ISET de Sfax - Département Technologie Informatique

Administration Linux

Chapitre 4

Configuration DNS

Azer ZAIRI

Courriels : Azer.ZAIRI@gnet.tn

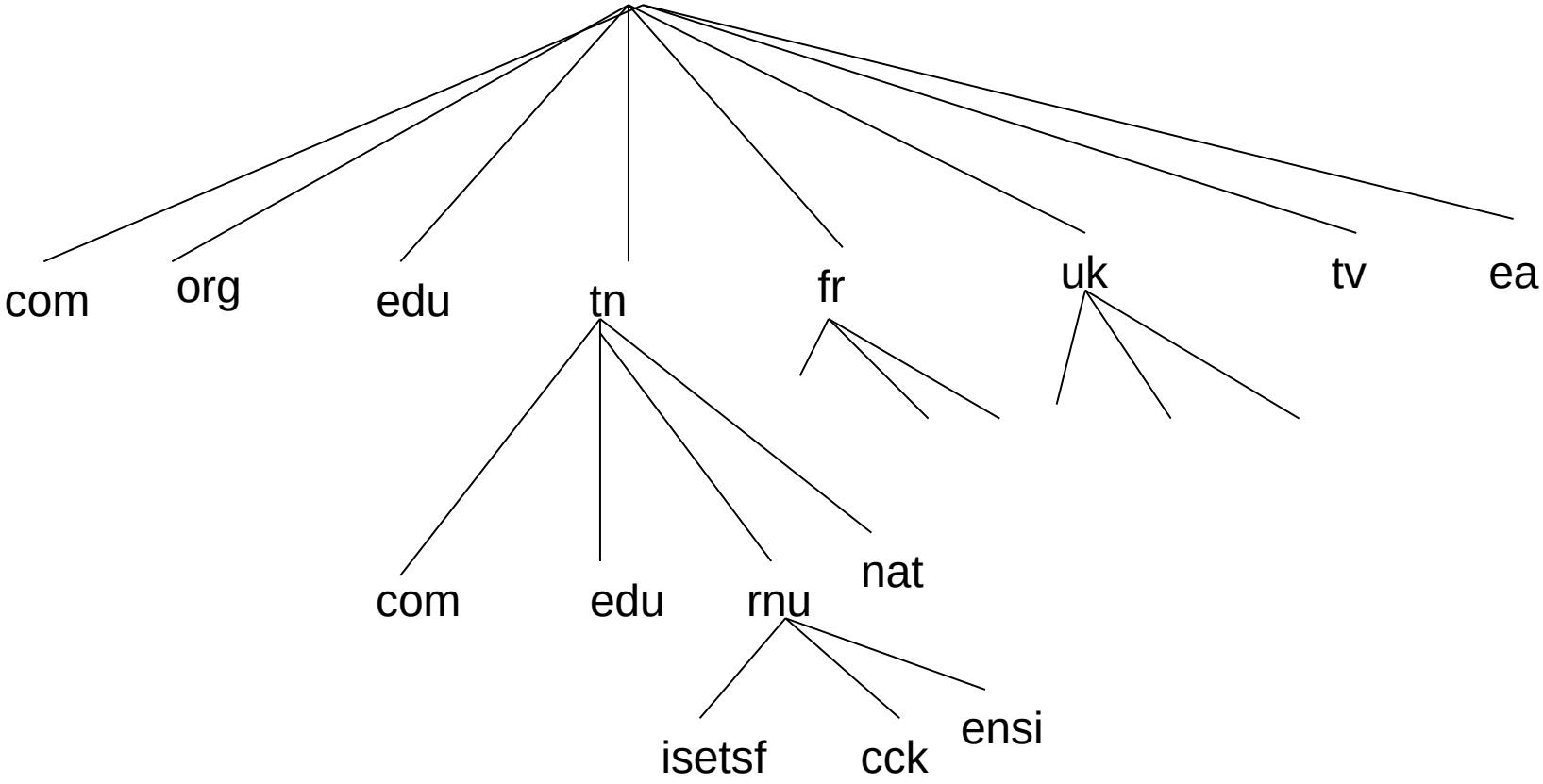
Introduction

- DNS : Domain Name System
- Le service DNS assure principalement :
  - la conversion de noms de domaine en adresses IP
  - et la détermination d'un serveur de messagerie pour une adresse électronique.
- Le service DNS d'Internet est un système distribué constitué de l'ensemble des serveurs DNS.

