Engineer

Google Cloud

G хмарна платформа Google

Що це таке

Google Cloud — це частина Google, що здає в оренду обчислення зі своїх дата-центрів: віртуальні машини в Compute Engine, об'єктне сховище в Cloud Storage, керовані бази даних у Cloud SQL, кластери Kubernetes у GKE, сховище даних BigQuery і ще багато сервісів, з оплатою за використання. Давня назва Google Cloud Platform і абревіатура GCP досі поширені, зокрема в частині власної документації Google.

Усе, що Google Cloud запускає для клієнта, живе всередині проєкту. Проєкт — це контейнер для ресурсів, для API, увімкнених для них, для квот, які вони використовують, і для зв'язку з платіжним обліковим записом, що за все платить. Він має відображуване ім'я, яке можна змінювати, та ідентифікатор проєкту (project ID), унікальний у всьому Google Cloud і незмінний відтоді, як проєкт створено. Проєкти можна групувати в теки (folders), теки можуть містити інші теки, а все дерево висить на ресурсі організації, що належить обліковому запису Google Workspace або Cloud Identity компанії. Ролі й політики організації, задані на рівні організації чи теки, успадковує кожен проєкт нижче, тож добре накреслене дерево легко контролювати, а погано накреслене важко розплутати.

Мережу влаштовано інакше, ніж в інших великих хмарах. Мережа VPC у Google Cloud разом зі своїми маршрутами й правилами брандмауера — глобальний ресурс поза будь-яким регіоном; регіональні лише її підмережі. Тож віртуальна машина в Бельгії та інша в Айові можуть ділити одну приватну мережу й досягати одна одної за внутрішніми адресами без VPN чи пірингу між двома регіонами. В AWS натомість кожна VPC живе в одному регіоні.

Ідентичності бувають двох видів. Люди входять з обліковими записами Google, зазвичай керованими через Workspace або Cloud Identity організації, і отримують ролі IAM на проєкт, теку чи всю організацію. Програми використовують сервісні облікові записи (service accounts): ідентичності, що належать одному проєкту і від імені яких може діяти віртуальна машина, контейнер чи пайплайн. Якщо прикріпити сервісний обліковий запис до інстансу Compute Engine, код на ньому зможе викликати API Google з ролями цього облікового запису без пароля чи файла ключа на диску.

Застосуйте поняття до рішення

Застосуйте «Що таке Google Cloud?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Сервери під те навантаження, яке у вас справді є, перенесені в хмару чи назад, із порахованим наперед місячним рахунком.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Вела 20 застосунків Docker у Google Cloud і AWS — 20 контейнеризованих застосунків розгорнуто й поставлено під моніторинг

Вела 20 застосунків Docker у Google Cloud і AWS Зв'язатися з нами →

Чому це важливо

Для багатьох команд причина обрати Google Cloud — дані. BigQuery — сховище даних без серверів, розмір яких треба підбирати: таблиці лежать у наборах даних (datasets) усередині проєкту, запити пишуть стандартним SQL, і в моделі on-demand кожен запит оплачується за байти, які він читає, тоді як ціноутворення за потужністю (capacity) натомість оплачує зарезервований обсяг обробки, виміряний у слотах. Зберігання колонкове, тож запит платить за колонки, яких торкається, а не за цілі рядки. Cloud Storage стоїть поруч як зона приймання, і завантаження файлів із бакета — один зі стандартних шляхів усередину. Команда, яка деінде мала б розгортати й налаштовувати кластер сховища даних, може почати з бакета, набору даних і запиту.

Друга причина — межа проєкту, бо до неї прив’язано дуже багато. Оплата, квоти, увімкнені API та IAM сходяться в проєкті, тож окремий проєкт на кожен застосунок і середовище проводить чітку межу: продакшн і тестування отримують окремі дозволи й окремі рядки в рахунку. Вимкнення проєкту одразу зупиняє оплату й усі ресурси в ньому. Власники можуть відновити його протягом 30 днів, хоча деякі сервіси, зокрема Cloud Storage, можуть видалити свої дані раніше. Над проєктами політика організації, задана один раз на теці, може заборонити цілі класи ризикованих налаштувань, як-от мережі за замовчуванням чи ключі сервісних

облікових записів, які можна завантажити, у кожному проєкті під нею. Так невелика команда тримає десяток проєктів однаковими, не перевіряючи кожен вручну.

Як це виглядає на практиці

Три записи в портфоліо показують Google Cloud як зону приймання для сховища даних, як офсайт-сховище для резервних копій і як один кінець приватної мережі.

У роботі з даними шість ETL/ELT-пайплайнів наповнювали BigQuery даними зі сховища за IPsec VPN. Упорядковані набори даних і таблиці експортували, стискали за допомогою gzip і передавали в бакет Google Cloud Storage, а завантаження та зіставлення схем у BigQuery автоматизували за допомогою bq CLI і скриптів на Python. Робота, що вручну забирала понад 3 години, стала тривати менш ніж 20 хвилин наскрізно, актуальність даних зросла із щотижневої до щоденної синхронізації, а Python API, що споживали ці дані, отримали приріст продуктивності на 30%.

