WebConf 2024 Taiwan
2024/12/27

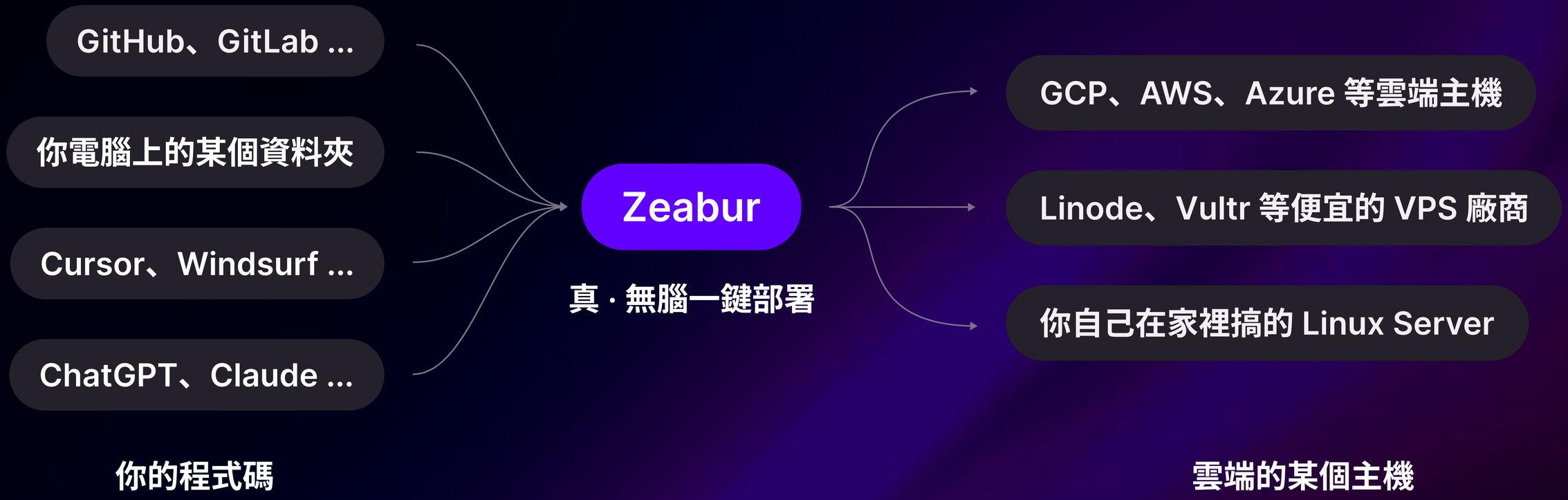
雲端部署平台核心技術大揭秘

Yuanlin Lin 林沅霖

創辦人 & CEO, Zeabur

WebConf 2024 Taiwan
2024/12/27

Zeabur 是什麼？簡單來說 ...



