenant que le serveur maître de la zone **iut-caen.fr** délègue la gestion du domaine **rt.iut-cean.fr** à la machine erX01 qui doit maintenant devenir serveur maître pour ce sous domaine. Pour cela, il faut suivre les étatpes suivantes:

- Sur la machine erX00:
  1. configurer le fichier /var/named/chroot/etc/named.rfc912.zones de votre serveur DNS **ns1** comme *serveur esclave* pour le sous domaine **rt.iut-cean.fr** (cf. annexe)
  2. donner les droits d'écriture au serveur **ns2** sur le répértoire "slaves/rt.iut-caen.fr.bak"; rt.iut-caen.fr.bak étant le nom sous lequel sera transferé le fichier de la zone **rt.iut-cean.fr** du serveur **ns2** vers la machine erX00.
  3. Ajouter les lignes suivantes au fichier iut.zone:

```
iut-caen.fr        IN    NS    ns2.rt.iut-caen.fr. ;; indique que ns2
fait office de serveur DNS sur le domaine iut-caen.fr

rt                 IN    NS    ns2.rt.iut-caen.fr.
;; indique que ns2 fait office de serveur DNS (primaire) sur
;; le domaine rt.iut-caen.fr
```

  4. ne pas renseigner l'enregistremt ci-dessous dans le fichier de zone iut.zone:

```
ns2                IN    A     192.168.1.4
```

- Sur la machine erX01,
  1. configurer le fichier /var/named/chroot/etc/named.rfc912.zones de votre serveur DNS **ns2** comme *serveur maître* pour le domaine **rt.iut-cean.fr** et comme *serveur esclave* pour le domaine **iut-cean.fr** (cf. annexe)
  2. donner les droits d'écriture au serveur ns1 sur le répértoire"slaves/iut-caen.fr.bak"; iut-caen.fr.bak étant le nom sous lequel sera transferé le fichier de la zone **iut-cean.fr** du serveur **ns1** vers la machine erX01.
  3. Ajouter la ligne suivante au fichier rt.iut-caen.zone:

```
rt.iut-caen.fr     IN    NS    ns1.iut-caen.fr.
;; indique que ns1 fait office de serveur DNS sur le domaine rt.iut-
caen.fr
```

  4. renseigner l'enregistremt suivant dans le fichier de zone iut.zone:

```
ns1                IN    A     192.168.1.2
```

a) Réalisez la configuration des fichiers sur les machines erX00 et erX01.

b) Une fois les modifications nécessaires effectuées, redémarrez Bind9 sur sur **ns1** et sur **ns2** et attendez quelques instants. Verifiez que les fichiers "slaves/iut-caen.fr.bak" et "slaves/rt.iut-caen.fr.bak" ont été bien reçues.

c) Vérifiez (à partir de la machine erX02) que la résolution de noms fonctionne sur : www.iut-caen.fr, www.rt.iut-caen.fr. (Pensez à renseigner dans **resolv.conf** les différents serveurs avec la commande **nameserver)**

5.3. Serveur secondaire

Maintenant, nous souhaitons configurer un serveur DNS secondaire **ns3** sur erX02 pour le domaine rt.iut-caen.fr. Il suffit pour cela d'indiquer dans le fichier de configuration /var/named`/chroot/etc/named.rfc912.zones` de votre serveur DNS **ns3** qu'il sera *serveur esclave* pour la zone **`rt.iut-caen.fr`**. La machine ns3 doit disposer de deux fichiers de configuration pour BIND : /etc/named.conf et /var/named/named.local.

- Sur la machine erX02:
  1. configurer le fichier /var/named`/chroot/etc/named.rfc912.zones` de votre serveur DNS **ns3** comme *serveur esclave* pour le domaine **`rt.iut-cean.fr`** `(cf. annexe)`
  2. Activez le serveur secondaire. Une fois les modifications nécessaires effectuées, redémarrez Bind sur **ns2** et sur **ns3** et attendez quelques instants.

Pour tester le serveur secondaire, il faut tout d'abord arrêter le serveur primaire « */etc/init.d/named stop* » **ns2**. Ensuite, tester le fonctionnement du serveur secondaire **ns3** en utilisant des requêtes sur www.rt.iut-caen.fr ou www.rt.iut-caen.fr. C'est le serveur secondaire qui doit répondre, le serveur primaire étant inactif.

5.4 Résolution de noms sur un routeur

Il est possible de configurer un routeur pour la résolution de noms. Ci-dessous la commande IOS (en configuration globale) permettant de mettre en place le système de nommage :

- **ip domain-lookup** : indique à l'IOS d'interroger un serveur de noms (DNS) ;
- **ip name-server** *serv1 serv2* : configure les adresses ip des serveurs de noms ;
- **ip domain-name** : définit le nom de domaine implicite pour les noms incomplets.

Vérifiez que la résolution de noms fonctionne à travers un routeur, pour une machine du réseau.

