DNS (Domain Name Server) : Installation et Configuration

Ce TP consiste à installer, configurer et tester un serveur DNS sous Linux.

- Serveur open source : **bind9**
- Distribution : **CentOs 6 (sur machine virtuelle)**

Objectifs :

L'objectif de ce TP est d'illustrer le concept et la configuration du service de nommage (DNS : *Domain Name System*) qui a une importance capitale dans les réseaux, élément clef permettant de surfer sur le web, d'accéder à sa messagerie.
Dans ce TP, nous allons aborder :

- Les différents outils qui nous permettent d'interroger un serveur DNS,
- La manière dont les informations de la structure DNS sont conservées,
- La manière dont le serveur DNS sert des informations aux différents utilisateurs,
- Le fonctionnement de la résolution de noms proprement dite.

Pré-requis :

- Protocoles TCP-IP, DNS

Remarques préliminaires :

Vous effectuerez toutes les manipulations de configuration sur le serveur en tant que root (commande « `su -` » si vous avez ouvert la session sous un autre compte).

Les configurations se feront en mode ligne de commande.

Faites systématiquement une sauvegarde des fichiers initiaux avant de les modifier

```
cp fichier.conf fichier_old.conf
```

La modification d'un fichier de configuration d'un serveur impose de relancer ce service.

```
/etc/init.d/serviced start ou restart
/etc/init.d/serviced stop
/etc/init.d/serviced status
```

Les aides pour vos configurations…

- Document de cours associé
- Pensez à utiliser le `man` pour vous aider dans vos configurations

1. Introduction

Rappeler brièvement le fonctionnement du DNS.
Où se situe le serveur DNS dans votre architecture réseau, quelles sont les machines qui vont être déclarées dans ce DNS ?

Les outils d'interrogation du DNS :

- **`nslookup`** et **`host`** sont deux commandes qui nous permettent de faire la correspondance entre adresse IP et nom d'hôte et vice/versa.
- L'utilitaire `dig` est extrêmement pratique et présente les informations telles qu'elles sont configurées au niveau du serveur DNS.

Pour plus de détails, regarder les `manpage` de ces deux commandes.

2. Configuration du client (Resolver)

Dans un premier temps vous allez tester les configurations DNS de votre poste avant de configurer vos propres serveurs. Cette première partie a pour but de vous familiariser avec les différents éléments intervenant dans la configuration d'un serveur DNS.

- Fichier `hosts`

Quel est le rôle du fichier `/etc/hosts` ?
RQ : ce fichier est très important, de nombreuses configurations Linux s'appuyant sur la définition du Localhost.

- Fichier `host.conf`

Quel est le rôle du fichier `/etc/host.conf` ?

- Fichier `resolv.conf`

Expliquer le rôle de chaque ligne de ce fichier.
Attention ce fichier sera très important dans les différentes configurations que vous allez tester. Penser à le modifier en fonction des configurations testées !!!

3. Le serveur BIND

BIND est l'implantation la plus utilisée du service DNS sur des machines Linux. Dans cette partie du TP, nous allons voir comment configurer notre propre serveur DNS (**http://www.isc.org/bind/**, Bindv9.2/9.3 Reference Manual accessible sur ce site).

ATTENTION : La configuration du DNS est très sensible à la syntaxe. Utiliser au maximum des fichiers déjà existants dont vous pouvez faire une copie pour les modifier ensuite en fonction des configurations que vous aurez à mettre en place.

3.1. Pré-Configurations

3.1.1. Installation Bind

Faire un clone de votre machine virtuelle CentOs qui vous servira à la configuration de votre serveur (garder une machine virtuelle Centos6 avec les configurations de base)
Faire une copie du répertoire contenant votre machine virtuelle initialement créée
Renommer ensuite votre nouvelle machine virtuelle.

Assurer vous en accédant au gestionnaire de votre poste de travail que toutes les fonctionnalités de sécurité soient désactivées (pas de firewall, pas de SELinux). Fonctionnalités normalement désactivées à l'installation.