La désignation universelle

- Un **nom symbolique** sert à désigner une machine, un service, une adresse, une route pour les atteindre.
- Le InterNIC (Centre d'information du réseau Internet) gère le domaine des noms et détermine si les noms proposés sont acceptables.
- Le système des domaines est un système **hiérarchique**. Ce qui permet de ne pas avoir à faire à une administration centrale à chaque fois que l'on rajoute une machine dans son réseau local.
- **Désignation : objet.sous-domaine.domaine**
- **Objet :** nom d'une machine, par exemple (rubis) ou de service (www, ftp,…)
- **Domaine :**
  - politiques (tn, fr, de, jp, nl,...)
  - ou institutionnels (com, org, gov, edu, net, mil,…)
- L'adresse complète d'un site Web ou un hôte est connue souvent sous le nom de **FQDN** : Fully Qualified Domain Name
  - C'est un nom de domaine pleinement qualifié.
  - Il indique la position exacte d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur.
  - On parle également d'un domaine absolu, par opposition à un domaine relatif.

Hiérarchie des noms de domaines

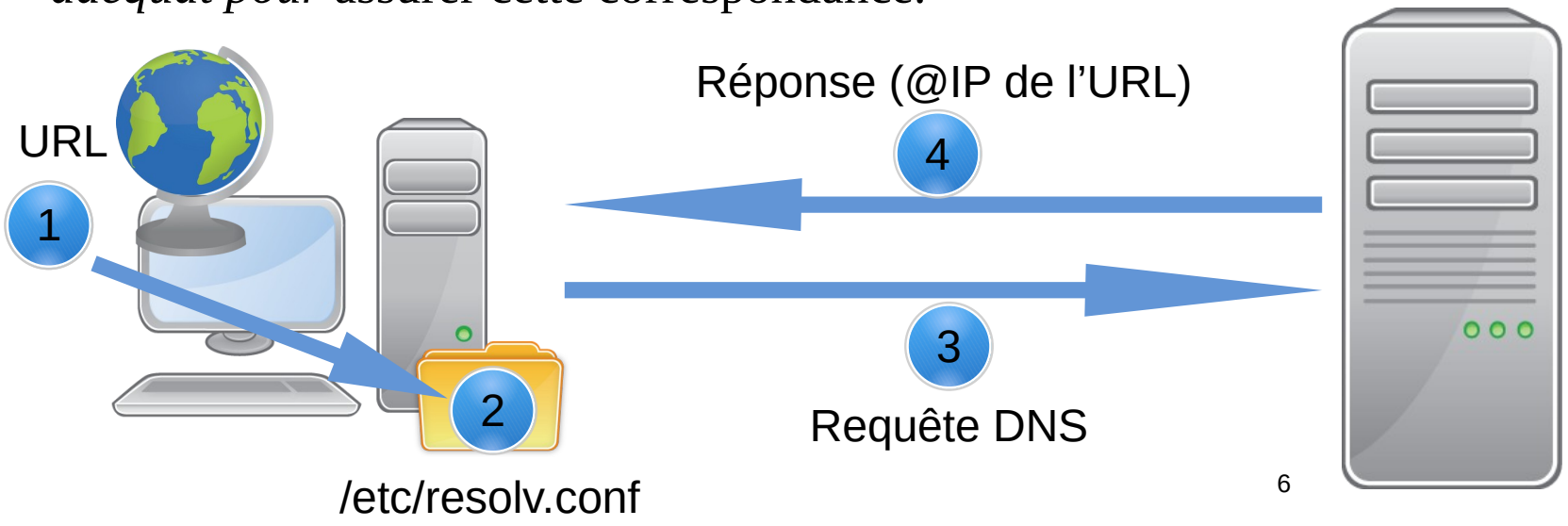


Terminologies

- **Domaine** : un domaine est un sous arbre de l’espace « nom de domaine »;
- **Zone** : une partie de l’espace « nom de domaine ».
- **Délégation** : transfert de la responsabilité d ’une zone à une ou plusieurs de ses sous-zones.

