Université Paris 13 Travaux Pratiques
IUT de Villetaneuse RESEAUX
Département T & R

TP DNS
Utilisation de BIND sous LINUX

Fait par : *Noureddine AWANE*

1- Utilisation basique d'un client DNS: démarré avec la distrub debian wireshark installer ou installable

Pour ce chapitre vous allez utiliser le PC de la salle de TP en installant Wireshark si ce n'est pas déjà installé.

Vérifiez que la configuration de votre poste est correcte (Poste linux voir le fichier /etc/resolv.conf) et que vous avez bien un serveur DNS configuré dessus.

Lancez une capture sur votre poste client en temps réel et capturez le trafic DNS échangé entre votre client et le serveur DNS de référence. Dans un deuxième temps, réalisez un certain nombre de requêtes DNS à l'aide du navigateur internet Firefox installé sur votre client (accédez par exemple à la page https://www.univ-paris13.fr/)

Utilisez Wireshark pour analyser le trafic échangé. Donner le protocole de transport ainsi que le port utilisé pour DNS?

Observez le trafic généré, sélectionnez les paquets relatifs au protocole DNS et retrouvez les séquences du protocole DNS présentées en cours.

Remarque: filtrer la capture pour garder que le flux DNS.

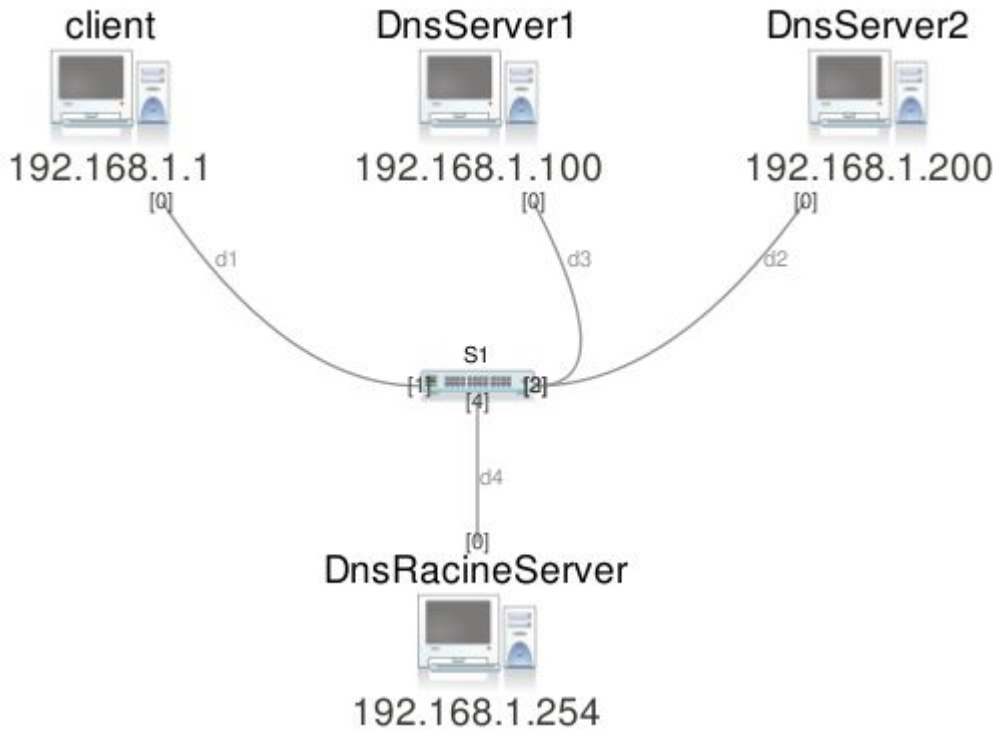
Faites correspondre une réponse DNS à sa requête. Quel paramètre permet cette correspondance?

Analysez les Paquets (requête et réponse) et détaillez les différents champs de l'entête, de la question et de la réponse?

2- Installation et configuration d'un serveur DNS :

Pour le reste du TP, on va utiliser l'outil Marionnet pour la simulation des serveurs DNS (Restaurer l'image **LINUX CRIT** et lancez Marionnet).

