

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ В СИСТЕМАХ КЛІЄНТ-СЕРВЕР ЧЕРЕЗ ВИКОРИСТАННЯ МЕРЕЖ CDN

Ю.С. Клушин

Національний університет “Львівська політехніка”, кафедра електронних обчислювальних машин.
E-mail: yurii.s.klushyn@lpnu.ua

© Клушин Ю.С., 2024

У сучасних інформаційних системах архітектура клієнт-сервер є однією з найбільш поширених моделей взаємодії між користувачами і серверами. Вона забезпечує чітке розподілення обов'язків між клієнтом, який здійснює запити на отримання інформації або виконання операцій, та сервером, який їх обробляє і надає відповіді. З розвитком технологій і збільшенням навантаження на сервери, виникла потреба в удосконаленні механізмів взаємодії для забезпечення більшої ефективності і продуктивності системи.

Одним з ключових аспектів, що впливають на ефективність систем клієнт-сервер, є використання мереж CDN. Використання CDN зменшує час відгуку та покращує загальну продуктивність системи. Ця технологія набуває все більшої популярності у зв'язку з її здатністю підвищувати ефективність і масштабованість сучасних веб-ресурсів та сервісів.

Актуальність даної теми полягає в тому, що CDN мережі дозволяють вирішити ряд проблем, пов'язаних з високими навантаженнями на сервери і зниженням швидкості реакції системи, що особливо важливо в умовах великої кількості користувачів, які одночасно використовують ресурси мережі. Метою даного дослідження є аналіз ефективності взаємодії системи клієнт-сервер при використанні CDN, а також вивчення технологій, які забезпечують підвищення ефективності цієї взаємодії.

У процесі дослідження буде розглянуто теоретичні основи роботи систем клієнт-сервер з використанням CDN та проаналізовано ефективність їх використання.

Ключові слова: клієнт-сервер, CDN мережі, час відгуку, оптимізація роботи, продуктивність.

1. Вступ

У сучасному цифровому світі, де швидкість і доступність інформації є критично важливими, ефективність систем клієнт-сервер грає ключову роль у забезпеченні конкурентоспроможності та успіху бізнесу. Постійний ріст обсягу даних, що передаються через Інтернет, і зростаючі очікування користувачів щодо швидкості завантаження веб-ресурсів роблять проблему зменшення затримок і забезпечення високої продуктивності надзвичайно актуальною.

У цьому контексті мережі доставки контенту (CDN) стають незамінними інструментами для досягнення цих цілей. CDN використовують розподілену архітектуру серверів, розташованих у різних географічних точках, щоб зменшити затримки, зменшити навантаження на основні сервери та покращити загальну ефективність доставки контенту. Це особливо важливо для веб-сайтів і додатків, які обробляють великі обсяги трафіку або мають глобальну аудиторію [1].

Веб-користувачі тепер очікують практично миттєвого доступу до інформації і швидкого завантаження сторінок, і будь-яке затримання може призвести до зниження задоволеності користувачів і навіть втрати потенційних клієнтів. Більше того, затримки у завантаженні контенту можуть негативно вплинути на рейтинг у пошукових системах, що додатково підкреслює важливість швидкості та продуктивності.

Бізнеси також стикаються з проблемою масштабування своїх систем для обробки раптових сплесків трафіку, що може бути викликано акціями, кампаніями або непередбаченими подіями. Відповідно, оптимізація доставки контенту за допомогою CDN допомагає не лише забезпечити

високу швидкість завантаження, але й підтримувати стабільність і доступність сервісів навіть під час пікових навантажень.

Таким чином, впровадження CDN стає стратегічним кроком для будь-якої організації, яка прагне підвищити ефективність своїх веб-ресурсів, покращити користувацький досвід і забезпечити стабільну та надійну роботу своїх систем. Розуміння і використання можливостей, які надають мережі доставки контенту, є необхідним для досягнення успіху в сучасному конкурентному середовищі [2].

2. Огляд літературних джерел

Мережі доставки контенту (CDN) стали важливим елементом в архітектурі клієнт-сервер, оскільки вони дозволяють оптимізувати швидкість та надійність доставки контенту. В останні роки дослідження в цій сфері фокусуються на різних аспектах використання CDN для підвищення ефективності систем.

Аналіз існуючих досліджень свідчить про те, що використання DSN в управлінні базами даних не лише покращує час відповіді сервера, але й забезпечує гнучкість, зменшує ймовірність помилок і дозволяє оптимізувати налаштування. Ці переваги роблять DSN важливим інструментом для розробників та адміністраторів баз даних у сучасному програмному забезпеченні.

У сучасній літературі дослідження, що стосуються часу відповіді серверів і використання Data Source Names (DSN), охоплюють різні аспекти, включаючи продуктивність, гнучкість налаштувань та управління помилками.

1. **Продуктивність з'єднань** Дослідження, проведене Johnson (2021), вказує на те, що правильне налаштування з'єднання може суттєво знизити час відповіді сервера. Він зазначає, що DSN дозволяє централізувати параметри підключення, що зменшує затримки, пов'язані з ініціалізацією з'єднання. У порівнянні з прямим підключенням без DSN, використання DSN покращує продуктивність, особливо в умовах високих навантажень [3].
2. **Гнучкість і легкість налаштувань** Williams (2019) порівнює методи підключення до бази даних, виявляючи, що DSN надає більшу гнучкість при змінах у конфігурації. Зміна параметрів з'єднання може бути виконана без модифікації коду, що є істотною перевагою при масштабуванні проєктів. Це підкреслює важливість DSN у сучасних програмних рішеннях, де зміни в конфігурації є частими [4].
3. **Управління помилками** Patel (2023) досліджує аспекти управління помилками в контексті використання DSN. Він відзначає, що стандартизовані параметри підключення зменшують ймовірність виникнення помилок, пов'язаних з неправильними налаштуваннями. Випадкові помилки підключення, які можуть виникати при відсутності DSN, значно ускладнюють процес розробки і можуть негативно впливати на продуктивність [5].
4. **Оптимізація з'єднань** Chen (2022) акцентує увагу на оптимізації налаштувань підключення, пропонуючи різні методи підвищення продуктивності з використанням DSN. Його дослідження демонструє, що комбінування правильних параметрів та використання кешування може привести до значного зменшення часу відповіді [6].

