Engineer

Хост

комп'ютер, під'єднаний до мережі

Що це таке

Хост — це комп’ютер на кінці мережевого шляху: машина, якій адресовано трафік і від якої він іде, на відміну від маршрутизаторів і комутаторів, що лише передають його далі. Інженери кажуть також *хост-машина*, ім’я, на яке вона відгукується, називають *ім’ям хоста* (hostname), а у віртуалізації говорять про фізичний хост, на якому працюють гостьові машини. *Хостити* щось, як у слові «хостинг», означає запускати це на такій машині.

Визначення хоста в інтернеті датоване жовтнем 1989 року. RFC 1122, документ із вимогами до інтернет-хостів, називає хост-комп’ютер, або просто хост, кінцевим споживачем послуг зв’язку, машиною, яка зазвичай виконує прикладні програми від імені своїх користувачів. Він відповідає тому, що модель OSI називала кінцевою системою. Мережі між хостами з’єднують шлюзи, які сьогодні називають маршрутизаторами. Той самий документ охоплює все від хостів з одним призначенням до хостів повного обслуговування, а хост із кількома мережевими інтерфейсами називає multihomed.

Межу між хостом і маршрутизатором проводить поведінка, а не залізо. RFC 1122 каже, що будь-який хост, який пересилає датаграми, створені іншим хостом, діє як шлюз, вимагає перемикача, що вимикає функцію шлюзу, і вимагає, щоб цей перемикач за замовчуванням стояв у положенні «вимкнено». Хост із двома мережевими інтерфейсами сам по собі пересилати не починає. Ноутбук, телефон, принтер, орендована віртуальна машина й контейнер із власною адресою — усе це хости.

Глосарій NIST тримає два визначення поруч. Одне зараховує сюди будь-який апаратний пристрій, що має вихід у мережу. Друге, з настанов щодо захисту вебсерверів, каже, що сервер є хостом для своїх клієнтів і що клієнтська

станція теж хост, бо вона є джерелом інформації для мережі, на відміну від маршрутизатора чи комутатора, які спрямовують трафік. Саме тут корисна протилежність до слова «сервер». Сервер — це роль, яку виконує програма, відповідаючи на запити. Хост — це машина, байдуже, відповідає вона комусь чи ні. Один хост може тримати багато серверів, а ноутбук, на якому не працює жоден, усе одно хост.

Хост збирає імена. Супутній документ, RFC 1123, установив правила для імен хостів: першим символом може бути літера або цифра, програмне забезпечення хоста мусить обробляти імена завдовжки до 63 символів; підтримка імен завдовжки до 255 символів рекомендована, а скрізь, де користувач може ввести ім'я хоста, має спрацьовувати й адреса в десятковому записі з крапками. Понад це DNS може спрямувати на одну адресу скільки завгодно імен, а HTTP дає клієнтові сказати, яке з них йому потрібне, у полі `Host` кожного запиту, тож один хост може відповідати за багато сайтів.

Застосуйте поняття до рішення

Застосуйте «Що таке хост?» 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

Хост — одиниця, якою рахує експлуатація. Інвентарі перелічують хости, моніторинг стежить за хостами, правила брандмауера й списки доступу називають їх, а хмарні провайдери виставляють за них рахунки щогодини чи щомісяця. План, що каже «додати хост», конкретний так, як «додати потужності» не буває ніколи: він означає ще одну машину, яку треба створити, назвати, оновлювати, резервно копіювати й оплачувати.

Це також одиниця компрометації. Хто контролює хост, той контролює кожну серверну програму на ньому, кожен ключ на його диску й кожне з'єднання, яке він може відкрити. Те, що тримає хост, визначає ціну його втрати, і тому

уважні оператори для кожного хоста окремо вирішують, які секрети, які дані й які мережеві шляхи він отримає, і не дають йому більшого.

І саме тут сходяться імена. Ту саму машину знають за ім'ям в інвентарі, за ім'ям, яким вона називає себе сама, за DNS-іменами, що вказують на її адресу, і за іменами в запитах, які вона отримує. Коли вони збігаються, рядок журналу, сповіщення й звернення в підтримку ведуть до однієї й тієї самої машини. Коли вони розходяться, людина, яку підняли вночі, витрачає перші хвилини інциденту на пошук машини.