Le but de ce TP est créer la topologie réseau suivante :



Après avoir réalisé la topologie ci-dessous, configurez les IP des différentes interfaces réseaux de toutes les machines :

ifconfig eth0 192.168.1.X/24 up (x : voir la topologie pour définir le dernier octet de l'@ IP)

Après avoir démarré toutes les machines sur Marionnet. Vous devez pouvoir faire un ping vers les différentes adresses IP en se positionnant à tour de rôle sur une machine (client, DnsServer1, DnsServer2 et DnsRacineServer).

Consultez le fichier */etc/nsswitch.conf* et trouvez la ligne qui détermine l'ordre d'utilisation des méthodes de résolution. Assurez-vous qu'on utilise d'abord la résolution statique, puis la résolution par serveur DNS.

2.1 ***Configuration du serveur master : DnsServer1***

2.1.1 Configuration du domaine principal:

Le serveur DnsServer1 sera notre serveur Master. Créer un répertoire qui contiendra les définitions des fichiers de zone sur ce serveur : ***/var/named/maitre***

Editez le fichier de configuration de BIND (programme ***named***) ***/etc/bind/named.conf*** et remplacez le contenu par celui-ci:

```
options {
        directory "/var/named" ;
        listen-on { any; };
        allow-query { any; };
} ;
```

```
zone ue31.p13.fr {
        type master ;
        file "maitre/ue31.p13.fr" ;
        allow-update { none ; } ;
        notify no ;

} ;
```

/etc/bind/named.conf

Ensuite, il faut créer le fichier de zone suivant : ***/var/named/maitre/ue31.p13.fr*** en vous appuyant sur le polycopié et les contraintes suivantes :

• numéro de série au format usuel (aaaammjj01 par exemple, avec 'aaaa' pour l'année, 'mm' pour le mois et 'jj' la date du jour), temps de rafraichissement (refresh) de 120 s.
• délai entre essais infructueux (retry) de 60 s.
• délai d'expiration définitif (Expire) de 300 s.
• TTL de 180 s.
• adresse mail du responsable : ***root@ue31.p13.fr***

Pour vous aider à corriger les erreurs de configuration ***/etc/bind/named.conf*** et ***/var/named/maitre/ue31.p13.fr*** vous avez à votre disposition deux utilitaires : ***named-checkconf*** et ***named-checkzone***

La syntaxe de ***named-checkzone*** est : ***named-checkzone zone fichier_zone.***

Démarrez ensuite le serveur de nom : ***service named start*** (ou ***/etc/init.d/bind9 start*** sur Marionnet)

Remarque: Après chaque modification des fichiers de configuration, il faut redémarrer le démon :

/etc/init.d/bind9 restart

Il est vivement conseillé de regarder les logs pour vérifier que le démarrage du démon s'est correctement effectué : ***tail -30 /var/log/messages***

Ou exécutez ***tail -f /var/log/messages*** sur un nouveau terminal. Cette commande permet de lire en continue un fichier dans lequel les messages d'erreurs du serveur DNS seront affichés. Attention le message OK est parfois faux.

2.1.2 Tests de la résolution des noms

Vous configurez tous le poste client de votre plate-forme sur DnseServer1.
Sous Linux, cette configuration se réalise dans le fichier /etc/resolv.conf en ajoutant la ligne suivante:

nameserver 192.168.1.100

Procédez ensuite à des batteries de tests pour valider la résolution DNS pour :

DnsServer1.ue31.p13.fr

DnsServer2.ue31.p13.fr

Validez que la résolution se passe correctement et analyser chaque champs des réponses. Voir Annexe1 pour les outils de tests.

En se basant sur le résultat de la commande ***dig***, faites la correspondance avec l'entête/champs DNS développée dans le cours.