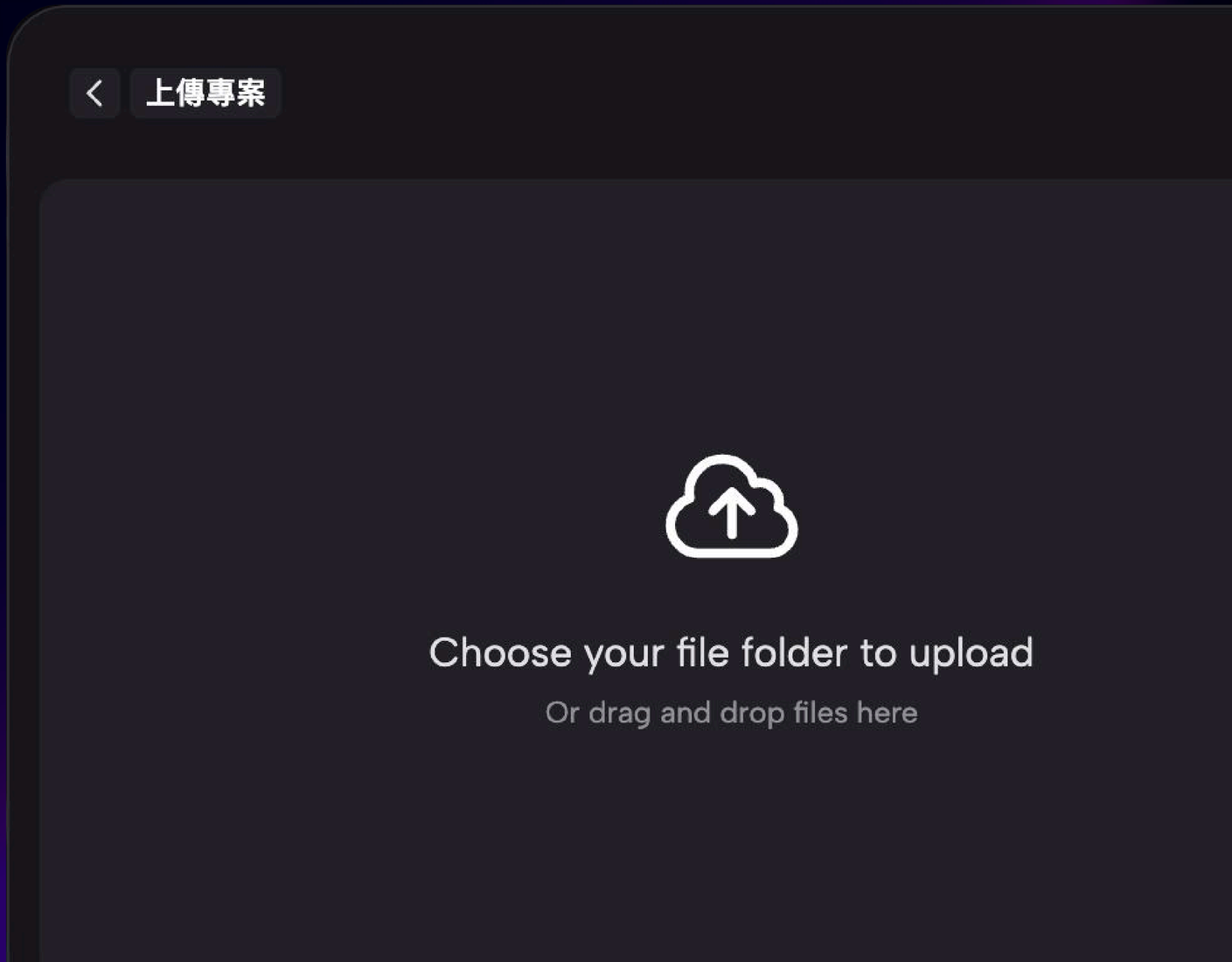
WebConf 2024 Taiwan
2024/12/27

工程師最愛的部署方法 ☕

從 GitHub 一鍵部署

不會用 Git 😨 別擔心

從桌面直接拖上來
也能部署



喜歡用 CLI？我懂你 😉

終端機輸入指令也能部署

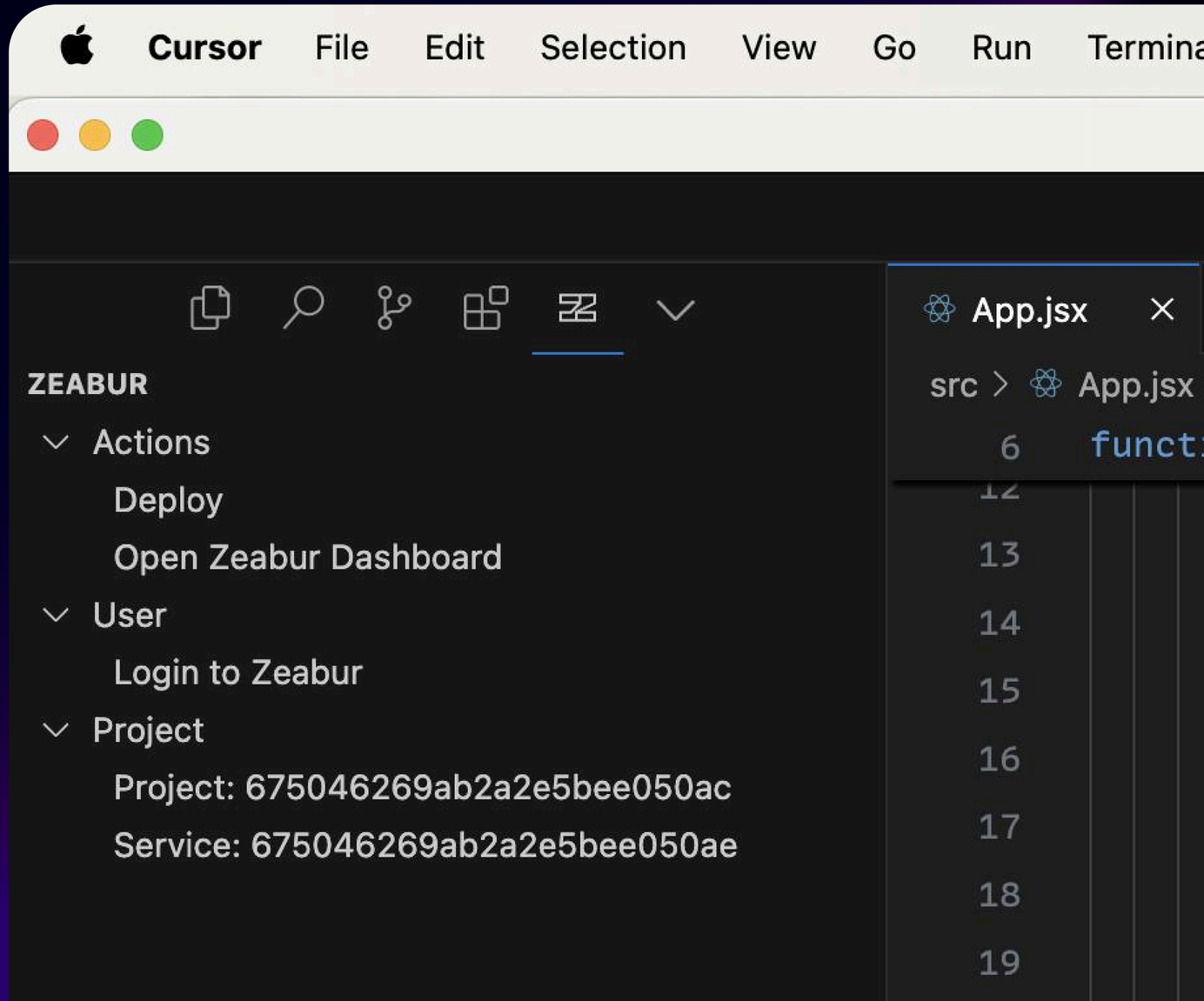
```
▶
~/Developer/vite-template via ⍰ v22.2.0 on ☁️  (ap-northeast-1) on ☁️  yuanlin@zeabur.com took 8s
❯ npx zeabur deploy
INFO    Select one project to deploy your service.
? Select project Create a new project
? Select project region Amazon Web Services - ap-east-1 (Hong Kong)
INFO    Only one environment in current project, select <production> automatically

INFO    Select one service to deploy or create a new one.
INFO    No service found, create a new one.
Service deployed successfully, you can access it via:
https://dash.zeabur.com/projects/6762ccf25cefea049a3e60b4/services/6762ccf3491a30e01c57717b?envID=6762ccf2364e13ab91986d55
▶
~/Developer/vite-template via ⍰ v22.2.0 on ☁️  (ap-northeast-1) on ☁️  yuanlin@zeabur.com took 12s
❯
```