Для резервних копій сто критичних резервних копій даних автоматизували: Barman на стороні PostgreSQL, Google Cloud для офсайт-копій. Bash і Python оркестрували й перевіряли весь процес, з політиками зберігання, щоб копії лишалися актуальними, і перевірками цілісності, щоб підтвердити, що кожна справді хороша, а не просто присутня. Після цього резервне копіювання виконувалося автоматично, і його можна було перевірити для кожної бази даних.

На мережевому боці вісьмома тунелями WireGuard та IPsec між Google Cloud і локальними Linux-системами керували як єдиним набором і так само усували в них несправності. Конфігурацію тунелів звели до одного стандарту, за їхнім станом стежили, а коли маршрутизація чи обмін ключами знову й знову давали збій, шукали першопричину замість перезапуску; після цього всі вісім тунелів між хмарою та локальними системами працювали безпечно й надійно.

Де виникають проблеми

Найгостріші краї Google Cloud — його зручності: налаштування, що полегшують перший день і все ще стоять на місці через рік, коли про їхній вибір давно забули.

Мережа за замовчуванням лишається відкритою. Якщо політика організації цього не забороняє, кожен новий проєкт починається з мережі за замовчуванням (default network), що має підмережу в кожному регіоні й чотири заздалегідь заповнені правила брандмауера. Три з них приймають трафік із 0.0.0.0/0, тобто з усього інтернету: SSH на tcp:22, Remote Desktop на tcp:3389 та ICMP. Четверте дозволяє весь трафік TCP, UDP та ICMP із 10.128.0.0/9 усередині мережі. Тож будь-яка віртуальна машина із зовнішньою адресою в цій мережі відкрита для спроб SSH звідусіль. Обмеження `compute.skipDefaultNetworkCreation` не дає новим проєктам її отримати, а власна мережа з правилами, що прямо називають свої джерела, замінює стару.

Ключ сервісного облікового запису потрапляє в репозиторій. Ключ, яким керує користувач, — це JSON-файл, що дає будь-кому, хто його має, діяти від імені сервісного облікового запису, і за замовчуванням строку дії в нього немає: він чинний, доки його хтось не видалить. Такі файли легко розповзаються: у секрети CI, в образи контейнерів і, помилково, в репозиторії. Настанова Google — обирати безпечнішу альтернативу скрізь, де вона є. Навантаження в Google Cloud використовують сервісний обліковий запис, прикріплений до ресурсу, на якому вони працюють, а навантаження деінде, як-от система CI чи інша хмара, використовують Workload Identity Federation, що обмінює власні облікові дані зовнішньої системи на короткоживучі токени Google. В організаціях, створених 3 травня 2024 року або пізніше, створення й завантаження ключів за замовчуванням вимкнено обмеженнями політики організації, а старіші організації можуть задати ті самі обмеження.

Малий запит читає велику таблицю. У моделі on-demand BigQuery виставляє рахунок за байти, які читає запит, і на таблиці без кластеризації (clustering) клауза `LIMIT` цього числа не змінює: `SELECT * ... LIMIT 10` повертає десять рядків і оплачує кожен байт кожної колонки. Варто вибирати лише потрібні колонки, розбивати великі таблиці на розділи за датою, щоб запити з фільтром за нею оминали старі розділи, перевіряти оцінку з пробного запуску (dry run), перш ніж запускати щось нове, і задавати максимальну кількість оплачуваних байтів (maximum bytes billed). Запит, чия оцінка перевищує цю межу, завершується помилкою ще до запуску, без жодної оплати.

Холодне сховище тримає теплі дані. Cloud Storage пропонує класи Nearline, Coldline та Archive, що коштують менше за гігабайт зберігання, ніж Standard, в обмін на плату за отримання даних і мінімальні строки зберігання

30, 90 і 365 днів. Об’єкт, видалений, замінений чи переміщений до спливу свого мінімуму, оплачується так, ніби зберігався весь період. Резервні копії, що ротуються щодня, чи тимчасові файли, які пайплайн записує й видаляє протягом години, тому можуть коштувати в Archive більше, ніж у Standard. Холодніші класи підходять для даних, які записують один раз і читають рідко, а правило життєвого циклу може переносити в них об’єкти, коли ті старіють.

Що почитати далі

- Google Cloud Documentation — покажчик посібників, довідників і навчальних матеріалів Google для кожного продукту Google Cloud.
- About resource hierarchy — як вкладаються організації, теки й проєкти і як ролі та політики успадковуються вниз.
- VPC firewall rules — як оцінюються правила брандмауера, зокрема ті, з якими починається мережа за замовчуванням.
- Best practices for managing service account keys — як ключі витікають, як їх обмежити і чим їх замінити.
- Estimate and control costs — настанови BigQuery щодо пробних запусків, maximum bytes billed і того, чому `LIMIT` заощаджує так мало.
- Storage classes — класи поруч, з мінімальними строками зберігання, платою за отримання й доступністю.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке Google Cloud?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/google-cloud/