Désactivation du firewall en ligne de commande :

- pour voir si votre firewall est activé : `/etc/init.d/iptables status`
- pour désactiver votre firewall : `/etc/init.d/iptables stop`

Avant de procéder à la configuration de votre serveur DNS, vérifier qu'il est bien installé sur votre machine.
Si ce n'est pas le cas, les packages à installer sont les suivants :

- `bind-9.dernière_version_stable`
- `bind-utils-9.dernière_version_stable`
- `bind-libs-9.dernière_version_stable`

Depuis votre CentOs : `yum install bind`

Vous pouvez vérifier que l'ensemble de ces packages a été correctement installé à l'aide de la commande suivante :

```
[root@localhost ~]# rpm -qa | grep bind
bind-9.version_installee
bind-utils-9. version_installee
```

Vous disposez de fichiers exemples dans les répertoires suivants :

- `/usr/share/doc/bind-9.x/sample/etc`
- `/usr/share/doc/bind-9.x/sample/var`

3.1.2. Le fichier `named.conf`

Le fichier de configuration principal pour le DNS est `/etc/named.conf`.
Identifiez les éléments principaux de ce fichier de configuration (votre ami : `man named.conf` !!)

A partir des fichiers installés avec l'installation de bind :

- Identifier le répertoire où se situent les fichiers de zone. Quels sont les fichiers dans lesquels sont définis les différents enregistrements du domaine ? Expliquer le rôle et les paramètres de chacun de ces enregistrements.
- Quel fichier donne la définition des serveurs de noms racines ? Expliquer leurs rôles.

Chaque modification du fichier `named.conf` nécessite le redémarrage du serveur.

Pour lancer, arrêter ou bien connaître le statut de votre serveur DNS il faut utiliser la commande suivante : `/etc/init.d/named start | stop | status.`

3.1.3 Configuration IP du serveur

La configuration de vos machines en serveur DNS oblige à repasser en adressage statique.

- Arrêt du processus `dc_client`
- Modification des paramètres IP dans `/etc/sysconfig/network-scripts/ifcfg-eth0`
- Pour connaître les paramètres de `sysconfig`, consulter le fichier `sysconfig.txt` dans le répertoire `/usr/share/doc/initscripts-8.45.19.EL/`

Exemple de fichier de configuration de votre interface (prendre les adresses en 192.168.100.x avec x, votre numéro de binôme et comme adresse de la gateway, celle de la salle ASR).

```
[root@localhost ~]# more /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
HWADDR=08:00:27:42:31:7c
IPADDR=192.168.100.15
NETMASK=255.255.255.0
GATEWAY=192.168.0.2
```

RQ : Votre machine virtuelle sera en mode bridge, expliquez ce que cela signifie.

Penser à redémarrer le service afin que vos configurations soient prises en compte.

```
/etc/init.d/network restart
```

3.2. Configuration d'un Serveur DNS Primaire

Chaque binôme doit configurer sa propre machine en tant que serveur primaire.

- Déclaration de la zone **`monsite.fr`** :

Modifier le fichier `named.conf` de façon à déclarer votre zone **`monsite.fr`** et la zone de résolution inverse.

- Création du fichier de zone pour la zone **`monsite.fr`** :

Ce fichier sera utilisé par le serveur DNS pour faire la correspondance nom de machine -> @IP.
Dans ce fichier vous allez déclarer toutes vos machines ainsi que leurs adresses IP

  - ServDNS ⇔ @IP1 (@ de votre machine)
  - PCtest ⇔ @IP2 (choisir une adresse quelconque)
  - www.monsite.fr déclaré comme un alias de PCtest

Pour éviter les erreurs de syntaxe, utiliser un fichier déjà existant (par exemple, `localdomain`), en faire une copie et modifier le pour créer votre propre fichier de zone.

Quel est le rôle des différents paramètres de ce fichier de zone ?
Faire un test du bon fonctionnement de la résolution de nom.

- Création du fichier de zone pour la résolution inverse de la zone **`monsite.fr`** :

Ce fichier sera utilisé par le serveur DNS pour faire la correspondance @IP -> nom de machine. Intégrer les machines déclarées dans la question précédente.

