Engineer

DNS

annuaire qui transforme un nom en adresse

Ce que c’est

Le DNS, Domain Name System, est l’annuaire distribué qu’Internet consulte avant presque toute autre opération. Un programme disposant d’un nom comme `example.com` lui demande l’adresse à laquelle se connecter. Le même système répond à quelques autres questions sur ce nom : quels serveurs acceptent son courrier, quel texte son propriétaire a publié et quels serveurs en ont la responsabilité.

Cet annuaire forme un arbre lu de droite à gauche. La racine est au sommet ; en dessous se trouvent les domaines de premier niveau comme `.com` ou `.dk`, puis les domaines enregistrés et enfin les sous-domaines créés par leurs propriétaires. Aucun serveur ne contient tout l’arbre. Chaque niveau délègue le suivant à des serveurs désignés. La partie pour laquelle un ensemble de serveurs fait autorité s’appelle une zone. Qui contrôle une zone décide vers quoi ses noms sont résolus.

Deux types de serveurs font le travail. Les serveurs faisant autorité conservent une zone et donnent la réponse de référence. Les résolveurs récursifs, exploités par des fournisseurs d’accès, des entreprises ou des services accessibles au public, parcourent l’arbre pour le client : ils demandent à une racine où se trouve `.com`, à `.com` où se trouve `example.com`, puis aux serveurs de ce domaine l’enregistrement, avant de rendre la réponse. Votre système d’exploitation n’exécute qu’un petit résolveur minimal, ou stub resolver, qui transmet la question à un résolveur récursif et attend.

Les réponses sont des enregistrements typés. Le fichier de zone est leur forme d’écriture classique :

```
$ORIGIN example.com.
$TTL 3600
@     IN  SOA    ns1.example.net. hostmaster.example.com. (
                 2026101701 7200 900 1209600 300 )
@     IN  NS     ns1.example.net.
@     IN  A      192.0.2.10
@     IN  AAAA   2001:db8::10
www   IN  CNAME  example.com.
@     IN  MX     10 mail.example.net.
@     IN  TXT    "v=spf1 include:_spf.example.net -all"
```

`A` et `AAAA` donnent les adresses IPv4 et IPv6. `CNAME` fait d'un nom l'alias d'un autre. `MX` nomme le serveur qui reçoit le courrier, et `TXT` transporte du texte libre : en pratique, des politiques d'authentification du courrier et des preuves de contrôle du domaine. `NS` et `SOA` décrivent la zone elle-même.

Chaque enregistrement porte une durée de vie, ici 3 600 secondes, qui détermine le comportement du DNS. Un résolveur ayant obtenu une réponse peut la réutiliser jusqu'à l'expiration de son TTL, sans redemander. Le système répond donc à la plupart des recherches depuis un cache proche du client et continue lorsqu'un serveur faisant autorité est brièvement inaccessible. La contrepartie est que personne ne peut forcer le monde à oublier plus tôt une ancienne réponse.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que le DNS ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Du Wi-Fi, des pare-feu et des accès à distance configurés pour travailler de partout, en laissant entrer uniquement les personnes autorisées.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 30 instances VPS Ubuntu Linux administrées — 30 serveurs Linux gérés, avec récupération prévue

30 instances VPS Ubuntu Linux administrées Contactez-nous →

Pourquoi c'est important

Toute connexion à un service nommé commence par une recherche. Si le DNS fournit des informations erronées, les serveurs peuvent être en parfaite santé et le site, l'API et la messagerie sembler pourtant arrêtés, puisque rien ne les atteint. Quand il est correct, personne ne le remarque ; il est donc souvent la partie la moins documentée du système.

Le DNS permet aussi d'exercer et de prouver le contrôle d'un domaine. Les fournisseurs de messagerie lisent les politiques SPF, DKIM et DMARC dans les enregistrements `TXT` pour décider si un message prétendant venir de votre domaine est authentique. Un enregistrement erroné ou manquant envoie donc du vrai courrier dans les indésirables. Les autorités de certification et les services hébergés demandent un enregistrement avec une valeur précise pour prouver que le nom vous appartient. Toute personne capable de modifier la zone peut rediriger le site, intercepter le courrier et obtenir des certificats pour le domaine. L'accès au compte DNS est donc aussi sensible que celui aux serveurs.

Le cache façonne chaque modification. Ce qu'on appelle propagation correspond en réalité à des milliers de résolveurs attendant chacun l'expiration de leur copie. Pour déplacer un site avec peu de perturbations, réduisez le TTL environ une journée avant, attendez l'écoulement de l'ancien TTL, effectuez le changement et relevez le TTL après stabilisation.

Le DNS classique circule en clair ; ni les réponses ni les questions ne sont confidentielles. DNSSEC permet au résolveur de vérifier qu'une réponse vient réellement du propriétaire de la zone et n'a pas été altérée, mais sa propre spécification précise qu'il n'ajoute aucune confidentialité. Les transports chiffrés comme DNS sur HTTPS cachent les questions au réseau traversé. Le résolveur à l'autre bout voit néanmoins chaque nom demandé. Choisir un résolveur revient à choisir qui reçoit cette liste.

