DNS : résolution, autorité et diagnostic

Formation : BTS SIO — Option SISR

1. Rôle du DNS

Le DNS associe des noms à des informations : adresses IP, serveurs de messagerie ou services d'un domaine Active Directory. Une résolution réussie ne garantit pas que le service recherché fonctionne.

2. Résolveur et serveur faisant autorité

Rôle	Fonction
Résolveur récursif	Recherche la réponse pour le client et la conserve en cache selon le TTL.
Serveur faisant autorité	Publie les enregistrements des zones dont il est responsable.
Primaire	Héberge la version de référence d'une zone dans une organisation primaire/secondaire.
Secondaire	Reçoit une copie par transfert et peut répondre aux requêtes faisant autorité.

Serveur du laboratoire	Adresse	Fonction
dns0	192.168.3.10	Résolveur Unbound
dns1	192.168.3.11	Second résolveur
ns0.californie.cub.sioplc.fr	192.36.3.10	Primaire de la zone Californie
ns1.californie.cub.sioplc.fr	192.36.3.11	Secondaire de la zone Californie

Un secondaire peut répondre en même temps que le primaire ; son rôle ne consiste pas seulement à attendre une panne.

3. Enregistrements et cache

Type	Usage
A / AAAA	Adresse IPv4 / IPv6
CNAME	Alias vers un autre nom
NS	Serveur faisant autorité pour une zone
SOA	Paramètres de la zone, notamment son numéro de série
MX	Serveurs de messagerie et priorité
PTR	Résolution inverse
SRV	Localisation d'un service

Le TTL fixe la durée de conservation en cache. Une modification de zone peut donc ne pas être visible immédiatement par tous les clients.

4. Déroulement d'une résolution

Le client interroge son résolveur. Celui-ci répond depuis son cache ou recherche les données selon sa configuration. En résolution itérative, il suit les délégations jusqu'aux serveurs responsables du nom.

```
Racine → fr → sioplc.fr → cub.sioplc.fr → californie.cub.sioplc.fr
```

Les NS de la zone parente désignent les serveurs de la zone déléguée. Lorsque leurs noms se trouvent dans cette zone, des adresses de raccordement (glue records) permettent d'éviter une dépendance circulaire.

5. Interroger avec dig

```
# Résolveur explicite
dig @192.168.3.10 google.fr A
# Autorité, sans demander de récursion
dig @192.36.3.11 californie.cub.sioplc.fr SOA +norecurse
dig @192.36.3.11 californie.cub.sioplc.fr NS +norecurse
# Vérification du transport TCP
dig @192.168.3.10 google.fr A +tcp
# Résolution inverse
dig @192.168.3.10 -x 8.8.8.8
```

Le DNS utilise UDP et TCP 53. Tester un transport ne valide pas l'autre. `dig A 8.8.8.8` demande un A pour le nom littéral `8.8.8.8.` ; cette commande ne réalise pas une résolution inverse.

6. Lire la réponse

Élément	Signification
NOERROR	Pas d'erreur DNS ; le type demandé peut toutefois être absent.
NXDOMAIN	Nom inexistant
SERVFAIL	Échec de traitement
REFUSED	Requête refusée
aa	Réponse faisant autorité
rd / ra	Récursion demandée / disponible
ad	Données annoncées comme authentifiées selon la politique du résolveur

Contrôler également SERVER, ANSWER SECTION, AUTHORITY SECTION, le TTL et Query time. Une réponse rapide peut venir du cache et ne prouve pas un échange récent avec la racine.

7. Suivre les délégations

```
dig +trace ns0.californie.cub.sioplc.fr
```

Avec `+trace`, dig interroge lui-même les serveurs successifs. Il ne s'agit pas d'une unique résolution récursive confiée à Unbound. La présence de DS, RRSIG ou NSEC3 ne suffit pas à démontrer une validation DNSSEC complète.

8. Diagnostic et continuité

Symptôme	**Contrôles**
Aucune réponse	Serveur interrogé, routage, écoute et filtrage UDP/TCP 53
SERVFAIL	Journaux, délégation, accès amont, heure et DNSSEC
REFUSED	Politique de récursion et réseaux autorisés
Ancienne adresse	TTL, cache client et cache résolveur
Primaire et secondaire différents	Séries SOA et transfert de zone
DNS correct, service inaccessible	Port applicatif, service, filtrage et NAT

Un test de basculement doit identifier le système client, le serveur arrêté et les délais observés. La présence de deux résolveurs ne garantit pas un comportement identique sur tous les clients.

9. Procédures associées

- Configurer et diagnostiquer Unbound
- BIND9 : zones, délégation et transferts

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:services:dns

Last update: **2026/10/18 01:23**