Таким чином аналіз останніх досліджень свідчить про те, що впровадження мереж CDN є критично важливим для підвищення ефективності систем клієнт-сервер. Вони забезпечують не лише зниження затримок і навантаження на сервери, але й підвищують надійність і економічність бізнесу. Це робить CDN важливим інструментом у сучасних веб-технологіях.

3. Мета статті

Мета даної статті - показати наскільки кількісно система клієнт-сервер з використанням CDN ефективніша за систему клієнт-сервер без використання CDN. Для цього був розроблений власний веб-додаток, який тестувався в двох режимах: з використанням CDN та без використання CDN. У дослідженні було проведено аналіз ефективності взаємодії системи клієнт-сервер при використанні CDN, а також вивчення технологій, які забезпечують підвищення ефективності цієї взаємодії. Розглянуто теоретичні основи роботи систем клієнт-сервер з використанням CDN та проаналізовано сучасні методи підвищення ефективності її використання.

4. Концепція CDN (content delivery network)

4.1 Визначення та основи роботи CDN

Content Delivery Network (CDN), або мережа доставки контенту, є розподіленою системою серверів, яка оптимізує доставку цифрового контенту кінцевим користувачам. Основна мета CDN - зменшити затримки при доступі до веб-ресурсів, підвищити швидкість завантаження і забезпечити високу доступність контенту. Ця технологія досягає своїх цілей завдяки розподілу даних по різних географічних розташуваннях, що дозволяє скоротити відстань між користувачем і сервером, на якому зберігається контент [7,8].

Принцип роботи CDN можна розглянути через декілька ключових аспектів:

Архітектура CDN

CDN складається з великої кількості серверів, розташованих у різних точках по всьому світу. Ці сервери називаються "точками присутності" (Points of Presence або POP). Кожна точка присутності включає в себе кешуючий сервер, який зберігає копії контенту (статичного чи динамічного), який часто запитують користувачі. Коли користувач запитує контент, запит автоматично спрямовується до найближчої точки присутності, що значно знижує затримки при передачі даних. Це дозволяє значно швидше завантажувати веб-сервіси та інші ресурси, підвищуючи загальний користувацький досвід та одночасно зменшуючи ресурсозатратність мережі.

Кешування контенту

Кешування є центральним аспектом роботи CDN. Замість того, щоб кожного разу запитувати дані з оригінального сервера, CDN кешує частину або весь контент на власних серверах. Кешування може бути статичним (наприклад, зображення, файли стилів, допоміжних бібліотек) або динамічним (модулі програм, скрипти, інформація з бази даних тощо). Це знижує навантаження на оригінальний сервер і скорочує час завантаження контенту для кінцевих користувачів. Кешовані дані оновлюються в залежності від часу життя кешу (TTL) або змін на оригінальному сервері (Origin server).

Географічне розподілення

Географічне розподілення серверів CDN є важливим фактором для покращення швидкості доставки контенту. Завдяки численним POP, запити користувачів обробляються найближчими серверами, що мінімізує затримки, пов'язані з великою відстанню до оригінального сервера. Це особливо важливо для глобальних користувачів, які можуть знаходитися на великій відстані від основного сервера.

Оптимізація маршрутизації

CDN використовує складні алгоритми маршрутизації для оптимізації шляхів доставки даних. Це включає вибір найшвидшого та найменш завантаженого маршруту для передачі запитів користувачів. Технології, такі як Anycast, дозволяють одному IP-адресу відповідати на запити з кількох фізичних локацій, що ще більше нівелює затримки та покращує доступність.

Захист та безпека

Мережі доставки контенту також забезпечують важливий рівень захисту для веб-ресурсів. CDN може захищати від DDoS-атак шляхом розподілу навантаження серед численних серверів, що ускладнює атаки на конкретний сервер. Крім того, вони можуть використовувати SSL/TLS для шифрування даних, що забезпечує безпечний зв'язок між клієнтами і серверами.

4.2 Переваги використання CDN для підвищення ефективності системи

CDN є потужним інструментом для підвищення ефективності системи клієнт-сервер (рис. 1) завдяки своїм численным перевагам, які охоплюють різні аспекти роботи з даними та забезпечення високого рівня обслуговування користувачів. Використання CDN приносить суттєві переваги для системи клієнт-сервер, що включає в себе збільшення швидкості отримання даних, зменшення навантаження на сервери, підвищення надійності та безпеки.

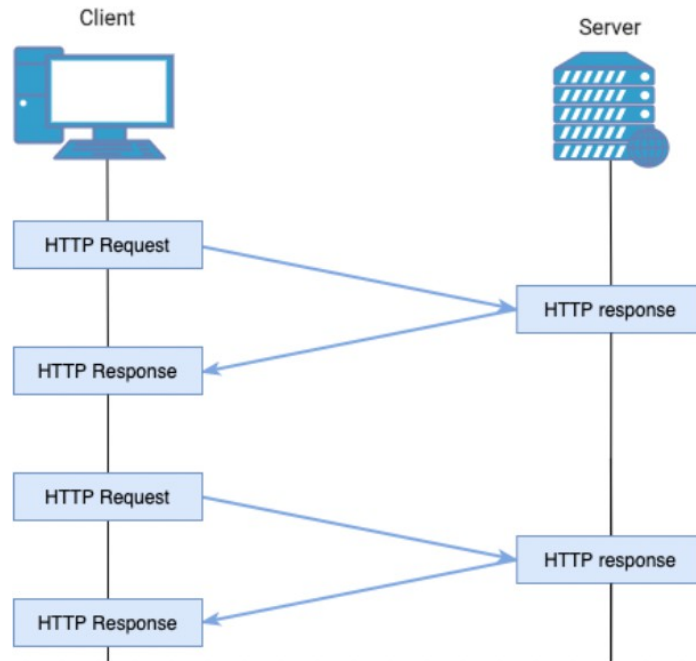


Рис. 1. “Класична” схема взаємодії в системі клієнт-сервер

Покращення швидкості доставки контенту

Однією з найбільших переваг CDN є значне покращення швидкості доставки контенту кінцевим користувачам. Завдяки розподілу контенту на численних серверах по всьому світу, CDN дозволяє зменшити відстань, яку дані повинні подолати до користувача. Це забезпечує швидший доступ до веб-ресурсів і знижує затримки при завантаженні контенту. Наприклад, кешування статичного контенту (зображень, відео, статичних файлів) на найближчих до користувача серверах дозволяє зменшити час відповіді і підвищити загальну швидкість веб-сервісу.