Tester de fonctionnement du serveur primaire en résolution directe et inverse.

Faire les modifications nécessaires pour tester le serveur DNS de votre voisin (vous êtes alors client pour son serveur DNS). Redevenez ensuite « client » de votre propre serveur DNS.

Dans une configuration réseau d'entreprise, il est nécessaire de configurer également un serveur DNS secondaire, quel est son rôle ?

3.3. Ajout dynamique d'une entrée dans le DNS

La commande **nsupdate** vous permet d'ajouter une entrée dans le DNS d'une façon dynamique sans avoir à modifier manuellement les différents fichiers de configuration.

ATTENTION : dans cette partie il faut être très vigilent à la notion de droit sur les fichiers et répertoires créés. L'utilisateur named doit avoir des droit d'exécution dans les répertoires créés, des doits de lecture pour les fichiers de clefs et des droits d'écriture pour le fichier de zone (puisque le nsupdate va modifier les fichiers de zone).

L'idéal est que ces différents répertoires ou fichiers appartiennent à l'utilisateur named et au groupe named (commandes chgrp et chown)

Génération de la clef

Tout d'abord, pour des problèmes de sécurité, il faut une clé de cryptage générée à l'aide de la commande **dnssec-keygen** (cf. man de cette commande) fournie avec BIND, la clé générée sera au format TSIG (on parle d'ailleurs de clé TSIG).

Créer un répertoire /var/named/keys dans lequel vous créerez votre clef via la commande suivante : `dnssec-keygen -a hmac-md5 -b 512 -n HOST key-dns` (`key-dns`, nom du fichier créé)

Expliquer le rôle de chaque argument donné ci-dessus.

A la suite de cette commande deux clés sont créées. Ces deux clés sont de la forme `Kkey-dns.+157+20468.key` et `Kkey-dns.+157+20468.private` (les valeurs de clef sont identiques).

Nous utiliserons la valeur de cette clé pour la rajouter dans le fichier named.conf.

Configuration de named.conf

Une fois la valeur récupérée, il faut rajouter une entrée dans named.conf pour cette clé. La syntaxe de cette entrée est :

```
key "key-dns." {
        algorithm hmac-md5;
        secret " +w88hwya1EWi+O oePGqs4NVtw8uP5tMLrdM2VqvJ5A6Q==" ;
          clef privée récupérée dans Kkey-dns.+157+20468.key
 };
```

Puis, dans la zone où l'ajout dynamique est permis, il faut ajouter l'option **`allow-udpate`**. Dans notre cas il s'agit de la zone monsite.fr. Les modifications à faire sont :

```
zone "monsite.fr" {
         type master;
         file "nom de votre fichier";
allow-update { key "key-dns."; };
 };
```

Ajout dynamique d'une entrée

Une fois que vous avez effectué toutes ces modifications, vous pouvez utiliser la commande **nsupdate**.

En vous appuyant sur le man de nsupdate, ajouter dynamiquement un hôte.

Vérifier que le nom d'hôte est bien ajouté dans le fichier de zone (attention cette entrée n'est pas immédiatement visible dans le fichier de zone, mais elle est bien ajoutée immédiatement de façon dynamique, ce qui peut être testé grâce à nslookup « nouvel hôte ajouté »).

Exemple d'utilisation de la commande nsupdate

```
[root@localhost etc]# nsupdate -k /var/lib/named/var/named/keys/Kkey-
dns.+157+15986.key
> server 192.168.101.131
> zone monsite.fr
> update add machine.cath.fr. 86400 IN A 192.168.101.77
> taper enter (permet d'envoyer la nouvelle entrée vers le serveur DNS)
>
```

Supprimer dynamiquement l'hôte que vous venez de créer et vérifier sa suppression du fichier monsite.fr.

4. Création d'un script de sauvegarde

Vous devez concevoir un script de sauvegarde permettant d'archiver la configuration (`/etc`) et les données du serveur de nom (`/var/named`) en utilisant la commande « `cp` ».