Résolution de noms

- Comme la majorité des application réseaux modernes, le service DNS utilise l'architecture client/serveur
- Lorsqu'une application réseau veut communiquer en utilisant un nom de domaine, elle demande la résolution de la correspondance IP à l'application client DNS locale (*resolver).*
- D'après la configuration (/etc/resolv.conf), le *resolver consulte le DNS adéquat pour* assurer cette correspondance.



Organisation en zones

- On parle de **Zone** pour une **partie contiguë de l'arborescence** sur laquelle un serveur a autorité.
- Le DNS peut être partitionné sur plusieurs serveurs.
- Aucun serveur DNS n'a une vue d'ensemble de l'Internet.
- Chaque **zone a un ensemble de serveurs** faisant autorité.
- Les informations sont dupliquées physiquement sur ces serveurs
- Les noms des domaines peuvent être de niveaux supérieure, de second niveau ou des sous domaines .
- Les **ressources** de chaque domaines sont **stockées** dans les **enregistrement de ressources .**
- La gestion interne des ressources de domaines est effectuée à l’aide de fichier de zone DNS.
- Un fichier de zone DNS est une base de données.

Les serveurs de noms

- Les serveurs de nom enregistrent les données propres à une partie de l'espace nom de domaine dans une zone.
- Le serveur de nom à autorité administrative sur cette zone.
- Un serveur de nom peut avoir autorité sur plusieurs zones.
- **Serveur de nom primaire** : maintient la base de données de la zone dont il a l'autorité administrative
- **Serveur cache** : son rôle est d'accélérer la résolution de nom et des adresses
- **Serveur de nom secondaire** : obtient les données de la zone via un autre serveur de nom qui a également l'autorité administrative
- La redondance permet la défaillance éventuelle du primaire et du (des) secondaire(s).
- Il y a un serveur primaire et généralement plusieurs secondaires
- Un serveur de nom peut être primaire pour une (des) zone(s) et secondaire pour d'autre(s).

Le démon named

- Le démon named est le serveur DNS fourni par le paquetage BIND (*Berkeley Internet Name Domain).*
- *L'Université de Berkeley est à l'origine de BIND mais, actuellement, c'est* l'Internet System Consortium (*ISC) qui assure sa maintenance.*
- Le fichier de configuration principal de named est named.conf (sous /etc/ ou /etc/bind/).
- Une fois lancé, named enregistre son numéro de processus (*PID : Process IDentifier) dans* le fichier /var/run/named/named.pid.

Fichier de configuration /etc/bind/named.conf

- named.conf est le fichier de configuration principal du serveur DNS BIND.
- Il est le premier fichier lu par le démon named.
- La directive include permet de répartir la configuration sur plusieurs fichiers pour des fins de clarté ou d'organisation.

Exemple :

```
$ cat /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";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Structure et format

- named.conf est structuré en clauses regroupant chacune un ensemble d'instructions sous la forme d'un bloc.
- Il faut impérativement respecter la syntaxe du fichier qui peut être résumée par les règles suivantes :
  - une instruction se termine par « ; » ;
  - un bloc d'instruction débute par « { » et se termine par « }; » ;
  - un commentaire est écrit sous l'une des formes suivantes :
    - /* commentaire au style C */
    - // commentaire au style C++
    - # commentaire au style PERL/SHELL

Structure et format (Suite)

Les fichiers de configuration (tel que named.conf) est généralement sous la forme :

// définition des ACL : Listes de contrôle d'accès

acl "nomACL" {...};

// configuration de la journalisation

logging {...};

// définition des options globales

options {...};

// déclaration des zones prédéfinies

zone {...};

...

// déclaration des zones à résoudre

zone {...} ;

...

Zones particulières

- Le fichier named.conf inclut par défaut la déclaration des zones particulières racine,
  - localhost
  - et « 127.in-addr.arpa » :
- le fichier de la zone racine, désigné par « . » et de type hint, contient la liste des serveurs à interroger lorsqu'un serveur de nom n'arrive pas à résoudre une requête ;
- la zone « localhost » permet la résolution du nom « localhost » à l'adresse de boucle locale « 127.0.0.1 » lors de l'utilisation du serveur DNS ;
- la zone « 127.in-addr.arpa » assure la résolution inversée de l'adresse de boucle locale « 127.0.0.1 ».

Zones particulières (Suite)

EXEMPLE

- La portion du fichier named.conf qui suit illustre la déclaration de ces zones particulières.