2.1.3 Configuration de la zone inversée :

Pour la résolution inverse, dans le fichier named.conf, on rajoute :

```
zone "1.168.192.in-addr.arpa" {
type master;
file "maitre/1.168.192.in-addr.arpa";
};
```

/etc/bind/named.conf

Ensuite, il faut créer le fichier suivant : */var/named/maitre/*1.168.192.in-addr.arpa en vous appuyant sur le polycopié et les contraintes suivantes :

- numéro de série au format usuel (aaaammjj01 par exemple, avec 'aaaa' pour l'année, 'mm' pour le mois et 'jj' la date du jour), temps de rafraichissement (refresh) de 120 s.
- délai entre essais infructueux (retry) de 60 s.
- délai d'expiration définitif (Expire) de 300 s.
- TTL de 180 s.
- adresse mail du responsable : ***root@ue31.p13.fr***

Votre configuration de la zone doit permettre une résolution inversée des deux IP suivantes :

192.168.1.100 ***DnsServer1.ue31.p13.fr***

192.168.1.200 ***DnsServer2.ue31.p13.fr***

N'oubliez pas de valider la conf DNS et Zone avec les utilitaires vus plus haut (**named-checkconf** et ***named-checkzone****) et* redémarrer le service bind pour la prise en charge des modifications/ajouts.

Refaites les mêmes batteries de tests et assurez-vous que la résolution inverse est fonctionnelle.

2.1.4 Configuration d'un serveur DNS secondaire

Pour équilibrer la charge des DNS Locaux, on mettra en place un autre DNS. Dans ce cas on configurera un serveur DNS secondaire: ***DnsServer2***

La connectivité IP a déjà été validée entre les deux serveurs précédemment. Maintenant, vous deviez valider l'accessibilité niveau transport L4 (Protocole/port).

Quel est le protocole/Port qui sera utiliser pour la communication entre le maitre et le slave? Validez cette accessibilité?

Une fois l'accessibilité validée, on configurera le serveur DNS secondaire. Pour cela, nous allons aussi utiliser le daemon named avec une configuration spécifique.

Modifier le fichier de configuration ***/etc/bind/named.conf*** par :

```
options {
        directory "/var/named" ;
} ;

zone ue31.p13.fr {
        type slave ;
        file "slave/ue31.p13.fr" ;
        masters { 192.168.1.100; };
} ;

zone 1.168.192.in-addr.arpa {
        type slave ;
        file "slave/1.168.192.in-addr.arpa" ;
        masters { 192.168.1.100; };
} ;
```

/etc/bind/named.conf

Le téléchargement des fichiers de zones entre le serveur primaire et le serveur secondaire se fera automatiquement au démarrage du daemon named.

Attention Bind doit pouvoir accéder au dossier des zones. Utilisez chmod pour régler tout cela.

Lancez une capture tcpdump sur le serveur primaire en filtrant sur l'IP du serveur secondaire (192.168.1.200).

Vous pouvez maintenant lancer votre serveur DNS secondaire:

 # /etc/init.d/named start

Il faut d'abord vérifier que les fichiers de zones sont bien présents dans le répertoire ***/var/named/slave/.***

Arrêtez et Analysez le résultat de la capture prise sur le DNS primaire. Quel protocole a été utilisé pour la communication entre le slave et Master ? Définissez le port utilisé?

Pour valider que la résolution sur serveur secondaire marche bien, il faut se mettre sur la machine client lancer la commande ***dig***:

 # dig @192.168.1.200 ue31.p13.fr

Changez la configuration du poste client pour mettre l'interrogation DNS vers le serveur Secondaire en premier. Et refaites les batteries de tests pour valider la résolution de domaine et la résolution inverse pour :

192.168.1.100 DnsServer1.ue31.p13.fr

192.168.1.200 DnsServer1.ue31.p13.fr

2.1.5 Mise à jour des zones:

Modifiez le numéro de série de la zone ***ue31.p13.fr*** sur le serveur primaire. La modification a-t-elle été répliquée immédiatement sur le serveur secondaire? Quand est ce qu'elle sera changée sur le secondaire ?

Modifier la configuration sur serveur DNS Master pour qu'il notifie toute modification sur ces zones au serveur Slave.

