Engineer

CDN

des serveurs proches du lecteur qui distribuent des copies

Ce que c’est

Un CDN, réseau de diffusion de contenu, est un ensemble de serveurs répartis dans de nombreuses villes. Il s’interpose entre les lecteurs et le serveur sur lequel le site fonctionne réellement, appelé origine, puis distribue des copies de ce que cette origine publie. Un lecteur à Sydney demandant une page dont l’origine se trouve à Toronto la reçoit d’une machine à Sydney ou à proximité. La requête peut ainsi ne jamais traverser le Pacifique.

Deux mécanismes dirigent chaque lecteur vers un serveur proche. Certains réseaux donnent une réponse DNS différente selon la provenance de la question. D’autres annoncent la même adresse IP depuis chaque emplacement et laissent le routage Internet conduire chaque paquet vers l’emplacement le plus proche. Dans les deux cas, le serveur qui répond assure généralement la terminaison TLS pour le site. Il détient donc un certificat du domaine et lit chaque requête en clair avant de décider quoi en faire.

La suite relève du rôle d’un cache partagé. S’il possède déjà une copie fraîche, il répond immédiatement : c’est un succès de cache. Sinon, il récupère la réponse auprès de l’origine, en garde une copie et répond : c’est un défaut de cache. L’origine décide de la durée pendant laquelle une copie est fraîche, au moyen d’en-têtes de réponse définis par la norme de mise en cache HTTP :

```
# A fingerprinted stylesheet: never changes under this name.
Cache-Control: public, max-age=31536000, immutable

# A page: browsers check back each time, the CDN keeps it ten minutes.
Cache-Control: no-cache
CDN-Cache-Control: max-age=600
```

```
# An account page: no cache may keep a copy.
Cache-Control: private, no-store
```

`max-age` donne une durée de vie en secondes. `immutable` indique au navigateur de ne pas revalider pendant cette période. `no-cache` permet de stocker une réponse, mais impose une vérification auprès de l'origine avant sa réutilisation, tandis que `private` l'exclut entièrement des caches partagés. Seuls les CDN lisent `CDN-Cache-Control` . Un site peut donc autoriser les serveurs périphériques à conserver une page plus longtemps que les navigateurs.

Le même mécanisme transporte désormais bien plus que des fichiers statiques. La plupart des CDN transmettent aussi à l'origine les requêtes non stockables en cache, absorbent des afflux de trafic hostile et exécutent de petits programmes en périphérie. Le terme couvre donc une large gamme de services partant tous de la même idée : servir des copies près du lecteur.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un CDN ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des serveurs dimensionnés selon vos usages réels, migrés vers le cloud ou hors du cloud, avec une estimation préalable de la facture mensuelle.

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. 20 applications Docker sur Google Cloud et AWS — 20 applications conteneurisées déployées et surveillées

20 applications Docker sur Google Cloud et AWS Contactez-nous →

Pourquoi c'est important

La distance coûte un temps qu'aucune optimisation de serveur ne peut récupérer. La lumière dans une fibre parcourt environ deux cents kilomètres par milliseconde. Un aller-retour entre l'Europe et l'Australie prend donc largement plus de cent millisecondes avant le moindre travail d'un serveur. Une nouvelle connexion sécurisée consomme encore un ou deux de ces allers-retours avant l'envoi de la première requête. Servir une copie proche supprime l'essentiel de cette attente pour chaque lecteur éloigné de l'origine.

La charge est la deuxième raison. Lorsque la plupart des requêtes trouvent leur réponse dans le cache, l'origine ne voit qu'une petite part du trafic. Une hausse soudaine arrive alors sur un réseau construit pour les pics plutôt que sur une

seule machine. Avec `stale-if-error`, les serveurs périphériques peuvent continuer à servir la dernière copie valide lorsque l'origine est indisponible. Une brève panne reste donc invisible pour de nombreux lecteurs.

Le coût est moins visible que la facture. Un CDN devant un site place une autre entreprise au milieu de chaque visite. Elle voit l'adresse IP de chaque lecteur, chaque URL demandée et, puisqu'elle assure la terminaison TLS, le contenu de l'échange. Elle traite le tout selon sa propre politique. C'est aussi une dépendance partagée : lorsqu'un grand fournisseur passe une mauvaise heure, des milliers de sites sans lien entre eux la passent ensemble.

L'ancien argument en faveur du chargement de bibliothèques et de polices depuis un CDN public populaire s'est lui aussi affaibli. Les navigateurs gardent désormais un cache séparé par site. Un fichier récupéré pour un site l'est donc à nouveau pour le suivant, et la copie partagée ajoute une requête vers un tiers sans bénéfice de cache en contrepartie.

Un site dont les lecteurs sont surtout dans une région, servi par une machine rapide dans cette région, peut simplement ne pas avoir besoin de CDN. Un site avec un public mondial, des médias lourds ou du trafic arrivant par vagues en a généralement besoin.

