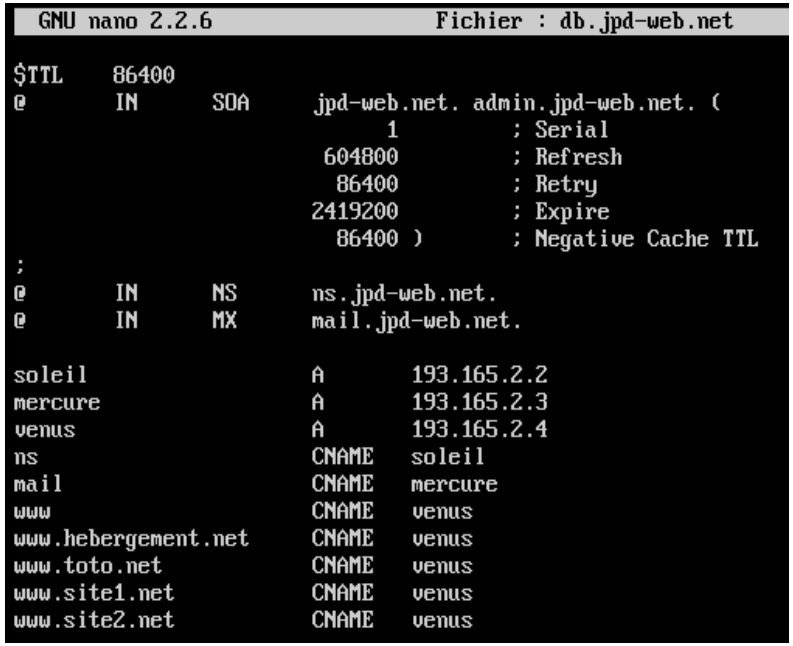
420-W45-SF Installation de serveurs et de services

Claude Roy et Jean-Pierre Duchesneau
DNS

Pourquoi étudier le DNS

- Tous notre travail DevSecOps utilise un service DNS
- Nous devons faire correspondent les bons types d'enregistrement : SOA, NS, MX, A, AAA, SRV, etc.
- Le cas des serveurs Apaches avec les vhost.
  - Un adresse IP plusieurs enregistrement.



Fonctionnement de base

- Base de données distribuée.
- Un site stocke les données des ordinateurs qu'il connaît.
- Un autre site stocke les données de son propre ensemble d'ordinateurs.
- Les sites coopèrent et partagent des données lorsqu'un site a besoin de rechercher les données de l'autre.
- D'un point de vue administratif, les serveurs DNS que vous avez configurés pour votre domaine répondent aux requêtes du monde extérieur sur les noms de votre domaine; ils interrogent également les serveurs d'autres domaines au nom de vos utilisateurs.

Requêtes

- Une requête DNS se compose d'un nom et d'un type d'enregistrement.
- La réponse renvoyée est un ensemble «d'enregistrements de ressources» (RR) qui répondent à la requête (ou, en variante, une réponse indiquant que le nom et le type d'enregistrement que vous avez demandé n'existent pas).
- La requête la plus courante concerne un enregistrement A, qui renvoie l'adresse IP associée à un nom.

Évolution

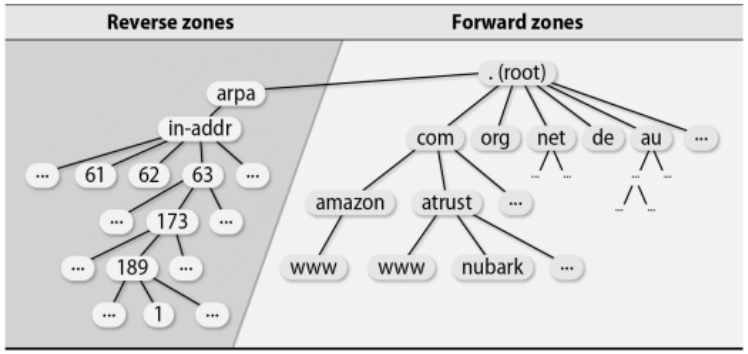
- Chacun maintenait un serveur DNS pour son organisation.
- Aujourd'hui, si une organisation gère un serveur DNS, il est souvent réservé à un usage interne.
- Il est désormais courant d’utiliser l’un des nombreux fournisseurs DNS commerciaux pour le DNS public.