```
zone "." {
type hint;
file "/etc/bind/db.root";
};
zone "localhost" {
type master;
file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
type master;
file "/etc/bind/db.127";
};
```

Fichier de zone

- Un fichier de zone contient les enregistrements de ressources (RR : *resource records) d'un* espace de noms.
- Le nom et l'emplacement d'un fichier de zone est spécifié par l'instruction file de la clause zone du fichier named.conf.

Format d’un fichier de zone

- Le format d'un fichier de zone peut se résumer par les points suivants :
  - un fichier de zone contient des commentaires, des directives et des enregistrements de ressources ;
  - un commentaire commence par « ; » et continue jusqu'à la fin de la ligne ;
  - une directive commence par « $ ». Les directives les plus courantes sont :
    - **$ORIGIN** : définit le nom de base qui sera concaténé à tous les enregistrements non totalement qualifiés,
    - **$INCLUDE** : inclut le fichier spécifié à l'endroit où apparaît la directive,
    - **$TTL** : règle la valeur par défaut de la durée de vie (*TTL : Time To Live) pour la* zone.
      - Elle doit être présente et doit figurer avant le premier enregistrement ;
  - le premier enregistrement de ressource doit être SOA (*Start Of Authority) ;*
  - le format général d'un enregistrement est : « nom ttl classe type valeur » où
- nom : nom (ou label) du noeud dans le fichier de zone auquel appartient cet enregistrement.
  - La valeur @ indique que la valeur de $ORIGIN sera utilisée et un blanc ou une tabulation indique que le dernier nom cité sera utilisé.

Format d’un fichier de zone (Suite)

- **ttl** : durée de vie (en seconde) de l'enregistrement dans un cache. La valeur 0 indique que l'enregistrement ne doit pas être maintenu dans un cache ;
- **classe** : définit la famille du protocole. La valeur normale est IN (*INternet protocol) ;*
- **type** : type de l'enregistrement de ressource ;
- **valeur** : valeur de l'enregistrement qui dépend du type et de la classe.

Format d’un fichier de zone (Suite)

- **Exemple**

