Jean Saquet – Université de Caen

Master 2 E-secure

Réseaux

DNS

Bureau S3-354
Mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M2/rezo

Domain Name System

Rappel : structure de noms de domaine hiérarchique en arbre (ex : info.unicaen.fr. , ibm.com., ...).
Indispensable à cause de la répartition des responsabilités.

IP ne fonctionne qu'avec des adresses.
==> nécessité de conversion nom --> adresses (et inv.)

La gestion de cette conversion est aussi répartie.

Resolver

Une application qui doit convertir un nom en adresse (ou inversement) fait un appel au resolver.
Ce dernier recherche l'information demandée :

- dans un fichier local (par ex. /etc/hosts)
- dans sa mémoire cache (si déjà résolu récemment)
- en faisant appel au service d'un serveur de noms (dont l'adresse est connue du système de la machine – dans le fichier /etc/resolv.conf par exemple)

Serveur de noms

Chaque domaine (ou sous, sous-sous, ... domaine) doit en posséder un (en fait deux, par sécurité).
Ce serveur contient les données concernant le domaine, sous la responsabilité de l'administrateur du domaine.
Il doit pouvoir être interrogé par tout resolver (donc par n'importe qui).

Le dialogue resolver / serveur utilise un protocole de niveau application spécifique.

Types de données

Resolver et serveur échangent donc des données relatives à un domaine. Les données sont organisées en "enregistrements" (Rrs=Ressource Records) comportant :

- un nom
- un type
- une classe
- une durée de vie
- une longueur de la partie données
- les données.

Ces enregistrements figurent dans la base de données des serveurs et peuvent être envoyés aux clients.

Le protocole du DNS

La plupart des requêtes / réponses utilisent UDP.
(le plus souvent, un seul datagramme)

Le port "bien connu" des serveurs est le 53 (décimal)

Les serveurs qui ne connaissent pas la réponse deviennent client d'un autre serveur de noms. Ils utilisent aussi le port 53 pour cela.

Le protocole permet également la mise à jour des données entre serveurs secondaires et primaire (en utilisant TCP à cause de la longueur).

Implémentation & détails

Un logiciel domine très largement : BIND
Simple au départ, assez complexe à présent.
Cause : NATs, vues internes / externes, ...

Bases de données dans fichiers textes :
Zone et Rev

Fichier de config named.conf pour déclarer les zones (direct, reverse; local, …)
Ajouter des zones dans named.conf.local

Zones

Zone pour conversion noms-->adresses (essentiellement)
ex info.unicaen.fr

Zone reverse v4 : xx.xx.in-addr.arpa
Zone reverse v6 : x.x.x.....x.ip6.arpa

Zone locale : localhost
Zone reverse locale v4 : 127.in-addr.arpa
Zone reverse locale v6 : 1.0....0.ip6.arpa