Lookup/recherche

- Pour faire une association nom de domaine adresse IP, vous devez configurer vos systèmes en tant que clients DNS.
- Fichiers pour le DNS
  - Statique : /etc/hosts.
  - Serveurs DNS : /etc/systemd/resolved.conf

Résolution

- L'espace de noms DNS est organisé en une arborescence qui contient à la fois des mappages directs et des mappages inverses.
- Nom -> IP
- IP -> Nom



Serveur de nom (NS)

- Un serveur de noms effectue plusieurs tâches:
  - Il répond aux questions sur les noms d'hôte et les adresses IP de votre site.
  - Il pose des questions sur les hôtes locaux et distants au nom de vos utilisateurs.
  - Il met en cache les réponses aux requêtes afin de pouvoir répondre plus rapidement la prochaine fois.
  - Il communique avec d'autres serveurs de noms locaux pour maintenir la synchronisation des données DNS.

Zones

- Les serveurs de noms traitent des «zones», où une zone est essentiellement un domaine moins ses sous-domaines.
- Vous verrez souvent le terme «domaine» utilisé là où une zone est ce que l'on entend réellement.

Modes

Type of server	Description
authoritative	Officially represents a zone
master	The master server for a zone; gets its data from a disk file
primary	Another name for the master server
slave	Copies its data from the master
secondary	Another name for a slave server
stub	Like a slave, but copies only name server data (not host data)
distribution	A server advertised only within a domain (aka "stealth server")
nonauthoritative [a]	Answers a query from cache; doesn't know if the data is still valid
caching	Caches data from previous queries; usually has no local zones
forwarder	Performs queries on behalf of many clients; builds a large cache
recursive	Queries on your behalf until it returns either an answer or an error
nonrecursive	Refers you to another server if it can't answer a query

a. Strictly speaking, "nonauthoritative" is an attribute of a DNS query response, not a server.

Enregistrements

- Chaque site gère un ou plusieurs éléments de la base de données distribuée.
- Votre partie de la BD se compose de fichiers texte contenant des enregistrements pour chacun de vos hôtes; «enregistrements de ressources».

Enregistrements

- Chaque enregistrement est une seule ligne composée d'un nom (généralement un nom d'hôte), d'un type d'enregistrement et de certaines valeurs de données. Le champ de nom peut être omis si sa valeur est la même que celle de la ligne précédente.

Enregistrements - exemple

- Fichier “forward” monsite.com

```
www             IN   A   63.173.189.1
                IN   MX 10 mailserver.monsite.com
```

- Fichier “reverse” 63.173.189.rev

```
1               IN   PTR   www.monsite.com
```

Types d'enregistrements

	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone
	NS	Name Server	Identifies servers, delegates subdomains
Basics	A	IPv4 Address	Name-to-address translation
	AAAA	IPv6 Address	Name-to-IPv6-address translation
	PTR	Pointer	Address-to-name translation
	MX	Mail Exchanger	Controls email routing
Security	DS	Delegation Signer	Hash of signed child zone's key-signing key
	DNSKEY	Public Key	Public key for a DNS name
	NSEC	Next Secure	Used with DNSSEC for negative answers
	NSEC3	Next Secure v3	Used with DNSSEC for negative answers
	RRSIG	Signature	Signed, authenticated resource record set
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	SRV	Service	Gives locations of a well-known service
	TXT	Text	Comments or untyped information

Comment le DNS fonctionne

- https://howdns.works/

Référence

- UNIX and Linux System Administration Handbook (5th Ed), Addison-Wesley.