WebConf 2024 Taiwan
2024/12/27

程式碼是 AI 🤖 幫我寫的

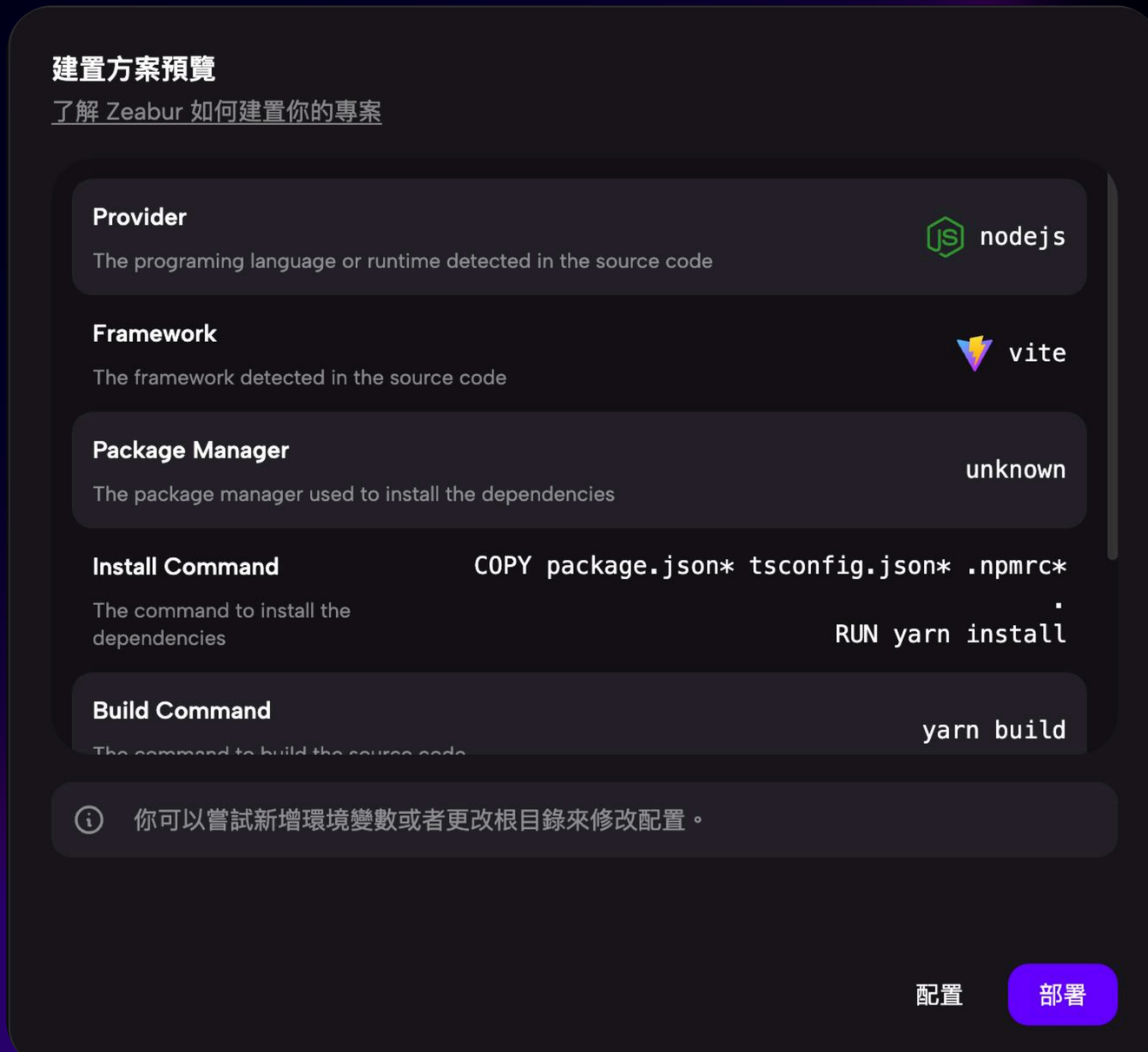
那就從 Cursor 裡面直接部署

其實從 Windsurf 或 VSCode 也可以，反正就是 VSCode 插件 🤣



連 Dockerfile 都不用寫 😌

自動根據程式碼內容
產生構建計畫



WebConf 2024 Taiwan
2024/12/27

Shared Cluster

彈性共享叢集

基於公有雲的 Managed Kubernetes 服務

WebConf 2024 Taiwan
2024/12/27

Dedicated Server

專用伺服器

基於 K3S 實現的單節點 Kubernetes 叢集

WebConf 2024 Taiwan
2024/12/27

01 About Zeabur

02 Architecture

