Engineer

CDN

ein Servernetz nahe am Leser, das Kopien ausliefert

Was es ist

Ein CDN, ein Content Delivery Network, ist ein über viele Städte verteilter Serververbund. Er steht zwischen Lesern und dem Server, auf dem eine Website tatsächlich läuft, dem Ursprungsserver, und liefert Kopien seiner Veröffentlichungen aus. Fragt ein Leser in Sydney nach einer Seite mit Ursprung in Toronto, erhält er sie von einer Maschine in oder nahe Sydney. Die Anfrage muss den Pazifik womöglich überhaupt nicht überqueren.

Zwei Mechanismen führen jeden Leser zu einem nahen Server. Manche Netze geben je nach Herkunft der Anfrage eine andere DNS-Antwort. Andere kündigen an jedem Standort dieselbe IP-Adresse an und überlassen es dem Internetrouting, jedes Paket zum nächstgelegenen Standort zu leiten. In beiden Fällen terminiert der antwortende Server meist TLS im Auftrag der Website. Er hält also ein Zertifikat für die Domain und liest jede Anfrage im Klartext, bevor er über das weitere Vorgehen entscheidet.

Was danach geschieht, ist die Aufgabe eines gemeinsamen Caches. Hält er bereits eine frische Kopie, antwortet er sofort: ein Treffer. Andernfalls ruft er die Antwort vom Ursprungsserver ab, behält eine Kopie und antwortet: ein Fehlzugriff. Wie lange eine Kopie als frisch gilt, entscheidet der Ursprungsserver mit den Antwortheadern, die der HTTP-Caching-Standard definiert:

```
# 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` nennt die Lebensdauer in Sekunden. `immutable` sagt dem Browser, während dieser Zeit nicht neu zu validieren. `no-cache` erlaubt einem Cache, eine Antwort zu speichern, verlangt aber vor ihrer Wiederverwendung eine Prüfung beim Ursprungsserver. `private` hält sie vollständig aus gemeinsamen Caches heraus. `CDN-Cache-Control` wird nur von CDNs gelesen. Eine Website kann die Kopie am Netzrand deshalb länger behalten lassen als in Browsern.

Derselbe Mechanismus trägt inzwischen weit mehr als statische Dateien. Die meisten CDNs leiten auch nicht cachebare Anfragen als Proxy zum Ursprungsserver weiter, fangen Fluten feindlichen Verkehrs ab und führen kleine Programme am Netzrand aus. Der Begriff umfasst deshalb ein breites Leistungsspektrum, das stets mit derselben Idee beginnt: Kopien nahe am Leser ausliefern.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ein CDN?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Server werden nach dem tatsächlichen Bedarf dimensioniert und in die Cloud oder aus ihr heraus verlagert — die monatlichen Kosten stehen vorher fest.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 20 Docker-Apps auf Google Cloud und AWS betrieben — 20 bereitgestellte und überwachte Containeranwendungen

20 Docker-Apps auf Google Cloud und AWS betrieben Kontakt aufnehmen →

Warum es wichtig ist

Entfernung kostet Zeit, die sich durch keine Serveroptimierung zurückholen lässt. Licht in Glasfaser legt ungefähr zweihundert Kilometer pro Millisekunde zurück. Ein Netzwerkumlauf zwischen Europa und Australien dauert deshalb deutlich über hundert Millisekunden, bevor ein Server überhaupt gearbeitet hat. Eine neue sichere Verbindung benötigt einen oder zwei dieser Umläufe, bevor die erste Anfrage gesendet wird. Eine nahe Kopie beseitigt den größten Teil dieser Wartezeit für jeden weit vom Ursprung entfernten Leser.

Last ist der zweite Grund. Sind die meisten Anfragen Treffer, sieht der Ursprungsserver nur einen kleinen Verkehrsanteil. Eine plötzliche Spitze trifft ein dafür gebautes Netzwerk statt eine einzelne Maschine. Mit `stale-if-error` kann der Netzrand die letzte gültige Kopie weiter ausliefern, während der Ursprungsserver ausgefallen ist. Ein kurzer Ausfall bleibt so für viele Leser unsichtbar.

Die Kosten sind weniger offensichtlich als die Rechnung. Ein CDN vor einer Website ist ein weiteres Unternehmen mitten in jedem Besuch. Es sieht die IP-Adresse jedes Lesers, jede angeforderte URL und wegen der TLS-Terminierung auch den Inhalt des Austauschs. Es verarbeitet alles nach seinen eigenen Regeln. Außerdem entsteht eine gemeinsame Abhängigkeit: Hat ein großer Anbieter eine schlechte Stunde, haben Tausende voneinander unabhängiger Websites sie gemeinsam.

Auch das frühere Argument, Bibliotheken und Schriften von einem beliebten öffentlichen CDN zu laden, ist schwächer geworden. Browser halten inzwischen für jede Website einen getrennten Cache. Eine für eine Website abgerufene Datei wird bei der nächsten erneut abgerufen. Die gemeinsame Kopie verursacht somit eine Drittanbieteranfrage ohne entsprechenden Cache-Vorteil.

Eine Website, deren Leser überwiegend in einer Region sitzen und die von einer schnellen Maschine in dieser Region bedient wird, braucht möglicherweise einfach kein CDN. Eine Website mit weltweitem Publikum, umfangreichen Medien oder stoßweise eintreffendem Verkehr braucht meist eines.

Wie es in der Praxis aussieht

