

STEAVE PORTFOLIO

DNS

DOCUMENTATION: DNS SYSTEM



RÉALISER PAR STEAVE.





À PROPOS DU TP

L'objectif est de reproduire le fonctionnement complet du système DNS dans la salle de TP.

Le professeur gère un serveur racine et chaque groupe d'étudiants gère son propre nom de domaine sans connaître les détails des domaines des autres groupes. La résolution de noms se fait par rapport au serveur racine local.

SOMMAIRE:

- Réservation et déclaration du nom de domaine
- Configuration de chaque domaine
- Configuration des postes clients
- Configuration de la zone inverse
- Sécurisation minimale du serveur
- Créations des sous domaines
- Configuration des serveurs secondaires







La première étape consiste à choisir son nom de domaine ainsi qu'à le déclarer au serveur.

Pour ma part mon nom de domaine est "steavi".

Pour enregistrer chaque nom de domaine

Il faut fournir les informations suivantes :

- nom du domaine pleinement qualifié
- adresse IP et nom du serveur principal du domaine
- éventuellement adresse(s) IP et nom(s) du ou des serveurs secondaires



À QUOI ÇA SERT?

Le but d'un nom de domaine est de retenir et communiquer facilement l'adresse d'un ensemble de serveurs (site web, courrier électronique, FTP). Par exemple, wikipedia.org est plus simple à mémoriser que 208.80.154.224 ou 91.198.174.192.

Dans mon cas:

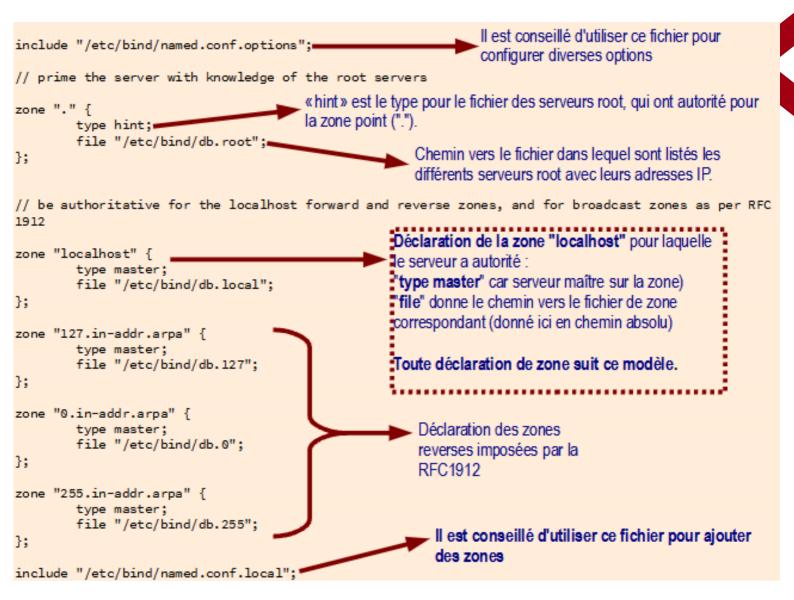
- nom de domaine pleinement qualifié = Steavi
- Adresse IP et nom du serveur = 172.25.54.254 / BBZ
- éventuellement adresse(s) IP et nom(s) du ou des serveurs secondaires = 172.25.50.254 / BBZ2



CONFIGURATION DE CHAQUE DOMAINE.



FICHIER NAMED.CONF









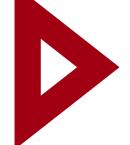


FICHIER DE ZONE DB.STEAVI.COM

TTL 86400			
@	IN	SOA	nsBBZ.steavi.com. hostmaster.steavi.com.
			2008113001 ;serial
			86400 ;refresh
			21600 ;retry
			3600000 ;expire
			3600) ;negative caching ttl
@	IN		NS nsBBZ
;@	IN		NS ns2.exemple.fr.
steavi.com	IN		MX 20 servmail
servmail	IN		A 172.25.54.254
nsBBZ	IN		A 172.25.54.254
;ns2	IN		A 172.25.50.254
servftp	IN		A 172.25.54.254
www	IN		CNAME www.steavi.com.
mail	IN		CNAME servmail.steavi.com.
ftp	IN		CNAME servftp







CONFIGURATIONS DES POSTES CLIENTS

Une des conditions de réussite du TP est de pouvoir faire un ping :

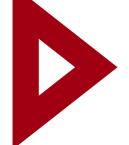
- sur chacune des trois machines déclarées dans tous les domaines affichés au tableau depuis

tout poste correctement configuré de la salle de TP, par exemple :

- ping www.steavi.com
- ping ftp.steavi.com
- ping mail.steavi.com
- sur chacune des machines déclarées sur une autre plate-forme.

vérifications des données relatives à chaque zone

```
dig www.steavi.com
; <<>> DiG 9.5.0-P2 <<>> www.steavi.com
                                                                      a requête a réussi
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26702
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3,
    flag "ra" : le serveur est récursif
                                                                 Nombre de réponses pour chaque
;; QUESTION SECTION: (1)
                                ΙN
;www.reseaucerta.org.
;; ANSWER SECTION: (2)
www.reseaucerta.org.
                        1785
                                        CNAME
                                                 strasbourg.steavi.com.
strasbourg.reseaucerta.org. 3585 IN
                                                 130.79.130.89
;; AUTHORITY SECTION: (3)
                                            c.dns.gandi.net.
steavi.com.
                   10785
                           IN
                                   NS
                   10785
                           IN
                                   NS
                                           b.dns.gandi.net.
Steavi.com.
                   10785
                           IN
                                            a.dns.gandi.net.
Steavi.com.
                                   NS
;; ADDITIONAL SECTION: (4)
a.dns.gandi.net.
                                                217,70,179,40
                        117683 IN
b.dns.gandi.net.
                        117683 IN
                                                217.70.184.40
c.dns.gandi.net.
                        117683 IN
                                                217.70.182.20
;; Query time: 2 msec (5)
                                                                     L'adresse IP du serveur
;; SERVER: 192.168.1.1#53(192.168.1.1) -
;; WHEN: Wed Jan 28 12:20:18 2009
                                                                       DNS qui a répondu
;; MSG SIZE rcvd: 187
```



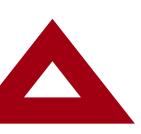
CONFIGURATION DE LA ZONE INVERSE:

Pour le réseau de votre groupe, vous avez obtenu une délégation de la racine sur la zone inverse que vous devez configurer.