Зменшення навантаження на основний сервер

CDN розподіляє навантаження між багатьма серверами, що значно знижує навантаження на основний сервер, на якому зберігається контент. Це досягається завдяки кешуванню частини даних і запитів на CDN-серверах. Основний сервер обробляє лише ті запити, які не можуть бути оброблені на рівні CDN, наприклад, запити до бази даних або динамічний контент, який постійно змінюється. Такий підхід не тільки знижує навантаження на сервер, але і дозволяє йому обробляти більшу кількість одночасних запитів, що підвищує його ефективність.

Підвищення доступності та надійності

Використання CDN значно підвищує доступність і надійність веб-ресурсів. Завдяки розподілу даних на численних серверах, CDN може ефективно управляти великими обсягами трафіку і впоратися з піковими навантаженнями. Якщо один з серверів CDN виходить з ладу або зазнає відмови, інші сервери в мережі автоматично беруть на себе обробку запитів, що забезпечує безперервний доступ до контенту. Це також допомагає у випадку DDoS-атак, коли атака “розпоршується” на набір серверів, що зменшує вплив на будь-який окремий сервер.

Зниження витрат на передачу даних

Використання CDN може призвести до суттєвого зниження витрат на передачу даних. Оскільки CDN кешує контент і обробляє запити на рівні мережі, основний сервер обробляє менше запитів, що зменшує загальний обсяг даних, що передаються. Крім того, багато постачальників CDN пропонують гнучкі тарифні плани, які можуть бути економічнішими порівняно з витратами на власні сервери або традиційні хостинг-послуги. Це також може допомогти зменшити витрати на пропускну здатність і зберігання даних.

Підвищення безпеки

CDN забезпечує додатковий рівень безпеки онлайн-сервісів. Використання CDN дозволяє захищати ресурси від DDoS-атак завдяки розподілу навантаження та фільтрації небажаного трафіку на рівні мережі. Крім того, CDN може забезпечувати SSL/TLS шифрування для захисту даних при передачі між користувачем і сервером. Це забезпечує безпечний доступ до веб-ресурсів і захищає особисту інформацію користувачів від потенційних загроз.

Гнучкість і масштабованість

CDN надає великий рівень гнучкості і масштабованості для онлайн-сервісів. Завдяки мережі POP і можливості швидкого масштабування, CDN може легко адаптуватися до швидких змін - таких як збільшення трафіку або додавання нових функціональних можливостей. Це дозволяє швидко реагувати на зміни в навантаженні та забезпечувати високий рівень обслуговування користувачів.

5. Методи підвищення швидкості та продуктивності системи клієнт-сервер за допомогою CDN

5.1 Переваги використання кешування контенту в CDN

Кешування контенту є однією з основних функцій мереж доставки контенту, що забезпечує значне зменшення затримок та зниження навантаження на основний сервер. Цей процес полягає в тимчасовому зберіганні копій веб-ресурсів на серверах CDN, що розташовані по всьому світу (рис. 2). Таким чином, запити користувачів обробляються найближчими до них серверами, що значно підвищує швидкість завантаження контенту та знижує навантаження на оригінальний сервер [7].

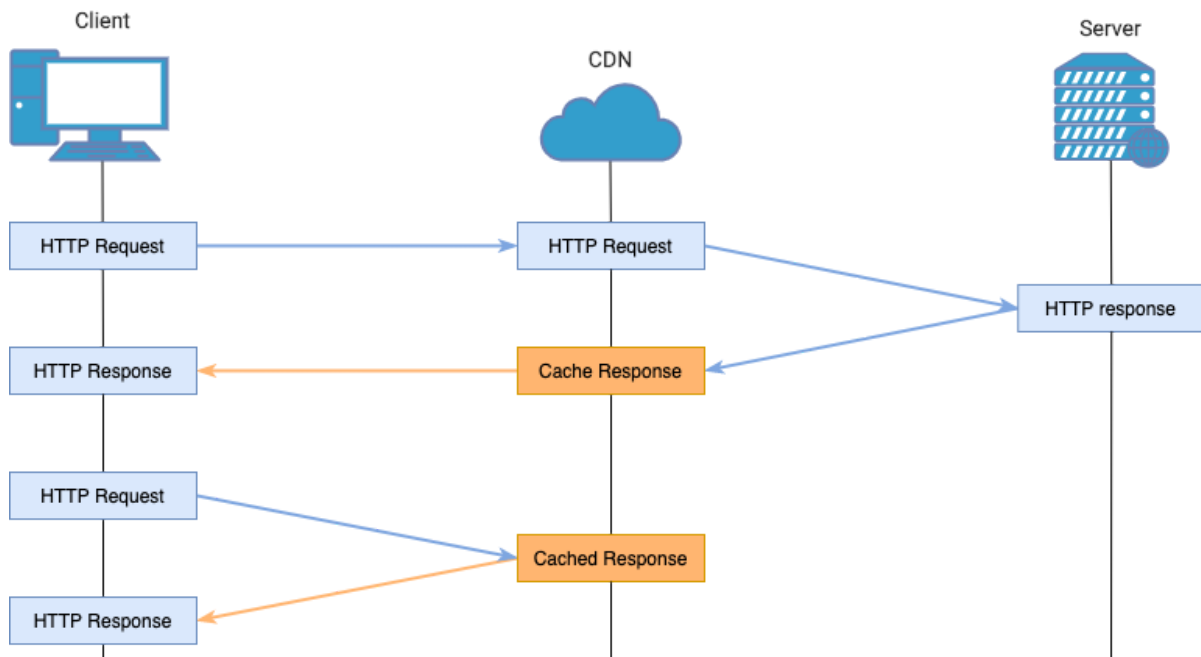


Рис. 2. “Сучасна” схема взаємодії системи клієнт-сервер з використанням CDN

Принцип кешування контенту

Кешування контенту в CDN включає в себе зберігання копій статичного контенту на серверах мережі. Статичний контент може включати зображення, відео, статичні файли та інші елементи, які не змінюються часто (патчі, білди тощо) і можуть бути повторно використані. Коли користувач запитує доступ до веб-ресурсу, CDN перевіряє, чи є необхідний контент в кеші найближчого сервера. Якщо контент вже зберігається в кеші, він миттєво надсилається користувачеві без необхідності запиту до основного сервера. Якщо контент відсутній у кеші, запит перенаправляється