Auf dieser Website wurde die CDN-Frage durch Ausprobieren und Abschalten entschieden. Die DNS-Arbeit des Unternehmens hält fest, dass die beiden Webauftritte über das Inhaltsnetz des Anbieters geleitet wurden: Die Lösung wurde gebaut, funktionierte und wurde anschließend wieder abgeschaltet. Mit dem Proxy verarbeitete ein anderes Unternehmen die Adresse jedes Besuchers und jede angeforderte URL, noch vor dieser Website und nach seinen eigenen Regeln statt denen dieser Website. Für ein Unternehmen, dessen besonderes Versprechen lautet, dass niemand zusieht, ist dieser Kompromiss nach Einschätzung der Seite nachteiliger als die Angriffe, vor denen der Proxy schützt. Die Begründung ist aufgeschrieben, damit niemand die Frage versehentlich neu aufrollt.

Dieselbe Haltung zeigt sich daran, was die Seiten laden. Die Credits-Seite nennt die fünf Dateiarten, die im Browser eines Lesers ankommen, und erklärt, warum die Schriften von der eigenen Maschine der Website stammen: Eine Webschrift aus dem CDN eines anderen ist ein Dritter, der beim Lesen zusieht. Cloudflare beantwortet die DNS-Anfragen der Website und tut nichts weiter. Die Website wird bewusst nicht über einen Proxy geleitet. Wer das Netzwerkpanel des Browsers öffnet, zählt einen Host.

Wo ein CDN seinen Platz verdient, sagen es die Notizen. Die Notiz über Blitzverkäufe argumentiert, dass das Abweisen eines Käufers der günstigste Vorgang im System sein muss. Bei einer Million Käufern und zehntausend Einheiten müssen 990.000 Anfragen scheitern. Als Möglichkeiten, sie früh abzufangen, nennt sie einen Warteraum, eine dem Bestand entsprechend dimensionierte Zugangsschranke, ein Anfragelimit pro Konto und ein `sold_out`-Flag, das das CDN ohne Nachfrage bei den dahinterliegenden Komponenten ausliefert. Ihr Rat zu Lasttests macht denselben Punkt von der anderen Seite: Wenn der Pfad für den Fall „ausverkauft“ 99 % des Verkehrs ausmacht, gehört dieser Verkehr an den Netzrand.

Wo es schiefgeht

Der Netzrand tut genau das, was Header und Konfiguration vorgeben. Das ist nicht immer das Gemeinte.

- Die nächste Person erhält die Seite einer anderen. Eine Antwort mit Konto, Warenkorb oder Begrüßung wird gecacht, weil sie niemand als privat markiert hat. Ein gesetztes Cookie verhindert Caching nicht, wie der HTTP-Caching-Standard festhält. Der nächste Leser erhält deshalb die Seite des ersten. Markieren Sie jede nutzerbezogene Antwort als `private` oder `no-store` und weisen Sie das CDN an, seinen Cache bei einem vorhandenen Sitzungscookie zu umgehen.
- Eine Bereitstellung hängt von einer Cache-Löschung ab. Neues HTML geht live, während manche Netzstandorte noch das alte Stylesheet halten, oder umgekehrt. Seiten erscheinen beschädigt, bis jede Kopie abläuft. Löschungen brauchen Zeit, um alle Standorte zu erreichen, und unterscheiden sich je nach Anbieter. Schreiben Sie einen Inhaltshash in den Dateinamen jedes Assets, cachen Sie diese Dateien ein Jahr lang als `immutable` und halten Sie nur das HTML kurzlebig.

- Der Cacheschlüssel ist in der einen oder anderen Richtung falsch. Trackingparameter wie `utm_source` machen jeden geteilten Link zu einem eigenen Cache-Eintrag und lassen die Trefferquote einbrechen. Wird ein Header, der die Antwort verändert, etwa `Accept-Language`, im Schlüssel ausgelassen, wird die Sprache eines Lesers an alle ausgeliefert. Entfernen Sie Parameter, die der Ursprungsserver ignoriert, und nennen Sie in `Vary` die Header, die er auswertet.
- Ein beliebtes Objekt läuft ab, und der Ursprungsserver wird überflutet. Tausende Leser finden im selben Augenblick keine frische Kopie im Cache, und jede ihrer Anfragen gelangt zum Ursprungsserver. Das Zusammenfassen gleichzeitiger Anfragen im CDN und `stale-while-revalidate`, das die alte Kopie ausliefert, während eine einzige Anfrage die neue holt, halten die Last des Ursprungsservers gleichmäßig.
- Der Ursprungsserver antwortet jedem, der ihn findet. Schutz am Netzrand bringt wenig, wenn Angreifer die Ursprungsadresse direkt erreichen. Alte DNS-Einträge, Mailheader oder eine vergessene Subdomain verraten sie häufig. Nehmen Sie am Ursprung Verkehr nur vom CDN an, anhand seines Netzbereichs oder über eine authentifizierte Verbindung.

Weiterführende Lektüre

- RFC 6707, Abschnitt 1.1: CDN-Begriffe — die Definitionen der IETF für CDN, Ersatzserver und Anfragerouting.
- RFC 9111: HTTP Caching — was gemeinsame Caches wie lange speichern dürfen und was `private` bedeutet.
- RFC 9213: Gezielte HTTP-Cachesteuerung — das Feld `CDN-Cache-Control`, das nur CDNs anspricht.
- RFC 5861: HTTP-Cache-Control-Erweiterungen für veraltete Inhalte — `stale-while-revalidate` und `stale-if-error`.
- RFC 8246: Unveränderliche HTTP-Antworten — wie eine Datei mit Inhaltsfingerabdruck eine erneute Prüfung vermeidet.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist ein CDN?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/cdn/