À quoi cela ressemble en pratique

Sur ce site, l'essai d'un CDN puis sa désactivation ont tranché la question. Le travail DNS de l'entreprise indique que le passage des deux façades Web par le réseau de contenu du fournisseur a été mis en place, a fonctionné, puis a été désactivé. Avec ce mandataire en place, une autre entreprise traitait l'adresse de chaque visiteur et chaque URL demandée avant le site et selon sa propre politique plutôt que celle du site. Pour une entreprise qui se distingue en affirmant que personne ne surveille, la page juge ce compromis plus défavorable que les attaques contre lesquelles le mandataire protège. Le raisonnement est consigné pour que personne ne rouvre la question par accident.

La même position apparaît dans ce que chargent les pages. La page des crédits nomme les cinq types de fichiers qui atteignent le navigateur d'un lecteur et explique pourquoi les polices viennent de la machine du site : une police Web provenant du CDN d'autrui est un tiers qui vous regarde lire. Cloudflare répond

aux requêtes DNS du site et ne fait rien de plus. Le site ne passe délibérément pas par son mandataire, et un lecteur ouvrant le panneau réseau du navigateur compte un seul hôte.

Lorsque le CDN se justifie, les notes le disent. La note sur les ventes éclair soutient que refuser un acheteur doit être l'action la moins chère du système. Avec un million d'acheteurs et dix mille unités, 990 000 requêtes doivent échouer. Parmi les moyens cités pour les écarter tôt figurent une salle d'attente, un sas dimensionné selon le stock, une limite de débit par compte et un indicateur `sold_out` que le CDN distribue sans consulter quoi que ce soit derrière lui. Son conseil sur les tests de charge exprime la même idée depuis l'autre côté : lorsque le parcours de rupture de stock représente 99 % du trafic, ce trafic doit rester en périphérie.

Où les problèmes surviennent

Les serveurs périphériques font exactement ce que disent les en-têtes et leur configuration, ce qui n'est pas toujours ce qui était voulu.

- La page d'une autre personne est servie au visiteur suivant. Une réponse affichant un compte, un panier ou une salutation est mise en cache parce que rien ne l'a marquée comme privée. Déposer un cookie n'empêche pas la mise en cache, comme le précise la norme HTTP de mise en cache. Le lecteur suivant reçoit donc la page du premier. Marquez chaque réponse propre à un utilisateur `private` ou `no-store` et demandez au CDN de contourner son cache en présence d'un cookie de session.
- Un déploiement dépend d'une purge. Le nouveau HTML est publié alors que certains serveurs périphériques gardent l'ancienne feuille de style, ou l'inverse. Les pages s'affichent mal jusqu'à l'expiration de toutes les copies. Les purges prennent du temps pour atteindre chaque emplacement et varient selon les fournisseurs. Placez un hachage du contenu dans le nom de chaque fichier de ressource, mettez ces fichiers en cache pour un an avec `immutable` et gardez une durée de vie courte pour le seul HTML.
- La clé du cache est fausse dans un sens ou dans l'autre. Des paramètres de suivi comme `utm_source` transforment chaque lien partagé en une entrée de cache distincte, et le taux de succès s'effondre. Omettre un en-tête qui modifie la réponse, comme `Accept-Language`, conduit à servir la langue d'un lecteur à tout le monde. Retirez les paramètres ignorés par l'origine et nommez dans `Vary` les en-têtes qu'elle lit.

- Un objet populaire expire et l'origine est submergée. Des milliers de lecteurs ne trouvent pas l'entrée au même instant, et chacune de ces requêtes passe jusqu'à l'origine. Le regroupement des requêtes au CDN et `stale-while-revalidate`, qui sert l'ancienne copie pendant qu'une seule requête récupère la nouvelle, maintiennent la charge de l'origine à un niveau constant.
- L'origine répond à quiconque la trouve. La protection en périphérie importe peu si des attaquants peuvent atteindre directement son adresse. D'anciens enregistrements DNS, des en-têtes de courriel ou un sous-domaine oublié la révèlent souvent. N'acceptez de trafic à l'origine que depuis le CDN, au moyen d'une plage réseau ou d'une connexion authentifiée.

Pour aller plus loin

- RFC 6707, section 1.1 : terminologie CDN — les définitions IETF d'un CDN, de ses serveurs de substitution et du routage des requêtes.
- RFC 9111 : mise en cache HTTP — ce que les caches partagés peuvent stocker, pour combien de temps et le sens de `private`.
- RFC 9213 : contrôle ciblé de la mise en cache HTTP — le champ `CDN-Cache-Control`, qui ne s'adresse qu'aux CDN.
- RFC 5861 : extensions HTTP de Cache-Control pour le contenu périmé — `stale-while-revalidate` et `stale-if-error`.
- RFC 8246 : réponses HTTP immuables — la manière dont un fichier portant une empreinte évite une nouvelle vérification.

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 qu'un CDN ? » 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/cdn/