Як це виглядає на практиці

Експлуатаційна робота цього сайту ставиться до хоста як до того, що будують із коду й наділяють власними секретами. Коли платформі знадобилася друга машина в іншого провайдера, зробили так, що другий хост можна створити або повторно підхопити з репозиторію. Першу машину створили вручну, а брандмауер додали згодом, і так лишається проміжок часу, коли щойно створений хост зі стандартною політикою паролів доступний з інтернету. Роль, що створює другу, підхоплює наявну машину замість того, щоб її дублювати, тож повторний запуск безпечний, а в її власному файлі записано тип інстансу, регіон, характеристики й щомісячну вартість у євро, бо це єдина роль у репозиторії, що витрачає гроші.

Перехід від одного хоста до двох потім виявив кожне значення, записане з припущенням, що хост завжди буде один. Кожен операційний секрет став словником, де ключем є хост. Сторінка наводить дві причини, чому спільне використання було хибним. Dead man's switch, спільний для двох хостів, сповіщає рідше, ніж два окремі перемикачі, а не частіше: поки бодай один хост надсилає сигнали, перевірка лишається зеленою, навіть коли другий не працює. А спільна парольна фраза резервних копій пов'язує ризики розкриття даних хостів. Окремі репозиторії restic можуть мати різні головні ключі навіть з однаковою парольною фразою, але той, хто отримає її та зможе прочитати зашифровані дані й файли ключів обох репозиторіїв, зможе відкрити обидва. Наявний хост внесли в усі чотири словники з його репозиторієм і з обома перемикачами порожніми, і сторінка називає це правдивим станом.

Для відвідувача це слово означає щось менше: ім'я, до якого звертається браузер. Сторінка про безпеку пропонує читачеві відкрити панель мережі в браузері й порахувати хости і каже, що він один і що він належить

самому сайту.

Де виникають проблеми

Хост починає пересилати трафік, який мав лише отримувати. Контейнерні мережі й програми VPN вмикають пересилання IP, і відтоді хост маршрутизує між своїми інтерфейсами. Документація Docker, наприклад, каже, що під час запуску він вмикає обидва параметри, наведені нижче, а потім відкидає переслані пакети, якщо їх не приймає якесь правило. Там, де пересилання ввімкнене без такого правила, правила брандмауера, написані для трафіку, адресованого хостові, не чіпають трафік, що проходить крізь нього, і мережа за ним стає досяжною шляхом, якого ніхто не малював. Прочитайте перемикачі й свідомо напишіть правила пересилання скрізь, де вони показують `1`:

```
sysctl net.ipv4.ip_forward net.ipv6.conf.all.forwarding
```

Імена суперечать одне одному. Інвентар каже одне, машина називає себе так, як вирішив образ провайдера, у DNS третє ім'я, а в TLS-сертифікаті четверте. Тоді кожне сповіщення приходить з іменем, яким ніхто не користується. Беріть власне ім'я машини з того самого джерела, що й інвентар і DNS-записи, і задавайте його під час створення хоста, а не тоді, коли хтось це помітить.

Сервер відповідає на будь-яке ім'я хоста, яке йому надіслали. Поле `Host` приходить від клієнта, і сервер, що відповідає на невідомі імена сайтом за замовчуванням, будує посилання, переспрямування й кешовані сторінки з імені, яке вибрав зловмисник. RFC 9110 застерігає, що це поле часто стає ціллю шкідливих програм, які намагаються отруїти спільний кеш або переспрямувати запит на непередбачений сервер. Відповідайте лише на ті імена, які хост справді обслуговує, відхиляйте решту й будуйте абсолютні посилання з конфігурації, а не із запиту.

Клоновані хости мають одну ідентичність на всіх. Машина, скопійована з образу, несе все, що було в образі: SSH-ключі хоста, токени, часом парольну фразу резервних копій. Тоді клієнти вже не можуть відрізнити копії одну від одної, а один витік відчиняє кожну з них. Генеруйте ключі хоста під час першого завантаження, не кладіть секрети в образи й давайте кожному хостові власний запис скрізь, де задається секрет.

Що почитати далі

- host — NIST CSRC Glossary — обидва визначення, зокрема те, що протиставляє хости маршрутизаторам і комутаторам.
- RFC 1122: Requirements for Internet Hosts, Communication Layers — визначення хоста 1989 року, multihoming і пересилання, яке за замовчуванням вимкнене.
- RFC 1123: Requirements for Internet Hosts, Application and Support — правила для імен хостів та їхньої довжини в розділі 2.1.
- RFC 9110, HTTP Semantics: Host and :authority — як один сервер розрізняє багато імен хостів і чому це поле стає ціллю.

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 хост?» 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/host/