3- Configuration de serveur de cache (en resolveur)

Sur le serveur DnsServer1, modifiez la configuration du fichier ***named.conf*** en ajoutant les lignes suivantes :

```
zone "." {
        type hint;
        file "hint/root.servers";
};
```

Créer le répertoire ***hint*** ainsi que le fichier ***root.servers*** en ajoutant les lignes suivantes :

.	***3600000***	***NS***	***DnsServerRacine.NET.***
DnsServerRacine.NET.	***3600000***	***A***	***192.168.1.254***

Sur le serveur racine, éditez le fichier de configuration de BIND (programme named) ***/etc/bind/named.conf*** et remplacez le contenu par celui-ci:

```
options {
        directory "/var/named";
};
zone univ-paris13.fr {
        type master;
        file    "univ-paris13.fr";
};
```

Créez la zone univ-paris13.fr :

```
$TTL 180
@       IN      SOA     DnsRacineServer.univ-paris13.fr.        root.univ-paris13.fr. (
2016112901 ;
120 ;
60 ;
300 ;
180 ;
)
@       NS      DnsRacineServer.univ-paris13.fr.        ;
www     IN      A       192.168.1.200
```

Et démarrez le service bind : ***/etc/init.d/bind start***

Lancez une capture sur DnsServer1 et sur DnsRacineServer

A partir du poste client faite un test de résolution pour www.univ-paris13.fr en utilisant l'outil dig.

Analysez le résultat des captures prises.

Refaites le même test et regardez les captures, quelle est la différence par rapport au 1er test de résolution ?

Vérifiez le contenu du cache par en utilisant la commande ***rndc dump_db*** qui dumpera le contenu du cache bind dans le répertoire spécifique. Vérifiez cela *en* lisant le fichier généré ***/var/named/named_dump.db***

Remarque: pour vider le cache utiliser la commande ***rndc flush***

Sur le serveur DnsServer1, limitez la récursion uniquement aux demandes venantes du client (192.168.1.1). Valider cela en faisant une demande de résolution www.univ-paris13.fr à partir du poste DnsServer2. Qu'avez-vous eu comme résultat à votre requête ?

4- Installation Forwarding Name Server:

Sur le serveur DnsServer2, remplacez le fichier named.conf par :

```
options {
        directory "/var/named";
        version "not currently available";
        forwarders {192.168.1.100 ;};
        forward only;
};
```

Configurez le poste client pour qu'il interroge le serveur DnsServer2. A partir du poste client, lancez deux fois des tests de résolution DNS vers :

www.univ-paris13.com

DnsServer1.ue31.p13.fr

Détaillez le cheminement pris pour chaque requête. Quelle est la différence entre les deux?

Quel est le rôle du serveur DnsServer2? Quel est l'intérêt de déployer un tel serveur?

Peut-on utiliser la fonctionnalité de ce serveur uniquement pour un domaine? Pourriez-vous configurer cela ?

Annexe : Commandes de tests

Il existe plusieurs outils pour tester le bon fonctionnement de la résolution des noms :

ping

La commande *ping* est la plus simple (mais la plus limitée). Elle permet de tester la résolution du nom, mais pas la résolution inverse :

$ ping NomDuServeur

host

La commande *host*, permet de tester la résolution du nom et la résolution inverse :

$ host NomDuServeur
ou :
$ host AdresseIPduServeur

nslookup

La commande *nslookup* du paquet *dnsutils*, permet également de tester la résolution du nom et la résolution inverse :

$ nslookup NomDuServeur
ou :
$ nslookup AdresseIPduServeur

dig

La commande *dig* du paquet *dnsutils*, permet également de tester la résolution du nom et la résolution inverse. Mais la commande *dig* permet surtout d'interroger directement le serveur bind et obtenir de nombreuses autres informations :

$ dig NomDuServeur.NomDuDomaine

Remarque : Le nom du domaine est obligatoire pour obtenir une réponse (**ANSWER SECTION**)

ou :
$ dig -x AdresseIPduServeur

Remarque : Le paramètre « -x » est obligatoire pour obtenir une réponse (**ANSWER SECTION**).Cette dernière commande est équivalente à :

$ dig PTR AdresseIPduServeurinversée.in-addr.arpa.