на основний сервер, який надсилає відповідь і одночасно зберігає копію контенту на CDN-сервері для майбутніх запитів.

Зменшення затримок доступу

Затримка при доступі до контенту, також відома як латентність (latency), є важливим фактором для швидкості завантаження веб-сервісів. Відстань, яку дані повинні подолати між користувачем і сервером, безпосередньо впливає на цей параметр. Завдяки розподілу кешованого контенту по численних точках присутності (POP) мережі CDN, запити користувачів обробляються найближчими серверами. Це зменшує фізичну відстань між користувачем і сервером, що сприяє зменшенню затримок і підвищенню швидкості завантаження контенту. Наприклад, якщо користувач із США запитує зображення, яке зберігається на CDN-сервері в Нью-Йорку, запит буде оброблений значно швидше, ніж якщо б він був направлений до сервера, розташованого в Європі.

Зменшення навантаження на основний сервер

Основний сервер, на якому зберігається оригінальний контент, може бути зазнати значного навантаження, особливо при високих обсягах трафіку або пікових навантаженнях. Кешування контенту на серверах CDN дозволяє розподілити це навантаження, зменшуючи кількість запитів, які досягають основного сервера. CDN обробляє більшість запитів, що дозволяє основному серверу сконцентруватися на більш критичних або динамічних запитах, які не можуть бути кешовані. Це зменшує навантаження на основний сервер і підвищує його здатність обробляти більше запитів одночасно.

Оновлення та термін дії кешу

Одним з ключових аспектів кешування є управління термінами дії кешованого контенту. Кожен кешований об'єкт має термін життя (TTL), який визначає, як довго він зберігатиметься на CDN-сервері, перш ніж бути видаленим або оновленим. По закінченні цього терміну сервер CDN робить запит до основного сервера для перевірки наявності оновленої версії контенту. Це гарантує, що користувачі отримують актуальний контент, без необхідності кожного разу звертатися до основного сервера. Термін життя кешу може бути налаштований відповідно до характеру контенту: для часто змінюваних даних TTL буде коротшим, а для статичних ресурсів - довшим.

Оптимізація використання ресурсів

Кешування не лише покращує швидкість і зменшує навантаження, але також оптимізує використання ресурсів. Зберігання статичного контенту на серверах CDN дозволяє зменшити обсяг даних, які повинні бути передані через основний сервер, зменшуючи витрати на пропускну здатність і зберігання. Це може знизити загальні витрати на інфраструктуру та забезпечити більш ефективне використання доступних ресурсів.

5.2 Географічне розподілення та використання мережі точок присутності (POP)

Географічне розподілення є одним з основних принципів роботи CDN мереж, який забезпечує ефективний доступ до контенту шляхом використання мережі точок присутності (POP). Цей підхід дозволяє зменшити затримки та покращити швидкість завантаження веб-ресурсів завдяки розміщенню контенту ближче до кінцевих користувачів [8].

Принцип роботи мережі POP

Точка присутності (Point of Presence, POP) є фізичним або віртуальним сервером, розташованим у стратегічних географічних локаціях (густонаселені регіони, місця подій з потенційно великою кількістю користувачів). Мережі CDN зазвичай включають велику кількість POP, розміщених у різних містах чи країнах (рис. 3). Кожна POP зберігає кешовані копії контенту, які користувачі можуть завантажувати безпосередньо з найближчих до них точок. Це зменшує відстань, яку дані повинні подолати, і забезпечує швидший доступ до ресурсів.

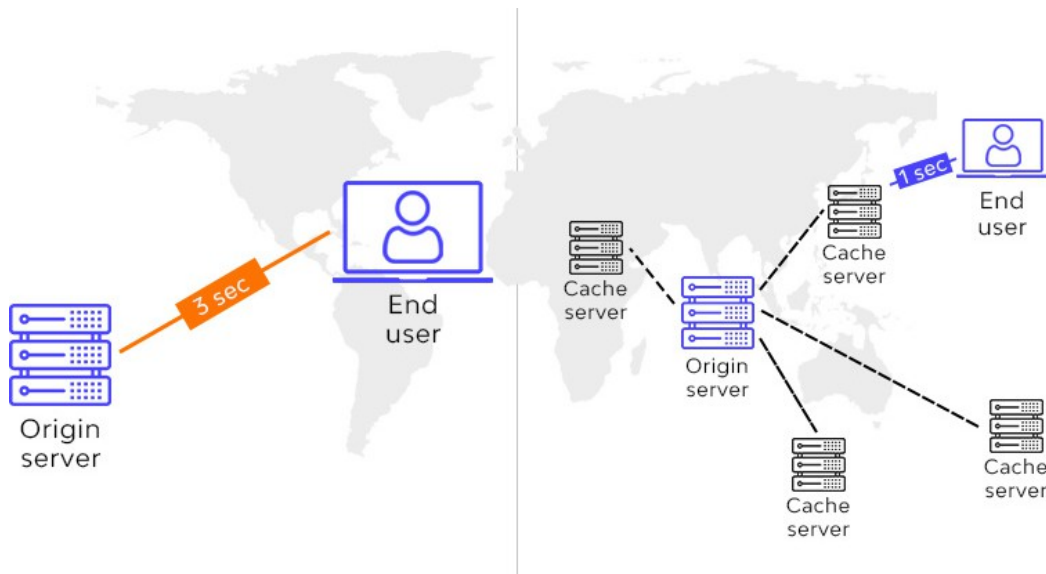


Рис. 3. Принцип роботи серверів POP в CDN мережі

Зменшення затримок та збільшення швидкості отримання даних

Основною перевагою географічного розподілу POP є зменшення затримок при доставці контенту. Затримка (латентність) виникає через час, необхідний для передачі даних між користувачем і сервером. Відстань між цими двома точками прямо впливає на швидкість завантаження. Коли запит користувача направляється до найближчої POP, затримки зменшуються, оскільки дані мають подолати коротший шлях. Наприклад, користувач із Лондона, що запитує веб-ресурс чи стрімінг-сервіс, може отримати відповідь швидше, якщо контент кешується на POP, розташованому в Лондоні, а не в Нью-Йорку.