Votre professeur a présumé que les mêmes serveurs sont utilisés pour gérer votre nom de domaine et votre zone inverse.

afin de configurer la zone inverse, il faut ce rendre dans le dossier : named.conf.local







SÉCURISATION MINIMALE DU SERVEUR LES ACL

Le fonctionnement par défaut de bind9 est récursif et ceci peut entraîner des problèmes de sécuri-

té. Il est normal de prendre en charge de manière récursive les interrogations émises par les hôtes

de votre réseau de manière à alimenter le cache et optimiser le fonctionnement du service.

Mais vous devez interdire la résolution récursive pour toute machine qui n'appartient pas à votre

groupe. Bien entendu les requêtes itératives sur votre nom de domaine sont autorisées pour tout

le monde. Vous devez pour cela utiliser les notions d'ACL et éventuellement de vues.

```
};
options {
directory "/var/cache/bind";
auth-nxdomain no; # conform to RFC1035
listen-on-v6 { any; };
allow-recursion { reseauInterne; };
};
acl reseauInterne {
localnets;
localhost;
};
acl servExterne {
!localnets;
!localhost;
};
```



CRÉATION DES SOUS DOMAINES :

INTRANET / EXTRANET

Une fois que les domaines principaux sont servis et sécurisés correctement, il faut restructurer l'espace de nom en créant, pour chaque domaine deux sous-domaines : intranet et extranet (intranet.mondomaine.org et extranet.mondomaine.org).

Sur le domaine intranet il faut créer les enregistrements pour les machines suivantes

:

- www
- ftp
- support

Sur le domaine extranet il faut créer les enregistrements pour les machines suivantes .



- www
- ftp
- clients
- fournisseurs

FICHIER DE ZONE EN AJOUTANT LE INTRANET ET LE EXTRANET :

TTL 86400			
@	IN	SOA	nsBBZ.steavi.com. hostmaster.steavi.com. (2008113001 ;serial
			86400 ;refresh
			21600 ;retry
			3600000 ;expire
			3600) ;negative caching ttl
@	IN		NS nsBBZ
;@	IN		NS ns2.exemple.fr.
steavi.com	IN		MX 20 servmail
servmail	IN		A 172.25.54.254
nsBBZ	IN		A 172.25.54.254
;ns2	IN		A 172.25.50.254
servftp	IN		A 172.25.54.254
www	IN		CNAME www.steavi.com.
mail	IN		CNAME servmail.steavi.com.
ftp	IN		CNAME servftp
intranet	IN		NS nsBBZ.intranet.steavi.com.
extranet	IN		NS nsBBZ.extranet.steavi.com.
nsBBZ.intranet.steavi.com.	IN		A 172.25.54.254
nsBBZ.extranet.steavi.com.	IN		A 172.25.54.254



CRÉATION DES SOUS DOMAINES :

INTRANET / EXTRANET

Une fois que les domaines principaux sont servis et sécurisés correctement, il faut restructurer l'espace de nom en créant, pour chaque domaine deux sous-domaines : intranet et extranet (intranet.mondomaine.org et extranet.mondomaine.org).

Sur le domaine intranet il faut créer les enregistrements pour les machines suivantes :

- www
- ftp
- support

Sur le domaine extranet il faut créer les enregistrements pour les machines suivantes .

- www
- ftp
- clients
- fournisseurs

FICHIER NAMED.CONF.LOCAL





CONFIGURATION DES SERVEURS SECONDAIRES

Délégation de zone

Un serveur de noms secondaire ne gère pas directement les informations sur les zones mais les obtient à partir du serveur de noms principal de la zone (ou d'un autre serveur secondaire) via le réseau (transfert de zone). Un serveur secondaire ne peut modifier des données de la zone mais il a lui aussi autorité sur la zone.

Cette redondance permet une meilleure tolérance aux pannes et une réduction de la charge de travail des serveurs principaux.

Dans le fichier de zone du serveur secondaire :

```
zone "steavi.com" {
    type slave;
    file "slave/db.steavi.com";
    masters { 172.25.54.254; };
};
```

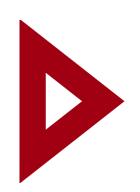
Dans le fichier de zone du serveur principal :

```
zone "steav1.com" {
    type master;
    file "db.steavi.com";
    allow-transfer { 172.25.50.254; };
};
```



db.steavi.com sur le serveur secondaire :

```
$TTL
     86400
exemple.fr. IN
                          bbz2.steavi.com. hostmaster.steavi.com. (
                  SOA
      2008113001 ;serial
                 ;refresh
      86400
      21600
                 ;retry
                ;expire
      3600000
      3600 ; negative caching ttl )
                                       bbz2.steavi.com.
                   IN
                          NS
servSec
                                       172.25.50.254
                   IN
                          A
```



STEAVE PORTFOLIO

DNS

DOCUMENTATION: DNS SYSTEM



RÉALISER PAR STEAVE.