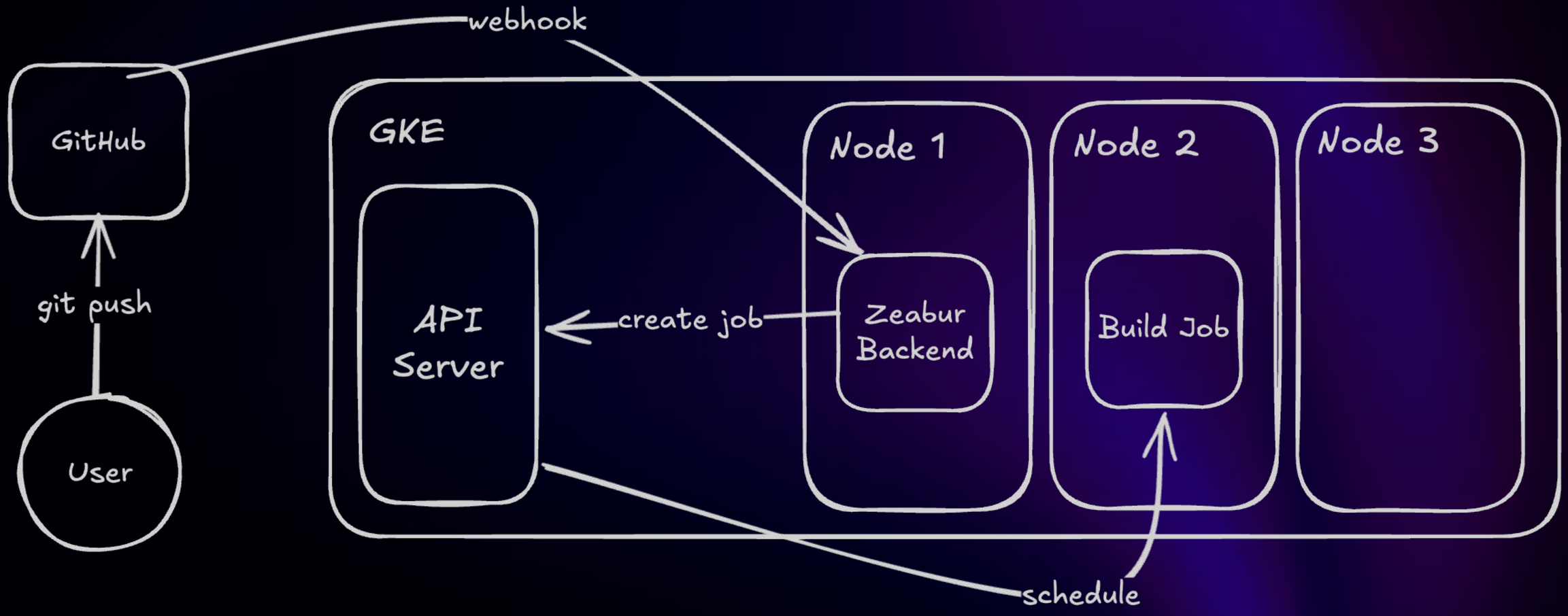
03 Storage

04 Builder

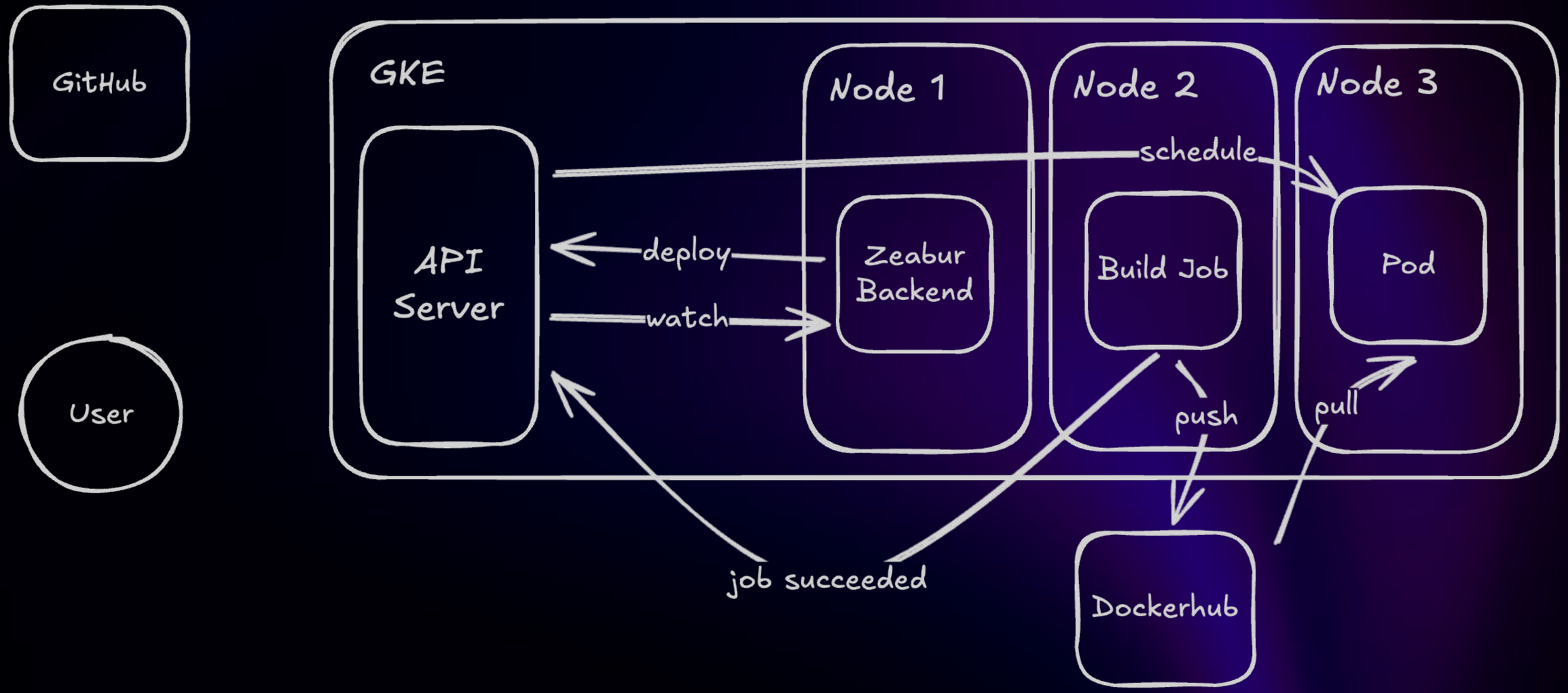
05 Ingress Layer

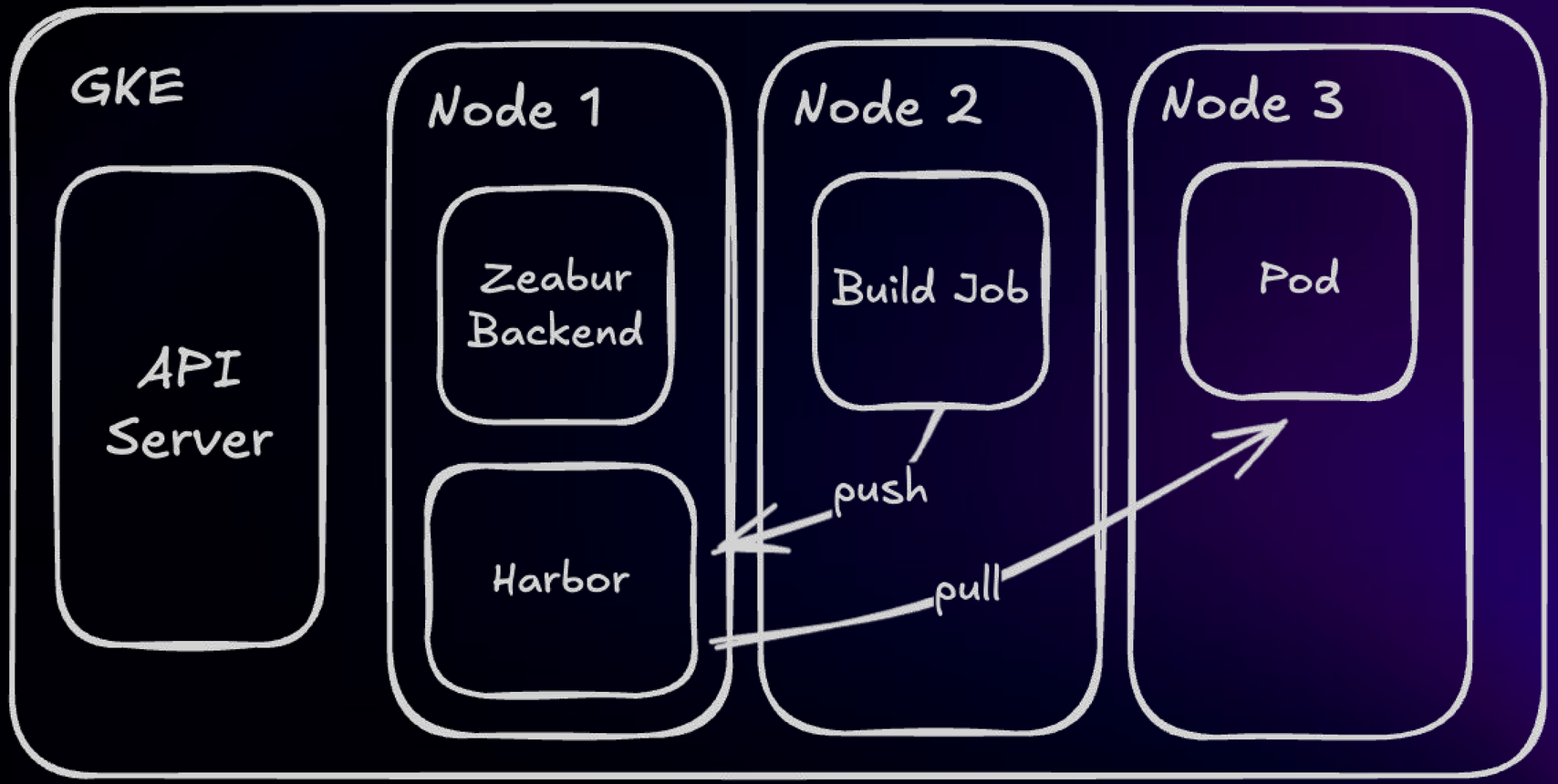
06 Observability

Zeabur 最初代的架構（畢業論文時期）



Zeabur 最初代的架構（畢業論文時期）



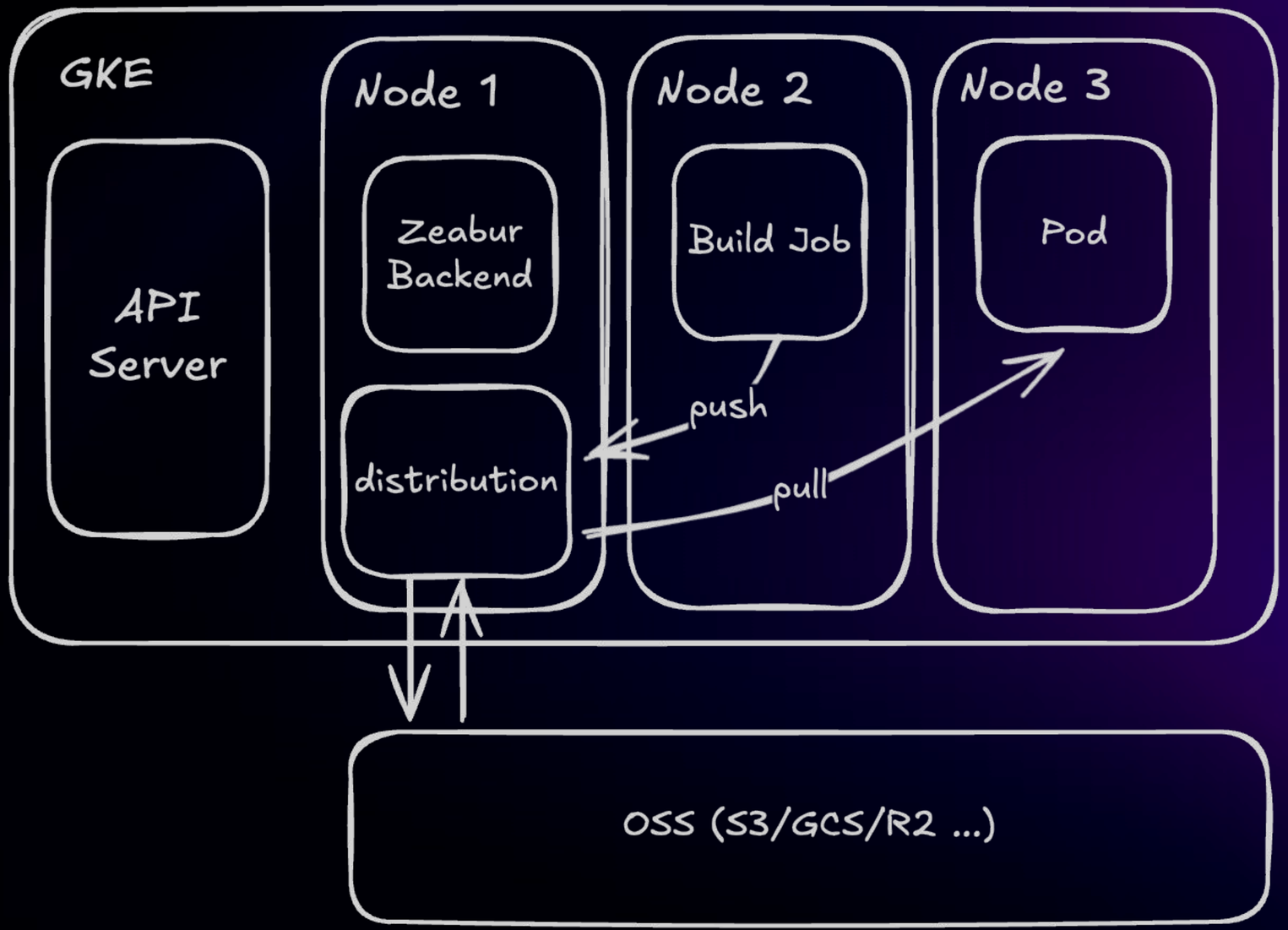


Problem:

後來發現從 Dockerhub 拉取的延遲太高

Solution:

改用 Harbor 走內網



Problem:

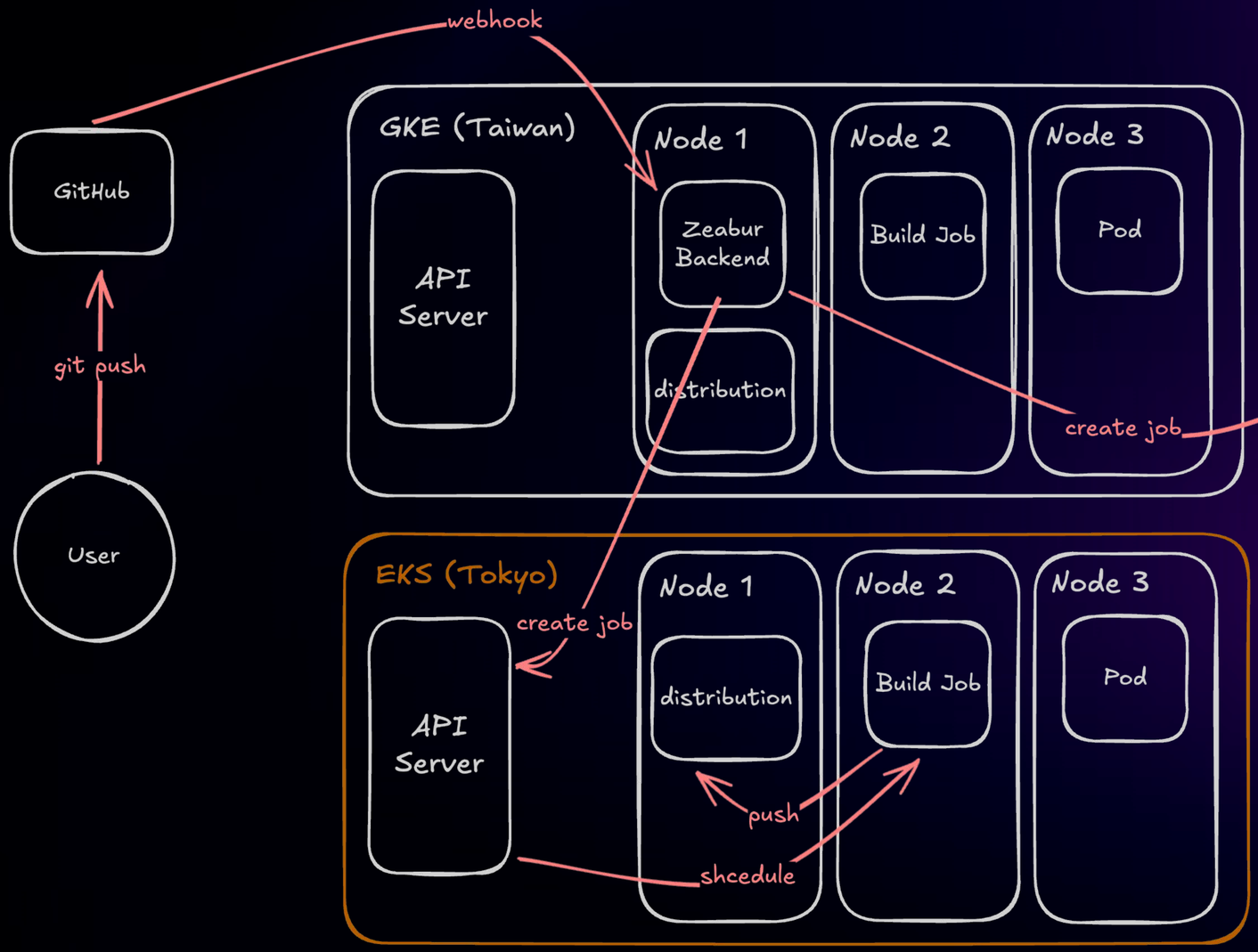
Harbor 開銷太大，且併發效率低

Solution:

改用 docker 官方的 distribution
搭配 OSS 作為 storage backend

Advantage:

distribution 本身是無狀態的
可以無限水平伸縮
OSS (S3, GCS, R2) 的併發量超高



Problem:

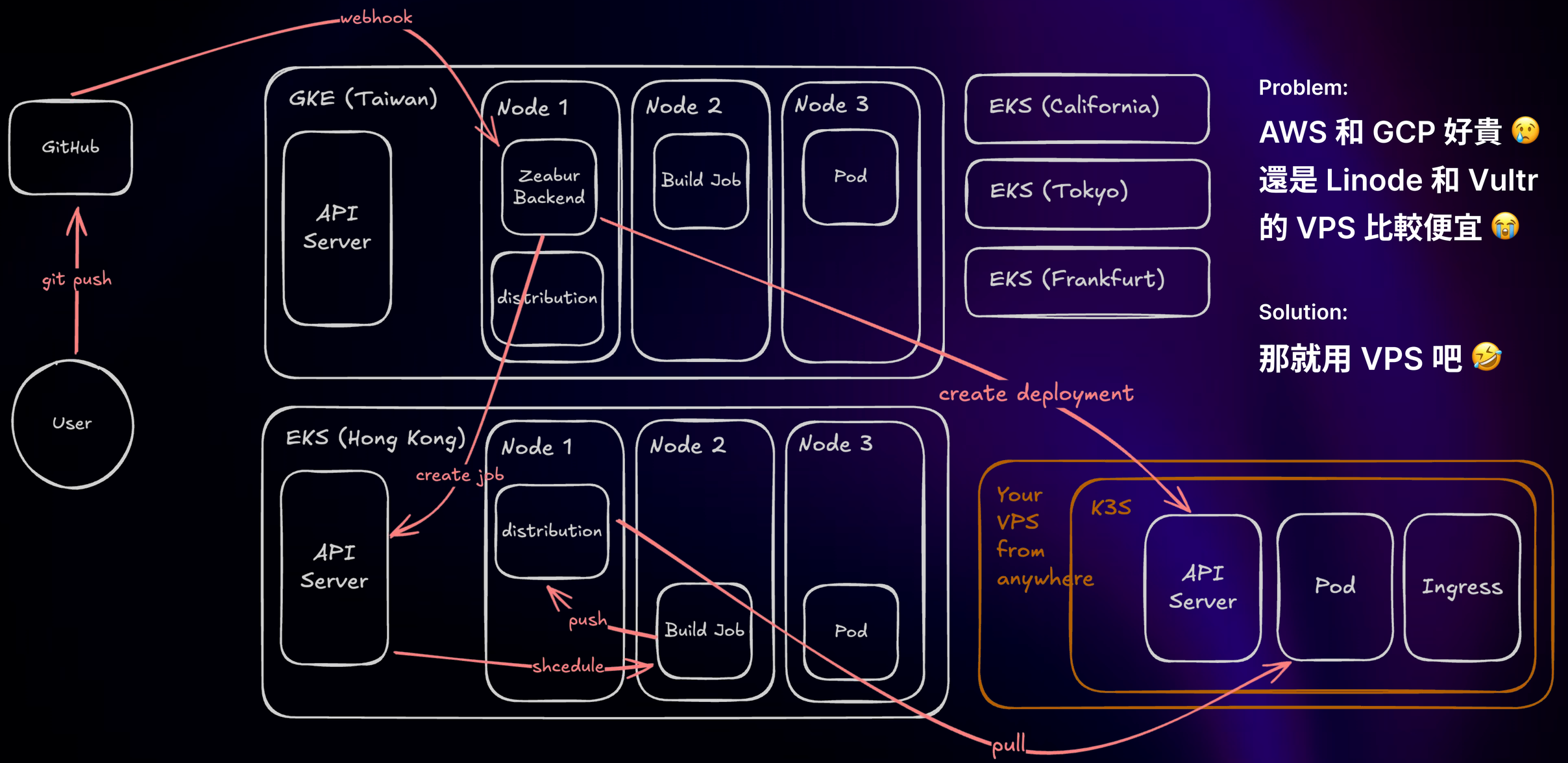
單個 Region 沒辦法服務全球的客戶

Solution:

在各個地方都開一個叢集

後端根據 Region 去用不同的 Kubernetes API

WebConf 2024 Taiwan
2024/12/27



Problem:

AWS 和 GCP 好貴 😢
還是 Linode 和 Vultr 的 VPS 比較便宜 😭

Solution:

那就用 VPS 吧 🤣

WebConf 2024 Taiwan
2024/12/27

Persistent Storage

GCP (GKE)	Persistent Disk CSI
AWS (EKS)	AWS EBS CSI
Digital Ocean (DOKS)	DO Block Storage CSI
Vultr (VKE)	Vultr Block Storage CSI

Persistent Storage

GCP (GKE)	Persistent Disk CSI	
AWS (EKS)	~~AWS EBS CSI~~	一個 Node 最多掛 16 個
Digital Ocean (DOKS)	~~DO Block Storage CSI~~	一個 Node 最多掛 16 個
Vultr (VKE)	~~Vultr Block Storage CSI~~	一個 Node 最多掛 16 個

Persistent Storage

GCP (GKE)	Persistent Disk CSI	
AWS (EKS)	~~AWS EBS CSI~~	AWS EFS CSI
Digital Ocean (DOKS)	~~DO Block Storage CSI~~	一個 Node 最多掛 16 個
Vultr (VKE)	~~Vultr Block Storage CSI~~	一個 Node 最多掛 16 個

Persistent Storage

GCP (GKE)	Persistent Disk CSI	
AWS (EKS)	~~AWS EBS CSI~~	AWS EFS CSI
Digital Ocean (DOKS)	~~DO Block Storage CSI~~	Ceph RBD CSI
Vultr (VKE)	~~Vultr Block Storage CSI~~	Ceph RBD CSI

Persistent Storage

GCP (GKE)	Persistent Disk CSI	雖然沒有數量限制， 但每一顆 PD 的大小都需要提前指定 並且按指定的量付費
AWS (EKS)	~~AWS EBS CSI~~	AWS EFS CSI
Digital Ocean (DOKS)	~~DO Block Storage CSI~~	Ceph RBD CSI
Vultr (VKE)	~~Vultr Block Storage CSI~~	Ceph RBD CSI

Persistent Storage

GCP (GKE)	Persistent Disk CSI	
AWS (EKS)	~~AWS EBS CSI~~	AWS EFS CSI
Digital Ocean (DOKS)	~~DO Block Storage CSI~~	Ceph RBD CSI
Vultr (VKE)	~~Vultr Block Storage CSI~~	Ceph RBD CSI

雖然按量計費，
但 Throughput modes 有一堆坑 = =

Throughput modes

A file system's throughput mode determines the throughput available to your file system. Amazon EFS offers three throughput modes: Elastic, Provisioned, and Bursting. Read throughput is discounted to allow you to drive higher read throughput than write throughput. The maximum throughput available with each throughput mode depends on the AWS Region. For more information about the maximum file system throughput in the different regions, see Amazon EFS quotas.

Your file system can achieve a combined 100% of its read and write throughput. For example, if your file system is using 33% of its read throughput limit, the file system can simultaneously achieve up to 67% of its write throughput limit. You can monitor your file system's throughput usage in the **Throughput utilization (%)** graph on the on the **File System Detail** page of the console. For more information, see Monitoring throughput performance.

Choosing the correct throughput mode for a file system

Choosing the correct throughput mode for your file system depends on your workload's performance requirements.