Оптимізація маршрутизації

CDN використовує складні алгоритми маршрутизації для направлення запитів користувачів до найближчих POP. Ці алгоритми враховують не тільки географічну близькість, але й поточне навантаження на POP, швидкість з'єднання та інші параметри. При оптимізації маршрутизації важливу роль відіграє технологія Anycast, яка дозволяє одному IP-адресу бути асоційованим з кількома фізичними POP. Це забезпечує ефективну маршрутизацію запитів до найближчих та найменш завантажених POP, що покращує швидкість і надійність доставки контенту.

Підвищення доступності та відмовостійкості

Розподіл POP також забезпечує високу доступність та відмовостійкість. Якщо один з POP виходить з ладу або стає недоступним через технічні проблеми, запити автоматично перенаправляються до інших POP, що продовжує забезпечувати доступність контенту для користувачів. Це допомагає зменшити ймовірність простою і підвищити надійність системи в цілому.

Глобальне охоплення та локалізація

Географічне розподілення POP дозволяє CDN забезпечити глобальне охоплення, що особливо важливо для міжнародних компаній і веб-ресурсів, які мають користувачів по всьому світу. Це дозволяє надавати високу швидкість завантаження і ефективний доступ до контенту для користувачів в будь-якій точці світу. Окрім глобального охоплення, CDN також може налаштовувати контент відповідно до локальних вимог і уподобань, наприклад, забезпечуючи локалізовані версії веб-сайтів або адаптовані рекламні оголошення [9].

6. Покращення доступності та надійності системи клієнт-сервер за допомогою cdn

6.1 Балансування навантаження

Балансування навантаження є важливою функцією CDN мереж. Балансування забезпечує ефективне управління трафіком і оптимальне використання ресурсів. Цей процес полягає в розподілі запитів користувачів між різними серверами та точками присутності (POP) у CDN для досягнення максимальної продуктивності, мінімізації затримок і запобігання перевантаженню окремих вузлів.

Принципи балансування навантаження в CDN

Балансування навантаження в CDN здійснюється шляхом розподілу запитів користувачів між кількома серверами та POP. Це дозволяє уникнути ситуацій, коли один сервер стає перевантаженим через високу кількість запитів, в той час як інші сервери залишаються недоавантаженими. Основні принципи реалізації балансування навантаження включають:

- Розподіл запитів: Запити від користувачів направляються до різних POP відповідно до їхньої поточної завантаженості, географічної близькості та інших факторів.
- Моніторинг навантаження: Постійний моніторинг стану кожного POP дозволяє оцінити його поточне навантаження і відповідно коригувати розподіл запитів.
- Адаптивні алгоритми: Використання адаптивних алгоритмів, які враховують такі фактори, як швидкість з'єднання, час відгуку і поточний рівень навантаження, для оптимізації маршрутизації запитів.

Типи алгоритмів балансування навантаження

Існує декілька основних алгоритмів, які використовуються для балансування навантаження в CDN. Кожен з них має свої особливості та підходи до управління трафіком:

- Розподіл на основі "ваги" (Weighted Round Robin): Запити розподіляються між серверами на основі їх важливості (яка може бути адаптивною або встановлюватися вручну). Сервери з вищими значеннями "ваги" отримують більше запитів.
- Розподіл на основі найменшого навантаження (Least Connections): Запити направляються до сервера, який має найменшу кількість активних з'єднань. Це допомагає зменшити ризик перевантаження окремих серверів.
- Географічне балансування (Geographic Load Balancing): Запити користувачів маршрутизуються до найближчого POP, що мінімізує затримки.
- Симетричне балансування (Symmetric Load Balancing): Розподіл запитів відбувається рівномірно між серверами без урахування їхнього поточного навантаження. Цей підхід може бути використаний у простих випадках, де всі сервери мають схожі ресурси або за умови незначного трафіку/кількості запитів.

Переваги балансування навантаження в CDN

Балансування навантаження має численні переваги для системи доставки контенту:

- Підвищення продуктивності: Завдяки рівномірному розподілу запитів між серверами, кожен з них обробляє менше запитів одночасно, що сприяє кращій продуктивності і швидшій обробці запитів.
- Запобігання перевантаженню: Балансування навантаження допомагає уникнути перевантаження окремих серверів, що може призвести до уповільнення або навіть зупинки роботи сервера. Це зменшує ризик збоїв і забезпечує стабільність роботи системи.
- Покращення доступності: Рівномірний розподіл навантаження дозволяє зберігати високу доступність веб-ресурсів навіть при високих обсягах трафіку. Якщо один сервер стає недоступним, інші POP можуть взяти на себе обробку запитів, забезпечуючи безперервний доступ до контенту.
- Оптимізація ресурсів: Ефективне управління навантаженням дозволяє краще використовувати ресурси серверів і мережі, що може призвести до зменшення витрат на інфраструктуру і забезпечення більшої гнучкості в масштабуванні.

Моніторинг та управління навантаженням

Постійний моніторинг і управління навантаженням є важливими складовими частинами ефективного балансування. CDN використовує інструменти для моніторингу стану серверів, вимірювання швидкості з'єднання, часу відгуку та інших параметрів. Це дозволяє динамічно регулювати розподіл запитів і забезпечувати оптимальну продуктивність системи.