À quoi cela ressemble en pratique

La zone de l'entreprise illustre le point de départ courant et une façon d'en sortir. Elle contenait une vingtaine d'enregistrements gérés dans la console web d'un fournisseur : présence web, sous-domaine git, deux redirections personnelles, courrier acheminé par un fournisseur de boîtes hébergées, domaine d'envoi transactionnel et authentification des deux usages de messagerie. Dans une console, l'état actuel est ce qu'a laissé la dernière personne à cliquer. La zone est désormais constituée de données dans un dépôt : enregistrements actifs, applicatifs, de politique de transport et liste séparée des suppressions prévues. Un play réconcilie cette déclaration avec l'API du fournisseur. Deux autres points d'entrée exigent des tags dont l'activation est explicite : un audit qui indique les écarts sans rien modifier et un export qui écrit la zone au format standard des fichiers de zone, pour qu'un autre outil que le dépôt puisse la lire. L'audit est le plus utilisé : on cherche plus souvent à connaître l'écart qu'à le résorber.

Le rôle du même fournisseur est volontairement étroit. La page des crédits explique que Cloudflare assure uniquement le DNS du site, sans proxy devant celui-ci. Elle publie sans détour l'adresse du serveur, puisque le DNS la fournit déjà à quiconque la demande.

La lecture du DNS fait aussi partie de la description courante du parc. Parmi les sept rôles de rapport en lecture seule qui décrivent l'hôte actif en Markdown figure un inventaire fournisseur lisant le DNS avec deux API cloud et une API de serveur dédié. La règle est qu'aucun rapport ne publie un nombre que son exécution n'a pas mesuré.

Où les problèmes surviennent

Les pannes DNS sont souvent retardées, mises en cache ou différentes selon le point de vue : le même nom fonctionne pour une personne et échoue pour une autre. Voici les cas récurrents.

Une modification refuse de s'appliquer. Quelqu'un modifie un enregistrement au TTL d'une journée et attend la nouvelle adresse immédiatement. Mais les résolveurs ayant l'ancienne réponse la servent jusqu'à l'expiration de leur copie. Une variante plus discrète touche les nouveaux noms : si un nom a été demandé avant la création de son enregistrement, la réponse négative est elle aussi mise en cache, pour la durée permise par le `SOA` de la zone (RFC 2308). Réduisez les TTL avant les changements prévus et créez les enregistrements avant toute requête.

Un alias est placé là où il ne peut l'être. La RFC 1034 dit qu'un nom portant un `CNAME` ne peut contenir aucune autre donnée. Le domaine nu, `example.com` lui-même, possède toujours des enregistrements `SOA` et `NS`. Une zone conforme ne peut donc faire du sommet un alias ; un `CNAME` sur un sous-domaine exigeant aussi des `MX` ou `TXT` enfreint la même règle. Les fournisseurs proposent leurs propres contournements, par aplatissement ou enregistrements `ALIAS`. Chacun se comporte un peu autrement ; lisez ce que le vôtre sert réellement.

L'authentification du courrier bascule en erreur. Chaque `include` d'un enregistrement SPF entraîne des recherches DNS, dont la RFC 7208 limite le total à dix. Ajouter un service d'infolettre ou de gestion de tickets peut dépasser ce plafond. Les destinataires traitent alors la politique comme une erreur permanente ; le courrier qu'elle devait authentifier est évalué sans elle. Comptez les recherches à chaque ajout d'expéditeur.

Un enregistrement survit à sa cible. Un sous-domaine pointe par `CNAME` vers un bucket de stockage cloud ou une application hébergée supprimée depuis. Si le fournisseur permet à quiconque de revendiquer ce nom de ressource, un tiers peut le prendre et publier son contenu sous votre sous-domaine, avec la réputation de votre domaine. Supprimez l'enregistrement en même temps que sa cible, dans la même modification.

La zone n'existe que dans une console. Sans historique, revue ni différence consultable, la suppression accidentelle du `MX` n'est découverte qu'à l'arrêt du courrier, et sa valeur précédente doit être reconstruite de mémoire. Exporter régulièrement la zone, ou mieux la déclarer sous forme de code, donne à chaque changement une trace et un chemin de retour.

Pour aller plus loin

- RFC 1035 : noms de domaine, implémentation et spécification — formats d'enregistrements, syntaxe des fichiers de zone et protocole sur le réseau.
- RFC 1034 : noms de domaine, concepts et fonctionnalités — arbre, zones, délégation et parcours des résolveurs.
- RFC 9499 : terminologie DNS — des définitions précises des mots employés ici.
- RFC 2308 : mise en cache négative des requêtes DNS — la durée pendant laquelle un résolveur peut retenir qu'un nom n'existe pas.
- RFC 4033 : introduction et exigences de sécurité DNS — les protections de DNSSEC et leurs limites.
- RFC 8484 : requêtes DNS sur HTTPS — transporter les recherches dans du trafic web chiffré ordinaire.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que le DNS ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/dns/