- **Elastic throughput** (Recommended) – Use the default Elastic throughput when you have spiky or unpredictable workloads and performance requirements that are difficult to forecast, or when your application drives throughput at an average-to-peak ratio of 5% or less. For more information, see Elastic throughput.
- **Provisioned throughput** – Use Provisioned throughput if you know your workload's performance requirements, or when your application drives throughput at an average-to-peak ratio of 5% or more. For more information, see Provisioned throughput.
- **Bursting throughput** – Use Bursting throughput when you want throughput that scales with the amount of storage in your file system.

  If, after using Bursting throughput, you find that your application is throughput-constrained (for example, it uses more than 80% of the permitted throughput or you have used all of your burst credits), then you should use either Elastic or Provisioned throughput. For more information, see Bursting throughput.

You can use Amazon CloudWatch to determine your workload's average-to-peak ratio by comparing the `MeteredIOBytes` metric to the `PermittedThroughput` metric. For more information about Amazon EFS metrics, see CloudWatch metrics for Amazon EFS.

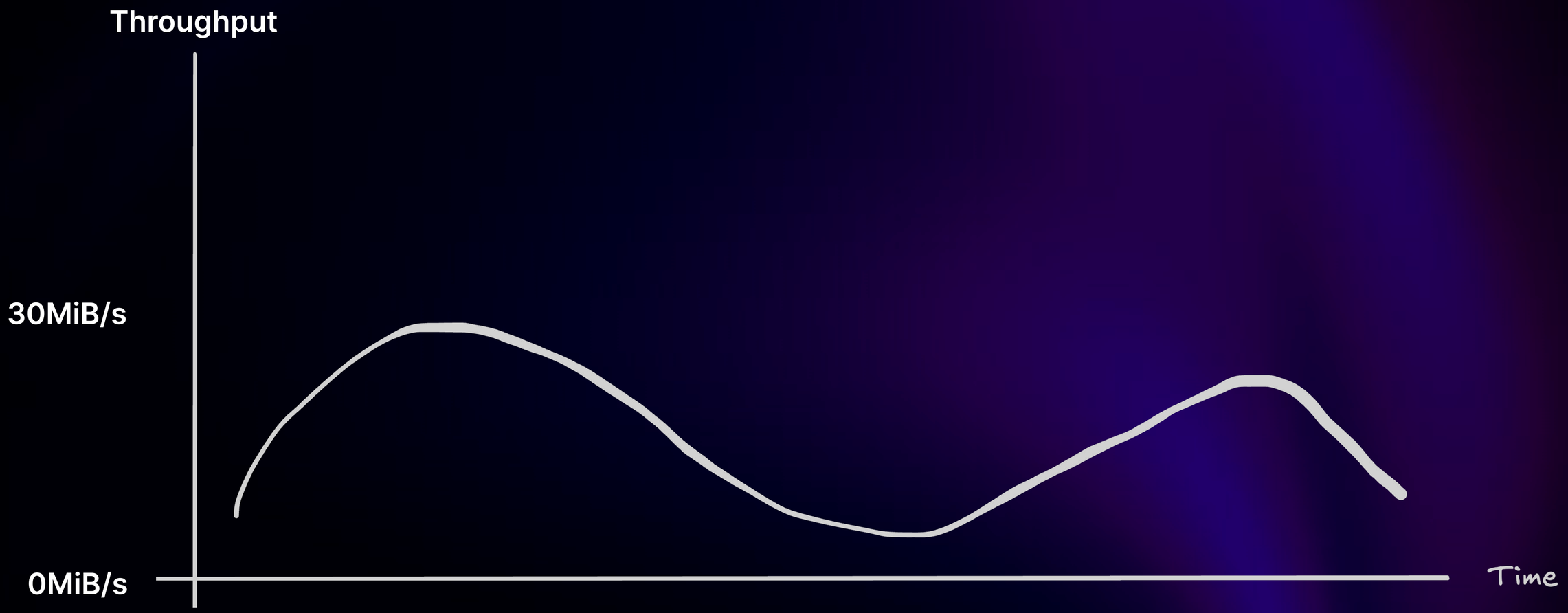
Storage：AWS EFS CSI

三種不同的 Throughput Mode

	Elastic（預設）	Provisioned	Bursting
簡單來說：	讀寫吞吐量最大 按流量計費 🙀	想要多少吞吐量 就付錢買多少	不需要額外為吞吐量付費 根據 EFS 實際容量計算出 baseline 吞吐低於 baseline 就存 credits 吞吐高於 baseline 就消耗 credits 沒 credits 以後速度降到 baseline