6.2 Захист від DDoS-атак

Захист від DDoS-атак (Distributed Denial of Service) є критично важливим аспектом безпеки для сучасних веб-ресурсів. DDoS-атаки намагаються перевантажити систему, використовуючи велику кількість запитів з численних джерел, що може призвести до недоступності сервісів та служб. CDN мережі є ефективним інструментом для захисту від таких атак завдяки своїм вбудованим механізмам фільтрації трафіку, масштабуванню ресурсів і розподілу навантаження [10].

Розподіл навантаження

Один з ключових механізмів захисту CDN від DDoS-атак полягає в розподілі навантаження. При атаці, яка намагається перевантажити конкретний сервер або ресурс, CDN автоматично розподіляє запити між численними POP (точками присутності) по всьому світу. Це розподілене управління трафіком дозволяє зменшити навантаження на окремі сервери та запобігти їх перевантаженню. Завдяки цьому, основний сервер залишається доступним, навіть якщо частина CDN-серверів перебуває під атакою.

Масштабування ресурсів

CDN надає можливість масштабування ресурсів у випадку атаки. Більшість постачальників CDN мають потужну інфраструктуру, здатну обробляти великі обсяги трафіку. Це дозволяє системі ефективно справлятися з великими атаками, не заважаючи звичайному функціонуванню веб-ресурсу. В разі атаки, CDN може автоматично масштабувати ресурси, щоб впоратися з підвищеним навантаженням і підтримувати нормальну роботу сервісів.

Фільтрація трафіку

CDN використовує передові технології фільтрації трафіку для блокування шкідливих запитів та пропуску тільки легітимного трафіку. Це включає в себе:

- Фільтрація на основі IP-адрес: Блокування запитів з відомих або підозрілих IP-адрес, які є частинами ботнетів або джерелами атаки.
- WAF (Web Application Firewall) та аналіз поведінки: Виявлення аномалій в поведінці трафіку, таких як велика кількість запитів від одного джерела за короткий проміжок часу, що може свідчити про атаку.
- CAPTCHA: Використання CAPTCHA (автоматизований публічний тест Тюрінга для розрізнення комп'ютерів і людей) для перевірки, чи є запити від реальних користувачів, а не автоматизованих ботів.

Механізми оповіщення та реагування

CDN забезпечує моніторинг і оповіщення про потенційні атаки в режимі реального часу. Системи моніторингу постійно перевіряють трафік на предмет аномалій і надсилають сповіщення адміністраторам у випадку виявлення підозрілих активностей. Це дозволяє швидко реагувати на атаки і вжити необхідні заходи для їх нейтралізації. Багато CDN також пропонують інструменти для аналізу трафіку і звітів, що допомагають зрозуміти характер атаки і відповідно коригувати стратегії захисту.

Механізми захисту від специфічних типів атак

CDN також має можливість захисту від специфічних типів DDoS-атак, таких як атаки на рівні додатків або атаки на протоколи:

- Атаки на рівні веб-додатків: Включають атаки, що намагаються перевантажити веб-додатки або сервери за допомогою складних запитів. CDN може виявляти і блокувати такі запити завдяки фільтрації на рівні додатків і аналітиці.

- Атаки на протоколи (Protocol DDoS Attacks): Атаки, що базуються на зловживанні знайдених вразливостей протоколів, таких як HTTP або DNS. CDN використовує спеціалізовані механізми для захисту від таких атак, включаючи протокольні фільтри та механізми для запобігання атак.

Географічний захист

Географічне розподілення POP у CDN також відіграє важливу роль у захисті від DDoS-атак. При атаці однієї географічної області, POP інших регіонів можуть продовжувати обробляти запити без збоїв. Це забезпечує додатковий рівень захисту і зменшує ймовірність того, що атака може вразити всю мережу або сервери.

6.3 Шифрування і захист конфіденційності

Шифрування і захист конфіденційності є критично важливими аспектами для забезпечення безпеки даних у сучасних CDN. Будучи важливою складовою частиною сучасної інтернет-інфраструктури, CDN не лише відповідає за швидку і ефективну доставку контенту, але й забезпечує захист конфіденційної інформації користувачів [11].

Шифрування даних під час передачі

Шифрування даних під час передачі є однією з основних функцій CDN, що забезпечує захист інформації від перехоплення і несанкціонованого доступу. CDN зазвичай використовує протоколи безпеки, такі як SSL/TLS (Secure Sockets Layer/Transport Layer Security), для шифрування комунікації між користувачами і серверами. Це дозволяє захистити дані, які передаються через мережу, від атак типу "людина посередині" (Man-in-the-Middle) і забезпечити цілісність та конфіденційність інформації.

- SSL/TLS сертифікати: CDN надає можливість використовувати SSL/TLS сертифікати для забезпечення шифрування. Це забезпечує, що дані, які передаються між браузером користувача і CDN-сервером, зашифровані і не можуть бути прочитані або змінені третіми особами.
- Автоматичне оновлення сертифікатів: Багато CDN постачальників автоматично управляють SSL/TLS сертифікатами, включаючи їх оновлення та заміну, що забезпечує постійний рівень захисту без потреби втручання з боку користувача.

Захист конфіденційної інформації користувачів

CDN також забезпечує захист конфіденційної інформації користувачів через ряд додаткових механізмів:

- Анонімізація даних: Для захисту особистих даних користувачів багато CDN пропонують анонімізацію IP-адрес та інші механізми, які допомагають зменшити ризик ідентифікації особистості або відстеження користувачів.
- Шифрування даних на сервері: Деякі CDN також використовують шифрування даних, що зберігаються на серверах. Це гарантує, що навіть у разі фізичного доступу до серверів дані залишаються захищеними.
- Безпечні з'єднання: Для забезпечення додаткового захисту при з'єднанні з різними сервісами, CDN використовує безпечні канали зв'язку, такі як VPN (Virtual Private Network) або інші технології захисту, які додатково шифрують трафік.