6. Annexe

6.1 Le fichier named.conf

Le fichier `named.rfc912.zones` est le centre de configuration de BIND. Ce fichier permet de spécifier :

- Les domaines pour lesquels le serveur possède l'information originale : il est alors appelé serveur primaire du domaine.
- Les domaines pour lesquels le serveur est un serveur secondaire, il rapatrie régulièrement l'information à partir du serveur primaire et possède toujours une copie à jour.
- Les domaines pour lesquels le serveur fait juste office de cache

Son contenu :

```
zone "." IN {
      type hint;
      file "named.ca";
};

zone "iut-caen.fr" IN {
      type master;
      file "iut.zone";
      allow-update { none; };
};

zone "localhost" IN {
      type master;
      file "localhost.zone";
      allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
      type master;
      file "iut.rev";
      allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
      type master;
      file "named.local";
      allow-update { none; };
};
```

Voyons maintenant la signification des directives de ce fichier :

```
zone "iut-caen.fr" {
      type master;
      file "iut.zone";
};
```

Chaque bloc **zone** "*non-de-la-zone*" contient la description d'une zone. La zone "iut-caen.fr" contiendra la description du domaine **iut-caen.fr**, c'est à dire la liste des adresses IP des machines du domaine, mais aussi la liste des serveurs de noms, des serveurs de courrier et quelques autres informations. La directive **type master** signifie que notre serveur est maître pour cette zone, c'est à dire qu'il dispose de tous les renseignements utiles. Enfin, **file "iut.zone"** donne le nom du fichier contenant les données de la zone.

```
zone "1.168.192.in-addr.arpa" {
      type master;
      file "iut.rev";
      };
```

En général, quand on interroge un serveur DNS, on lui indique un nom de machine (par exemple **ns1.iut-caen.fr**) et le serveur renvoie son adresse IP (par exemple 192.168.1.1).

Parfois, il est utile de faire la résolution inverse. Dans ce cas, on résout l'adresse **<IP avec les octets inversés>.in-addr.arpa** ; par exemple, pour trouver le nom de 192.168.1.1, on résout **1.1.168.192. in-addr.arpa**. C'est ce à quoi sert cette zone.

```
zone "0.0.127.in-addr.arpa" {
      type master;
      file "named.local";
      };
```

Cette zone est similaire à la précédente ; en principe, elle ne devrait pas servir, dans la mesure où 127.0.0.1 se trouve en général dans le fichiers hosts de chaque machine.

6.2 Les fichiers de zone

Tous les fichiers de zone doivent se trouver dans **/chroot/var/named**. Voyons à présent un exemple de fichier de zone définissant le sous-domaine **ucla.edu :**

```
; exemple de fichier définissant le sous-domaine ucla.edu
@       IN      SOA     eagle.ucla.edu  root.eagle.ucla.edu. (
                                1 ; Numéro de série du fichier
                            86400 ; Période de mise à jour des secondaires
                             3600 ; En cas d'échec intervalle entre deux essais
                            86400 ; Temps maximum de validité
                            86400 ) ; TTL par défaut

@       IN      NS      eagle.ucla.edu.
fox     IN      A       131.23.6.121
                HINFO   PC Linux i486

lynx    IN      A       131.23.6.135
                HINFO   PC Linux i486
eagle   IN      A       131.23.6.123
                HINFO   Sun Sparc Server
```

Chaque domaine possède un certain nombre d'information stockées dans des enregistrements.
Un enregistrement est de la forme: **Domain_name Time_to_live Class Type Value**
Le symbole @ désigne la zone décrite par le fichier de configuration. Le mot clé **IN** signifie qu'il s'agit d'une zone Internet. Les principaux types sont :

- L'attribut **A**: l'adresse IP.
- L'attribut **CNAME**: synonyme (alias) pour une machine.
- L'attribut **HINFO**: information ASCII sur le type de CPU...
- L'attribut **NS**: le serveur de nom pour un sous-domaine.
- L'attribut **MX**: le serveur mail pour un domaine donné.
- L'attribut **SOA**: spécification des différents paramètres (email de l'administrateur, période de mise à jour, période de validité etc.).

6.3 Déléguation de zone

Pour ns1 et pour la zone rt.iut-caen.fr, le fichier de configuration du serveur primaire ns1 doit inclure les nouvelles directives (en gras) ci-dessous:

```
zone "iut-caen.fr" IN {
      type master;
      file "iut.zone";
      allow-update { none; };
      allow-transfer { 192.168.1.4; };
      notify no;
};
```

et la déclaration de la zone ci-dessous:

```
zone "rt.iut-caen.fr" IN {
      type slave;
      masters { 192.168.1.4; };
      file "slaves/rt.iut-caen.fr.bak";
};
```

- **allow-update** précise les clients autorisés à mettre à jour dynamiquement le fichier de zone. Par défaut, elle est définie à **none**, ce qui signifie que les mises à jour dynamiques sont interdites.

- **allow-transfert** déclare les serveurs autorisés à recevoir un transfert de zone (ns2 dans notre exemple)

- **notify** permet au serveur esclave de demander une mise à jour du fichier de zone

Le fichier de configutaion du serveur **ns2** doit contenir la déclaration des zones ci-dessous:

```
zone "rt.iut-caen.fr" IN {
      type master;
      file "rt.iut-caen.fr.zone";
      allow-update { none; };
      allow-transfer { 192.168.1.2; };
      notify yes;
};

zone "iut-caen.fr" IN {
      type slave;
      file "slaves/iut-caen.fr.bak";
      masters { 192.168.1.2; };
};
```

Pour aller plus loin…

Ce TP montre un exemple de configuration, mais il reste beaucoup de choses à savoir sur DNS. Par exemple, **(1) comment sécuriser un server de nom Bind9** avec les **Acess Control Lists**, ou encore **(2) comment définir des vues différentes des données de la zone aux différents clients** (Bind 9 uniqement) avec la commande **view**.