Storage：AWS EFS CSI

Bursting Throughput Mode

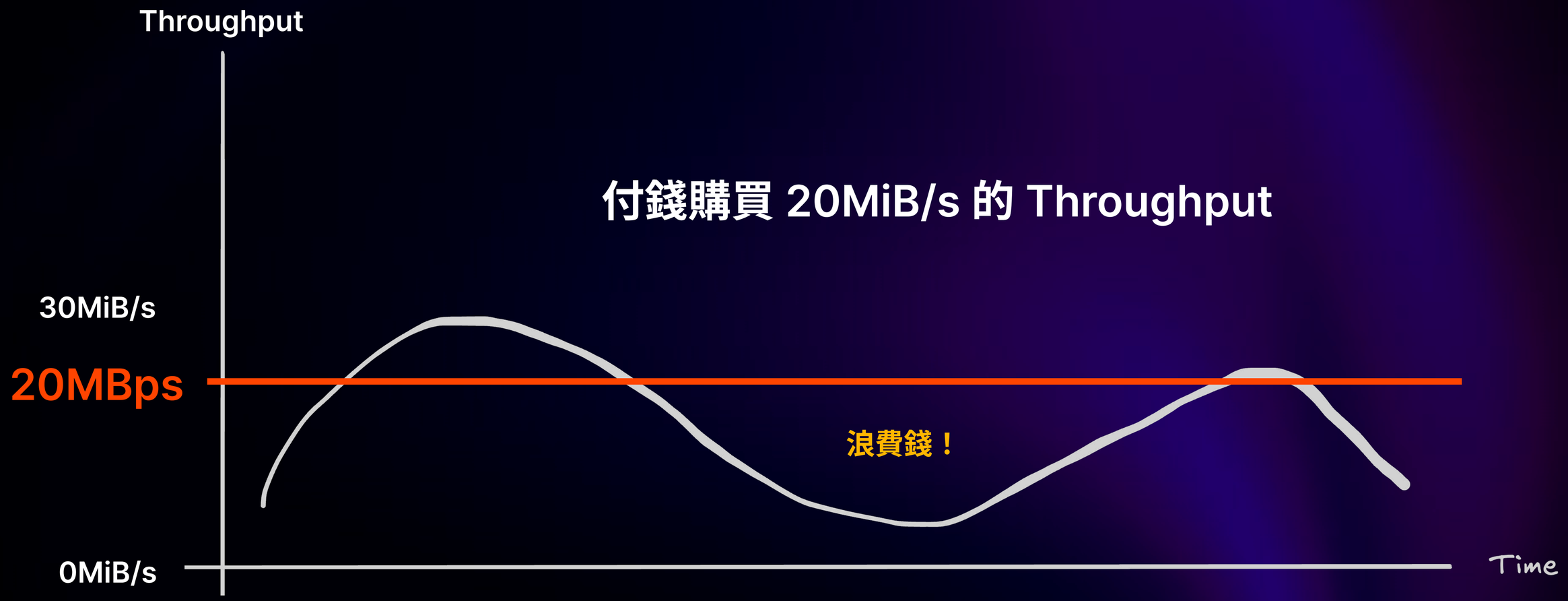


Storage：AWS EFS CSI

Bursting Throughput Mode

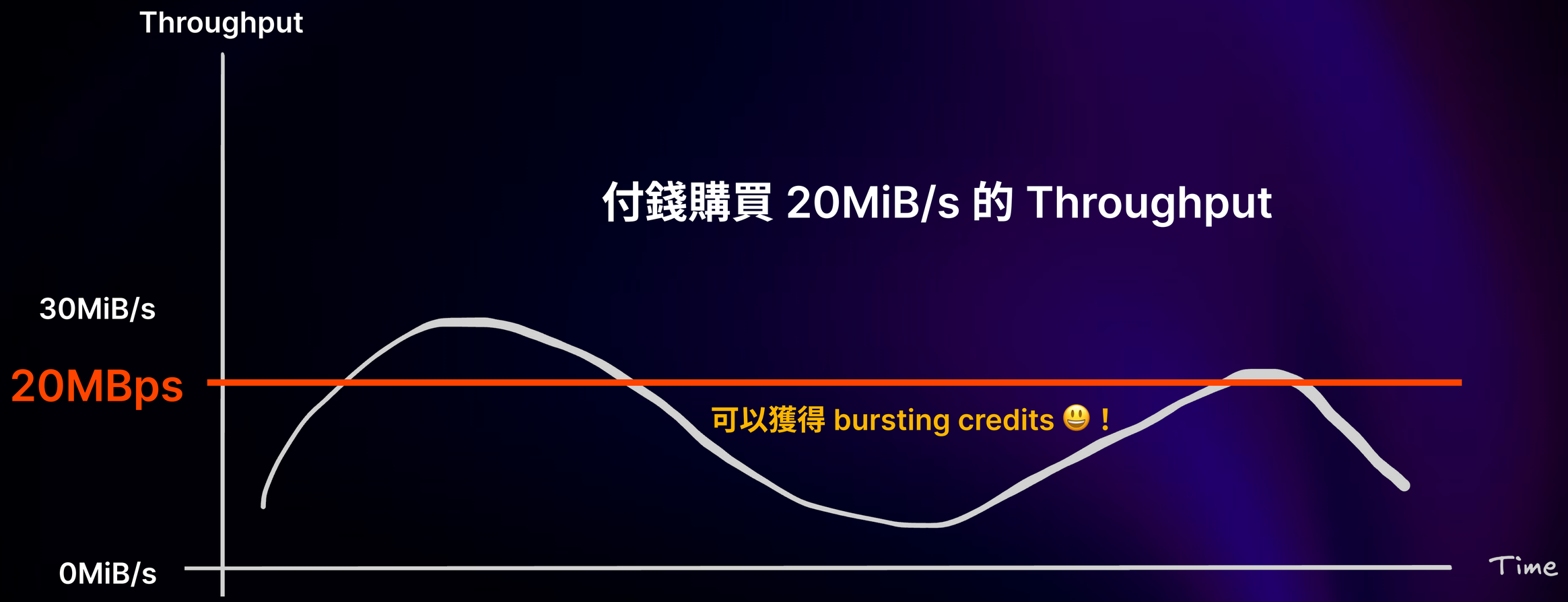
Storage：AWS EFS CSI

Provisioned Throughput Mode



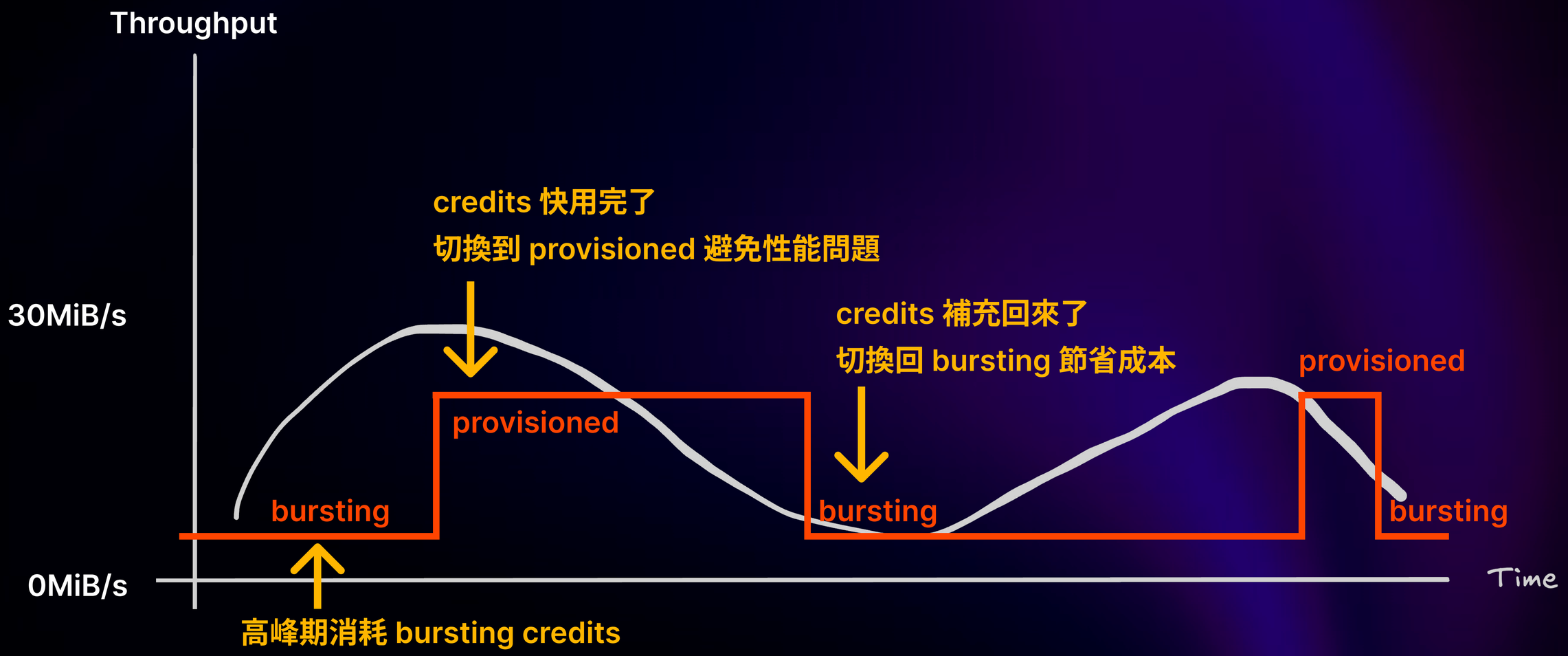
Storage：AWS EFS CSI

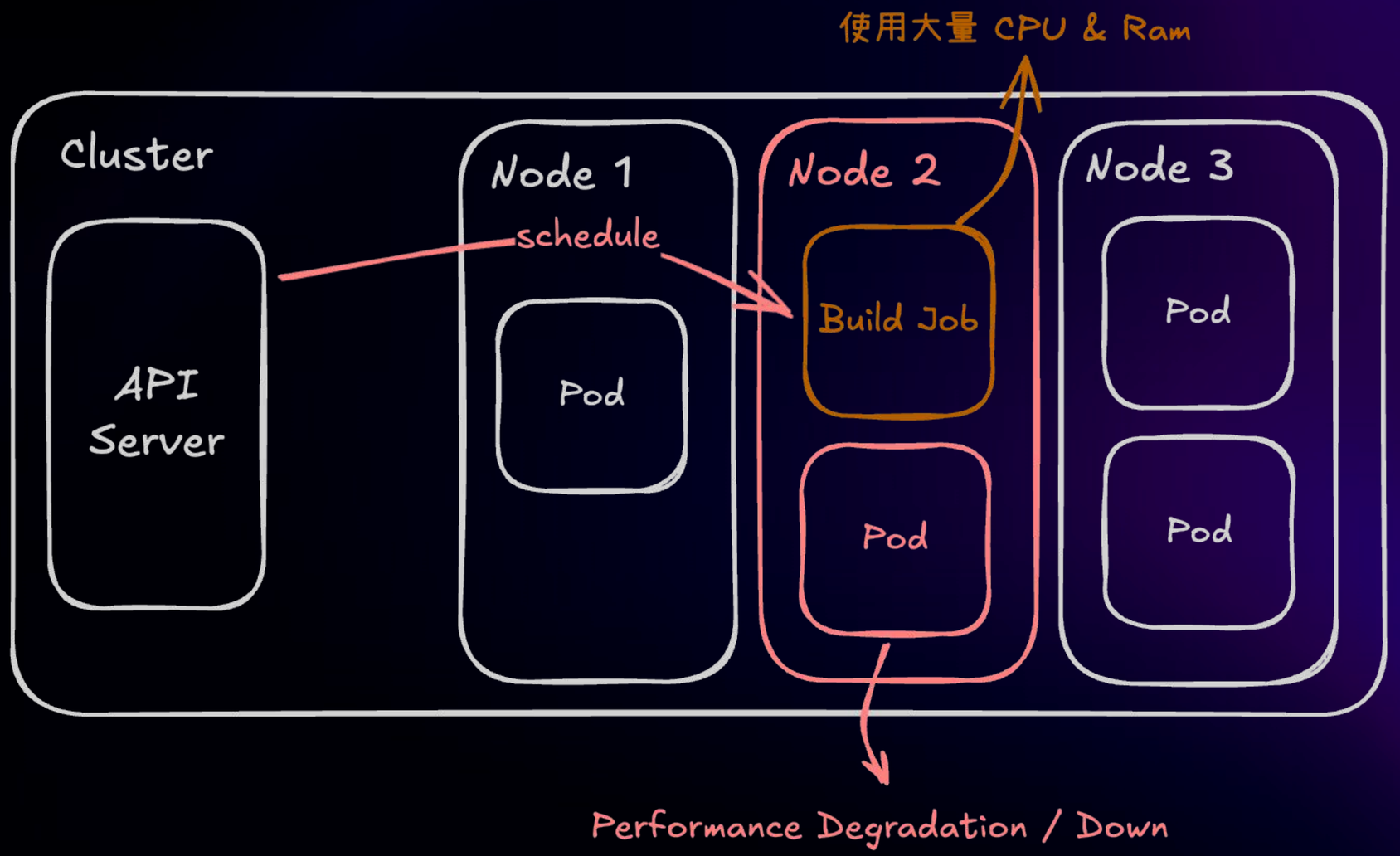