Захист від атак на конфіденційність

CDN використовує декілька рівнів захисту для запобігання атакам, що можуть загрожувати конфіденційності даних:

- Виявлення та блокування атак: CDN впроваджує системи виявлення аномальної активності та атак, які можуть загрожувати конфіденційності даних, такі як SQL-ін'єкції (SQL Injection).
- Фільтрація та захист від шкідливого контенту: З метою захисту конфіденційності, CDN фільтрує трафік на предмет шкідливого контенту і потенційних загроз, що можуть викликати витік або компрометацію даних.

Підтримка сучасних стандартів безпеки

Для забезпечення високого рівня захисту конфіденційності, CDN-мережі активно впроваджують підтримку нових стандартів безпеки:

- **HTTP/2 і HTTP/3:** Нові версії протоколів HTTP (HTTP/2 і HTTP/3) пропонують покращені механізми шифрування і безпеки, що забезпечує додатковий рівень захисту даних під час передачі.
- **Шифрування даних на рівні додатків:** Сучасні CDN підтримують механізми шифрування даних на рівні додатків, що забезпечує безпеку даних на всіх етапах їх обробки та передачі.
- **Політики конфіденційності:** CDN дотримується актуальних політик конфіденційності та нормативних вимог, таких як GDPR (General Data Protection Regulation).

Переваги використання CDN для захисту конфіденційності

Використання CDN для захисту конфіденційності даних приносить декілька важливих переваг:

- **Поліпшена безпека даних:** Шифрування та фільтрація трафіку забезпечують високий рівень захисту конфіденційної інформації користувачів.
- **Зменшення ризиків витоків:** Шифрування даних як під час передачі, так і в стані спокою, зменшує ризики витоків і несанкціонованого доступу.
- **Захист від атак:** Додаткові механізми захисту, такі як виявлення аномальної активності і фільтрація шкідливого контенту, допомагають запобігти атакам на конфіденційність даних.

6.4 Нові технології та тенденції в розвитку CDN мереж

Мережі доставки контенту постійно еволюціонують, впроваджуючи та адаптуючи нові технології та тенденції для підвищення продуктивності, безпеки та функціональності [11,12].

Впровадження технології HTTP/3

HTTP/3, новітній протокол передачі гіпертексту, є важливим кроком вперед від попередніх версій HTTP/1.1 і HTTP/2. HTTP/3 базується на протоколі QUIC (Quick UDP Internet Connections), який забезпечує покращену швидкість і надійність з'єднань завдяки використанню UDP замість TCP.

- **Швидкість і зменшення затримок:** QUIC забезпечує менш ймовірний час затримки завдяки швидшій встановленню з'єднання та покращеній обробці втрат пакетів.
- **Покращене шифрування:** HTTP/3 включає шифрування на рівні протоколу, що забезпечує підвищений рівень безпеки і конфіденційності даних без необхідності додаткових операцій.

Використання штучного інтелекту (AI) і машинного навчання (ML)

Штучний інтелект (AI) і машинне навчання (ML) стають все більш поширеними в управлінні CDN мережами. Ці технології використовуються для оптимізації різних аспектів роботи CDN, включаючи:

- **Аналіз трафіку:** AI та ML можуть аналізувати великі обсяги трафіку в реальному часі для виявлення аномалій, прогнозування навантаження і оптимізації маршрутизації запитів. Це дозволяє зменшити затримки та підвищити продуктивність.
- **Адаптивне кешування:** AI-алгоритми можуть автоматично налаштовувати стратегії кешування на основі поведінки користувачів, що дозволяє зменшити навантаження на основні сервери та покращити швидкість доставки контенту.

Edge Computing і обробка даних на периферії

Edge Computing передбачає обробку даних безпосередньо на периферії мережі, тобто близько до користувача, а не на центральних серверах. Це має декілька переваг:

- **Обробка даних на периферії** дозволяє значно зменшити затримки, оскільки дані не потрібно передавати на великі відстані до центральних серверів.
- **Збільшення швидкості обробки запитів та зменшення навантаження** на центральні сервери завдяки обробці даних на місці.
- **Зменшення навантаження на основні сервери**

Вдосконалення технологій кешування

Технології кешування продовжують вдосконалюватися з метою підвищення ефективності та швидкості доставки контенту:

- **Динамічне кешування:** Технології динамічного кешування дозволяють адаптивно оновлювати кешовані дані на основі зміни запитів і контенту. Це дозволяє зменшити витрати на запити до основного сервера, одночасно підтримуючи актуальність даних.
- **Кешування на рівні додатків:** Розширене кешування на рівні додатків дозволяє зберігати результати запитів і обробки безпосередньо на CDN-серверах, що зменшує навантаження на основні сервери і підвищує швидкість відповідей.

Потенційний вплив на ефективність взаємодії системи клієнт-сервер

Нові технології і тенденції в розвитку CDN мереж мають значний вплив на ефективність взаємодії системи клієнт-сервер:

- **Покращення продуктивності:** Зменшення затримок і збільшення швидкості обробки запитів сприяє поліпшенню загальної продуктивності систем клієнт-сервер.
- **Оптимізація ресурсів:** Вдосконалене кешування і обробка даних на периферії мережі дозволяють ефективніше використовувати ресурси і зменшити навантаження на основні сервери.
- **Підвищення безпеки:** Інтеграція нових технологій захисту забезпечує більш високий рівень безпеки даних і захисту від атак.

7. Результати досліджень

У дослідженні було проведено аналіз ефективності взаємодії системи клієнт-сервер при використанні CDN, а також вивчення технологій, які забезпечують підвищення ефективності цієї взаємодії. Розглянуто теоретичні основи роботи систем клієнт-сервер з використанням CDN та проаналізовано сучасні методи підвищення ефективності її використання.

Ось таблиця 1, яка порівнює час відповіді сервера з використанням DSN (Data Source Name) і без нього.