Zone "." (racine) de type hint pour récursion

Types et classes

Classe IN : internet

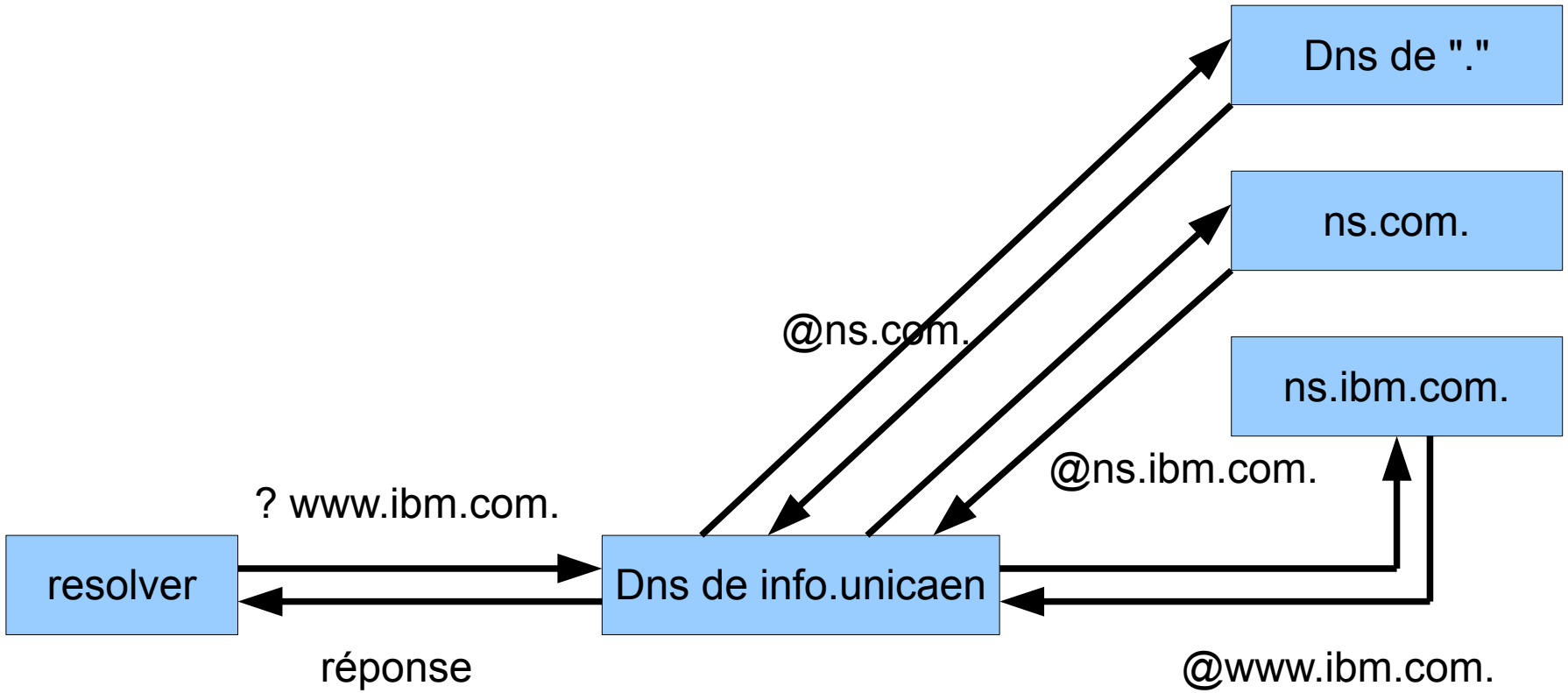
Principaux types:
A ou AAAA : adresses
PTR : pointeur (reverse)
NS : Name Servers
MX : Mail recorder
CNAME : aliases
INFO : information
TXT : texte
SOA : Start Of Authority

Fonctionnement

Le NS répond directement à toute question dont il connaît la réponse
Sinon, il recherche un serveur la connaissant,
en s'adressant d'abord à un serveur "racine" (zone ".") (comportement par défaut) ou à un autre serveur défini par un "forwarders".

Les serveurs racine sont déclarés dans un fichier spécifique, fourni avec la distribution, pouvant être mis à jour.

Fonctionnement (exemple)



Autres RRs

Position géographique (longitude, latitude, altitude)
Permet les traceroute graphiques

Divers essais plus ou moins obsolètes

en v6 : A6 et DNAME : définition "répartie" des adresses

Interrogations

Le plus souvent records A ou AAAA ou PTR

Mais aussi :
SOA (serveur ayant autorité sur le domaine)
MX (serveur mail du domaine)
NS (serveurs de noms du domaine)
CNAME (nom canonique)

Voir l'utilisation de Host ou Dig

UDP ou TCP ?

Le plus souvent UDP, mais :

Passage en TCP si réponse trop longue
exemple : liste d'une zone complète

Pas toujours autorisé par config DNS ou firewall

TCP utilisé pour communication serveur primaire / secondaire

Champ SOA

Définit :
Le serveur ayant autorité sur le domaine
L'adresse du "postmaster"
Des paramètres de temps pour la mise à jour des serveurs secondaires, et le TTL par défaut
Le numéro de version des données
(le plus souvent sous la forme YYYYMMJJVV)
Les timers pour maj secondaire/primaire

Champs courants

Nom class type donnée

Exemples :
www IN CNAME panoramix
panoramix IN A 193.55.128.30
info.unicaen.fr IN MX 10 averell
info.unicaen.fr IN NS calvin

Autres champs

Champs pour info, texte
Champs de localisation géographique → traceroute graphique
Champs pour déclaration de services → cf. DNS « distribué »
Champs relatifs à la sécurité (DNSSEC)

Compléments dans l'unité « Compléments routage et DNS »