Chihaia Vlad, Anul IV, IS

Platforma Google Cloud

Oferită de Google, este o suită de servicii de cloud computing care rulează pe aceeași infrastructură pe care Google o utilizează intern pentru produsele sale finale, cum ar fi "Căutarea Google" și YouTube-ul. Pe lângă un set de instrumente de gestionare, acesta oferă o serie de servicii cloud modulare, inclusiv calcul, stocare de date, analiză de date şi învăţare automată.

Depozitare şi baze de date :

- Cloud Storage – stocare de obiecte cu cache integrat pentru stocarea datelor nestructurate
- Cloud SQL – baza de date cu un serviciu bazat pe MySQL şi PostgreSQL.
- Cloud BigTable – gestionat serviciului de baze date NoSQL.
- Cloud Spanner- bază de date NoSQL pentru aplicaţii web si mobile
- Cloud Datastore- blocare de stocare pentru maşinile virtuale Compute Engine
- Cloud MemoryStore – stocare de date bazată pe Redis

Acces Token

Token-ul de acces este o acreditare care poate fi utilizată de o aplicaţie pentru a accesa un API. Acesta poate fi orice tip (cum ar fi opaque string sau un JWT) şi este destinat unui API. Scopul său este de a informa API că purtătorul acestui jeton a fost autorizat să acceseze API şi să efectueze acţiuni specifice (aşa cum sunt specificate în domeniul de aplicare care a fost acordat). Token-ul de acces ar trebui să fie folosit ca acreditare la purtător şi trimis într-un antet de autorizare HTPP la API.

Cum să obțineți un Token de acces ?
Token-urile de acces sunt emise prin intermediul punctelor finale OAuth 2.0 ale Auth0: / authorization and / oauth / token . Puteți utiliza orice bibliotecă compatibilă cu OAuth 2.0 pentru a obține jetoane de acces. Dacă nu aveți deja o bibliotecă preferată OAuth 2.0, Auth0 oferă biblioteci pentru mai multe limbi și cadre care funcționează perfect cu punctele noastre finale.

Cross-Origin Resource Sharing (CORS)

Este un mecanism care utilizează antete HTTP suplimentare pentru a spune unui browser să permită unei aplicații web care rulează la o singură origine (domeniu) să aibă permisiunea de a accesa resursele selectate dintr-un server de origine diferită. O aplicație web face cross-origin HTTP request atunci când solicită o resursă care are o origine diferită (domeniu, protocol și port) decât originea proprie.

Un exemplu de cross-origin HTTP request : codul JavaScript pentru o aplicație web difuzată de la http://domain-a.com utilizatori XMLHttpRequest pentru a face o solicitare http://api.domain-b.com/data.json. Din motive de securitate, browserele restricționează cererile HTTP cross-origin

inițiate din cadrul scripturilor. De exemplu, XMLHttpRequest și Fetch API respectă politica de același tip . Aceasta înseamnă că o aplicație web care utilizează acele API poate solicita numai resurse HTTP de aceeași origine din care a fost încărcată aplicația, cu excepția cazului în care răspunsul de la cealaltă origine include și antetele corecte CORS. Mecanismul CORS acceptă cereri cross-origin și transferuri de date între browsere și servere web. Browserele moderne utilizează CORS într-un container API cum ar fi XMLHttpRequest sau Fetch pentru a ajuta la atenuarea riscurilor legate de cererile HTTP de cross-origin.