```
$TTL 86400
$ORIGIN isetsfax.org.
@ IN SOA ns.isetsfax.org. hostmaster.isetsfax.org. (
        2024110818   ; Serial
        10800   ; Refresh (3 heures)
         600   ; Retry (10 minutes)
         1814400   ; Expiry (3 semaines)
         10800 ) ; TTL ou minimum (3 heures)
IN                      NS      ns.isetsfax.org.
isetsfax.org.           A       192.168.220.174
ns          IN          A       192.168.220.174
mail        IN          A       192.168.220.174
www     CNAME                   isetsfax.org.
```

Format d’un fichier de zone (Suite)

- **hostmaster.isetsfax.org** définit l’adresse mail de l’administrateur de la zone.

  L’adresse hostmaster est recommandée, mais n’importe quelle adresse mail valide peut être définie ici.

  Étant donné que le symbole @ a une signification spécifique dans le contexte, on utilise les points comme séparateurs, ce qui explique cette syntaxe « étrange ».

  L’adresse mail définie ici est donc **hostmaster@isetsfax.org**.
- **Serial** : 2024110818 définit le numéro de série associé à la zone.

  Par convention, on utilise le format AAAAMMJJSS.

  Le numéro de série doit impérativement être mis à jour à chaque fois que l’on modifie le domaine.
- **Refresh** contrôle la mise à jour des informations du serveur de noms esclave de la zone.

  Les valeurs typiques se situent entre 3 heures (10800) et 24 heures (86400).
- **Retry** définit le temps d’attente avant une deuxième tentative lorsque le serveur de noms esclave n’arrive pas à contacter le serveur maître pour rafraîchir les informations.

  Les valeurs typiques se situent entre 10 minutes (600) et 60 minutes (3600).
- **Expiry** définit le laps de temps au bout duquel les enregistrements de zone sont considérés comme ne faisant plus autorité.

  On choisit généralement une valeur assez élevée, située entre une semaine (604800) à trois semaines (1814400).
- **Minimum** définit le laps de temps durant lequel des réponses négatives (Réponse NXDOMAIN) peuvent être gardées en cache par le serveur de noms esclave.

  Cette valeur se situera entre 0 et 3 heures (10800).

Format des enregistrements des ressources

$ORIGIN isetsfax.org.

;nom ttl classe type ip

serveur1	IN.	**A**	**192.168.1.10**
mail	IN	**A**	**192.168.1.20**
	IN	**A**	**192.168.1.21**

Format des enregistrements des ressources (Suite)

- CNAME (*Canonical NAME) : l'enregistrement de type nom canonique (ou alias) permet* d'attribuer un deuxième nom au nom réel de l'hôte, qui peut être dans un autre domaine, selon le format « nom ttl IN CNAME nomRéelle ».

EXEMPLE

- L'exemple qui suit attribue les alias « www.isetsfax.org » et « pop3.isetsfax.org » à l'hôte « serveur1.isetsfax.org » et l'alias « ftp.isetsfax.org » à un hôte « serveur2.isetsfax.org »

$ORIGIN isetsfax.org.
;nom ttl classe type nomRéelle

www	IN	**CNAME**	**serveur1.isetsfax.org**
pop3	IN	**CNAME**	**serveur1.isetsfax.org**
ftp	IN	**CNAME**	**serveur2.isetsf.tn**

Format des enregistrements des ressources (Suite)

- MX (*Mail eXchange) : l'enregistrement de type MX spécifie les noms et les préférences des* serveurs de messagerie de la zone.
- Il est utilisé par les applications agents de messagerie (*mail agents) pour router les courriers électroniques du domaine. Le format de* l'enregistrement de type MX est : « nom ttl IN MX préférence nom ».

EXEMPLE

- D'après l'exemple qui suit, les courriers électroniques du domaine « isetsfax.org » sont routés vers l'hôte « mail.isetsfax.org ».
- Si ce dernier n'est pas disponible (arrêté, dérangé ou en panne) alors les courriers seront routés vers « mail2.isetsfax.org ».

$ORIGIN isetsfax.org.
;nom ttl classe type préfé. nom
IN **MX 20 mail ;forme courte**
; ceci est équivalent à
; isetsfax.org. IN **MX 10 mail.isetsfax.org.**
IN **MX 21 mail2.isetsfax.org.**

Format des enregistrements des ressources (Suite)

- NS (*Name Server) : l'enregistrement de type serveur de noms définit les serveurs de noms* autoritaires de la zone.
- En général, Il est situé juste après l'enregistrement SOA et il est utilisé aussi pour définir les délégations des sous domaines.
- Le format de l'enregistrement NS est : « nomDomaine ttl IN NS nom ».

EXEMPLE

- La configuration qui suit déclare les hôtes « dns.isetsfax.org » et « dns2.isetsfax.org » comme les serveurs DNS de la zone « isetsfax.org » et délègue la gestion du sous-domaine « sd.isetsfax.org » au serveur DNS « dns.sd.isetsfax.org ».

Format des enregistrements des ressources (Suite)

$ORIGIN isetsfax.org.
SOA ...
;nom ttl classe type nom
IN **NS** **dns.isetsfax.org.**
IN **NS** **dns2.isetsfax.org.**
dns IN A 192.168.1.1
dns2 IN A 192.168.1.2
;sd.isetsfax.org est un sous domaine isetsfax.org
$ORIGIN sd.isetsfax.org.
IN **NS** **dns.sd.isetsfax.org.**
...
dns IN A 192.168.2.1
;ou sans utiliser la directive $ORIGIN
;sd.isetsfax.org. IN **NS dns.sd.isetsfax.org.**
;dns.sd.isetsfax.org. IN A 192.168.2.1

Format des enregistrements des ressources (Suite)

- PTR (*PoinTeR) : l'enregistrement de type PTR sert à la résolution inversée des noms selon le* format : « nomARPA ttl IN PTR nom ».

EXEMPLE

- D'après l'exemple qui suit, l'adresse ip « 192.168.1.10 » sera retournée pour une recherche inversée pour l'hôte « serveur1.isetsfax.org ».

$ORIGIN 1.168.192.IN-ADDR.ARPA.

...

;nomARP A ttl classe type nom

10 IN PTR serveur1.isetsfax.org.

Commandes de diagnostique et de configuration

- Commande host
- Commande nslookup
- Commande dig
- Commande named-checkconf
- Commande named-check-zone
- Commande dnssec-keygen
- Commande dnssec-signzone