Les archives seront placées dans le dossier « `/home/Bind_BackUp/YYYY-mm` » avec la convention de nommage suivante :

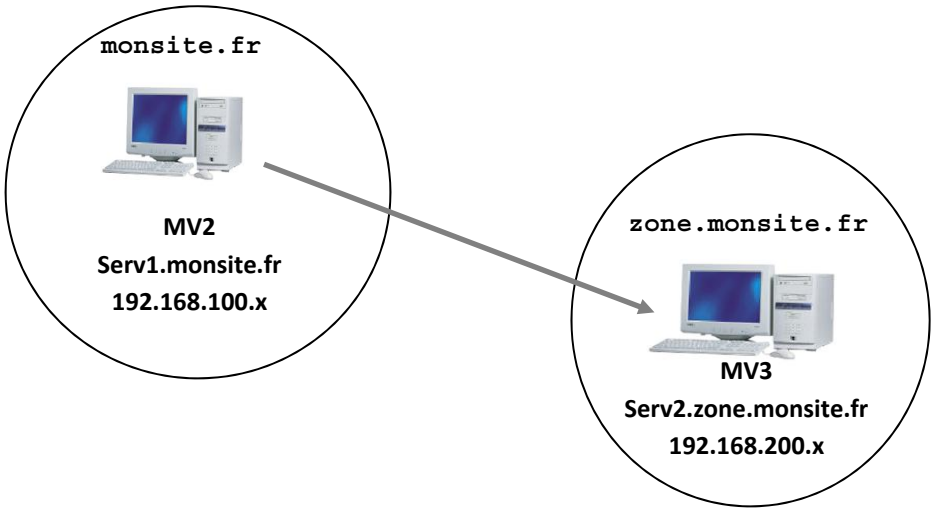
- Pour la configuration : `dd-HHMMSS_etc/`
- Pour les données : `dd-HHMMSS_var/named/`

Modifier votre script pour produire des archives comprimées (cf. `tar`) l'archive se nommera « `dd-HHMMSS_named.tgz` » sera placée en « `/home/Named_BackUp/YYYY-mm` » et contiendra les fichiers présents dans « `dd-HHMMSS_etc` » et « `dd-HHMMSS_var` ». Une fois l'archive créée, on pourra supprimer les copies.

5. En bonus : Délégation de zone

Dans cette partie, nous allons voir comment on peut mettre en œuvre le mécanisme de délégation de zones.

A partir de deux machines virtuelles, utiliser la topologie suivante (valeurs données à titre d'exemple):



Le service DNS pour la zone **`zone.monsite.fr`** est délégué au serveur `Serv2.zone.monsite.fr`. Pour que la chaîne de délégation fonctionne, il faut modifier le fichier de zone de **`monsite.fr.`** Dans ce dernier il suffit d'indiquer que la zone `zone.monsite.fr` est gérée par le serveur `Serv2.zone.monsite.fr`.

- Déclaration de la délégation au niveau du serveur primaire

Modifier le fichier de zone de **`monsite.fr`** afin de respecter la chaîne de délégation.

```
zone.monsite.fr.          IN    NS    Serv2.zone.monsite.fr.

Serv2.zone.monsite.fr.    IN    A     192.168.200.x
```

Cette partie indique que le service DNS pour la zone : « zone.monsite.fr » est délégué au « Serv2.zone.monsite.fr » dont l'@IP est 192.168.200.x

- Configuration du serveur `Serv2.zone.monsite.fr`

Modifier le fichier `named.conf` du serveur `Serv2.zone.monsite.fr`. et les fichiers de zones pour la zone `zone.monsite.fr`..

- Modification du fichier `/etc/resolv.conf`

`Serv1.monsite.fr`. sera le serveur DNS déclaré.

- Test de la délégation de zone

Redémarrer les différents serveurs que vous venez de configurer. Tester à travers différentes requêtes les réponses renvoyées par vos serveurs.

Utiliser l'utilitaire `dig` pour voir les détails de la chaîne de délégation ? Que constatez-vous ? Observez les mécanismes de délégation.