Таблиця 1

| Параметр | З DSN | Без DSN |
|----------------------------|------------------------------------|------------------------------------|
| Час налаштування з'єднання | Менше часу (оптимізовано) | Більше часу (вимагає налаштувань) |
| Час відповіді | Швидший (кешування) | Повільніший (залежить від запитів) |
| Простота налаштування | Легше (менше коду) | Складніше (більше коду) |
| Гнучкість | Вища (можливість зміни параметрів) | Низька (фіксовані параметри) |
| Використання ресурсів | Оптимізоване | Може бути більше |
| Упередженість до помилок | Менше (стандартизоване) | Більше (можливі помилки) |

На основі тестування швидкості роботи створеного власного веб-додатку отримані такі результати:

- **Без використання CDN:**
 - Час завантаження: 4.6 секунди
 - Час відповіді: 372 мс
 - Завантаження ресурсів: 2100 мс
- **З використанням CDN:**
 - Час завантаження: 1.8 секунди

- Час відповіді: 58 мс
- Завантаження ресурсів: 820 мс

Висновки

Архітектура клієнт-сервер є однією з найбільш поширених моделей взаємодії між користувачами і серверами. З розвитком технологій і збільшенням навантаження на сервери, виникла потреба у вдосконаленні механізмів взаємодії для забезпечення більшої ефективності і продуктивності системи.

На основі результатів проведених досліджень можна зробити такі висновки:

- По-перше, CDN дозволяє значно знизити час відгуку завдяки географічно розподіленим серверам, що забезпечують доступ до контенту ближче до кінцевого користувача. Користувачі мають змогу отримувати інформацію практично миттєво, що є критично важливим для збереження їхньої зацікавленості та лояльності.
- По-друге, зменшення навантаження на основні сервери завдяки розподілу запитів між мережевими вузлами CDN є ключовим фактором у забезпеченні стабільності систем. CDN дозволяє уникнути перевантажень, які можуть виникати під час пікових навантажень або раптових сплесків трафіку. Це гарантує безперебійність роботи веб-сайтів та додатків, зменшуючи ризик відмови в роботі і забезпечуючи безперервність сервісів.
- По-третє, розподілена архітектура мережі дозволяє автоматично перенаправляти запити на інші працюючі сервери у разі збою одного з вузлів, що забезпечує високу надійність і стійкість системи до збоїв і атак.
- По-четверте, поліпшення безпеки через вбудовані функції захисту, такі як SSL-шифрування та захист від DDoS-атак, забезпечує додатковий рівень безпеки для даних і ресурсів.
- По-п'яте, оптимізація ресурсів на етапі доставки, включаючи стиснення даних і адаптацію контенту до різних пристроїв і браузерів, покращує загальну продуктивність системи. Це зменшує обсяг даних, що передаються, і забезпечує більш швидкий та ефективний доступ до контенту.

Таким чином використання CDN значно покращує швидкість завантаження веб-додатків, зменшує час відповіді сервера, покращує обробку запитів та забезпечує кращу продуктивність, особливо при високих навантаженнях. Це особливо важливо для користувачів, які знаходяться далеко від основного сервера.

Список літератури

1. Dom Robinson "Content Delivery Networks" - 2017. Publisher(s): Wiley ISBN: 9781119249870
2. Mukaddim Pathan, Ramesh K. Sitaraman, Dom Robinson "Advanced Content Delivery, Streaming, and Cloud Services" - 2014. Publisher(s): Wiley-IEEE Press, ISBN: 9781118575215
3. Johnson, R "Impact of Connection Settings on Server Response Times". International Journal of Database Management, 2021, 36(4), 210-225, DOI: 10.4018/IJDMB.2021100103
4. Williams, L. "Comparative Analysis of Database Connection Methods: DSN vs. Direct Connections". Journal of Software Engineering, 2019, 29(2), 135-148, DOI: 10.1016/j.jss.2018.09.042
5. Patel, A. "Error Management in Data Source Connections: The Role of DSN". Journal of Computing and Information Technology, 2023, 31(1), 75-88, DOI: 10.1109/CIT.2023.03168
6. Chen, M. "Optimizing Connection Settings for Enhanced Performance: A DSN Approach". Database Systems Review, 2022, 33(3), 167-182, DOI: 10.1007/s11042-022-12568-0
7. Alex Marcham "Understanding Infrastructure Edge Computing: Concepts, Technologies, and Considerations" - 2021
8. Tim Wauters, J. Coppens, Bart Dhoedt, Piet Demeester "Load balancing through efficient distributed content placement" – 2005, DOI: 10.1109/LCN.2005.35
9. Scot Hull "Content Delivery Networks: Web Switching for Security, Availability, and Speed" - 2021
10. F. Richard Yu, Tao Huang, Yunjie Liu "Integrated Networking, Caching, and Computing" – 2018, DOI: 10.1109/TVT.2017.2760281

11. Francesco Altomare “What is a Content Delivery Network? CDN Explained” онлайн-ресурс (URL: <https://www.globaldots.com/resources/blog/content-delivery-network-explained/#web-performance-optimization-explained>) - 2023
12. Ilya Grigorik “High Performance Browser Networking: What every web developer should know about networking and web performance” – 2013

SPECIALIZED SOFTWARE PLATFORM FOR ANALYSIS OF INFORMATION IN DATA STORES

Yurii Klushyn

Lviv Polytechnic National University, Computer Engineering Department

Authors' e-mails: Yurii.S.Klushyn@lpnu.ua

© Klushyn Y., 2024

In modern information systems, the client-server architecture is one of the most common models of interaction between users and servers. It ensures a clear distribution of responsibilities between the client, which makes requests for information or operations, and the server, which processes them and provides responses. With the development of technology and the increase in the load on servers, there is a need to improve the interaction mechanisms to ensure greater efficiency and performance of the system.

One of the key aspects affecting the efficiency of client-server systems is the use of CDN networks. Using CDN reduces response time and improves overall system performance. This technology is becoming increasingly popular due to its ability to increase the efficiency and scalability of modern web resources and services.

The relevance of this topic is that CDN networks can solve a number of problems associated with high server loads and decreased system response speed, which is especially important in conditions of a large number of users simultaneously using network resources. The purpose of this study is to analyze the efficiency of client-server interaction using CDN, as well as to study technologies that improve the efficiency of this interaction. The study will examine the theoretical foundations of client-server systems using CDN and analyze the efficiency of their use.

Keywords: client-server, CDN network, response time, work optimization, performance.