Provisioned Throughput Mode



Storage：AWS EFS CSI

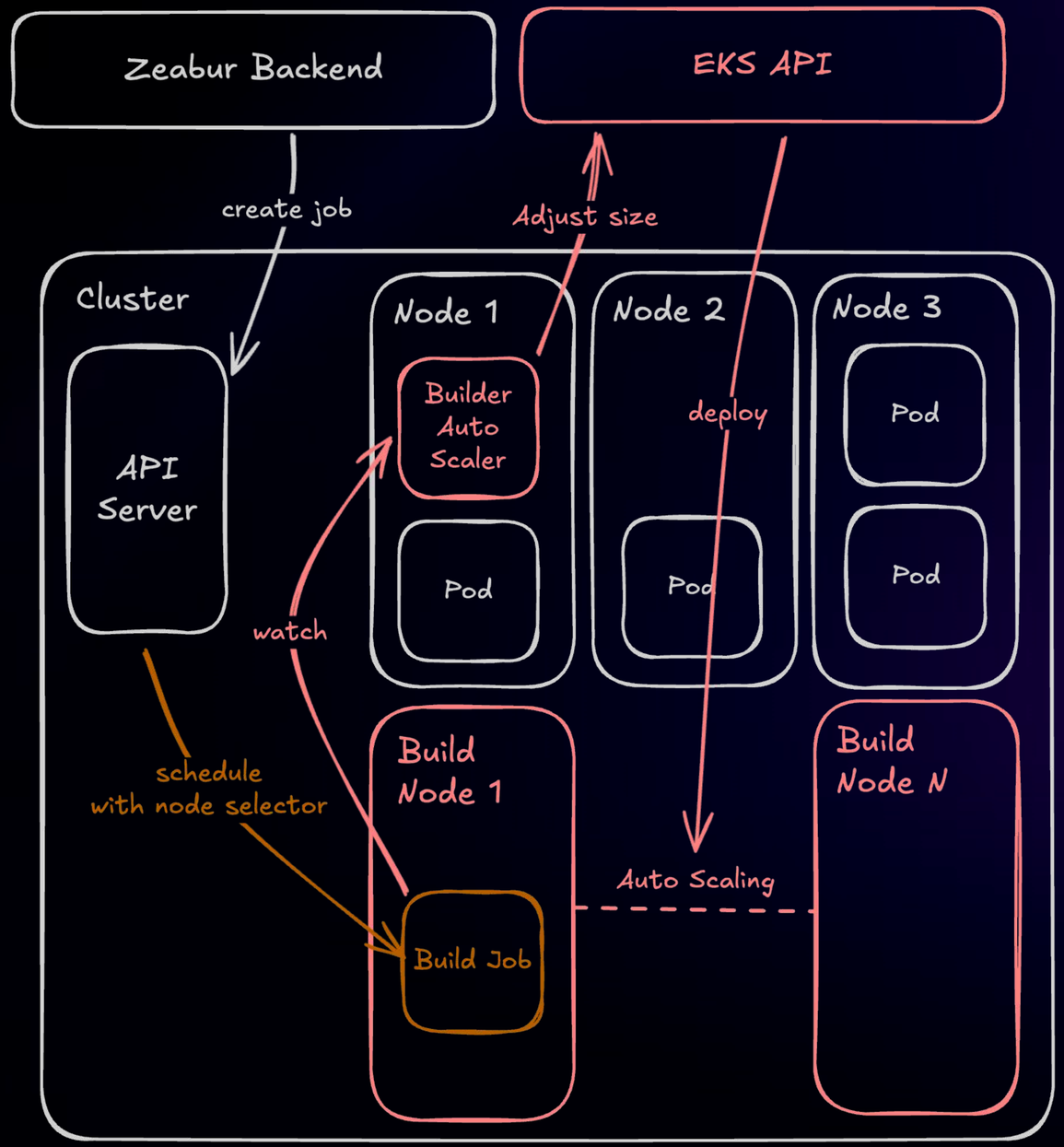
動態根據 EFS Bursting Credits 自動切換 Bursting / Provisioned





Problem:

Build 需要使用大量資源
影響同個節點的其他 Pod 的性能
而且大量同時 Build 會導致
整個 Region 不穩定



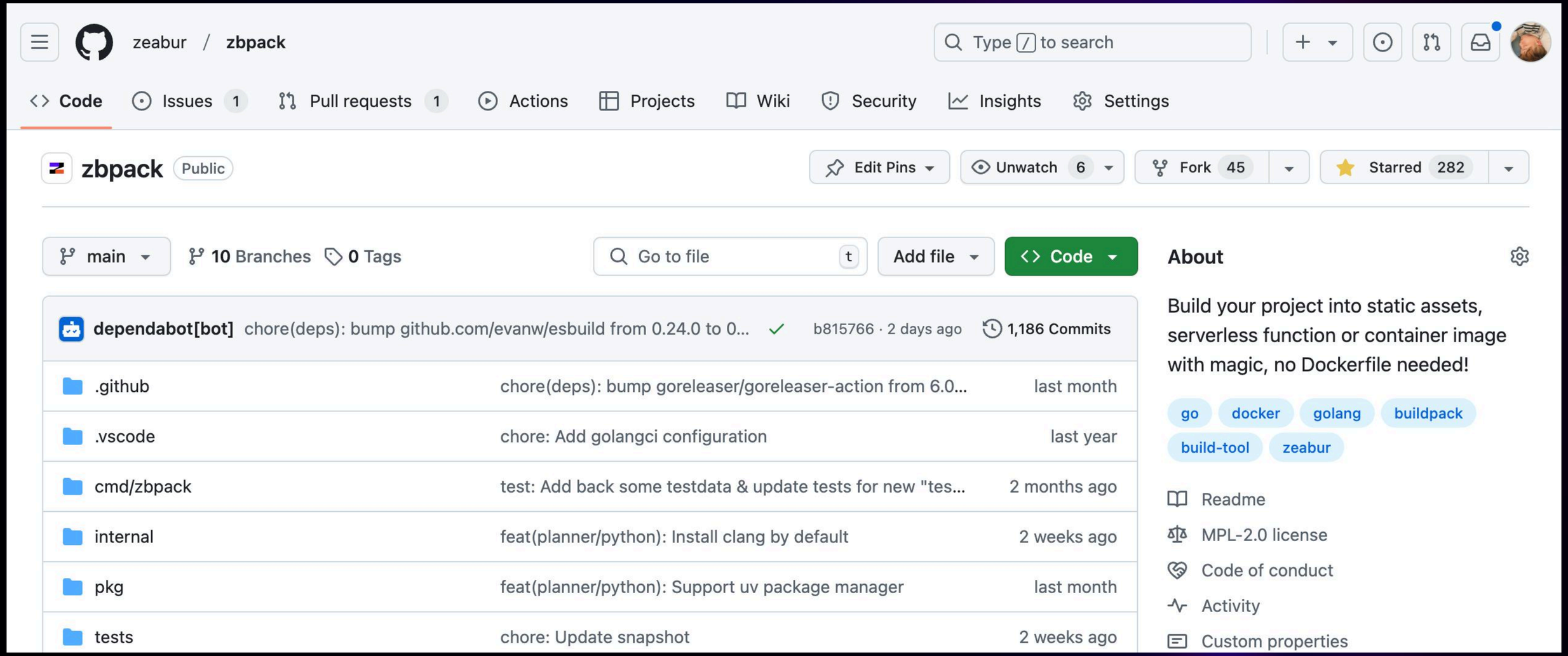
Problem:

Build 需要使用大量資源
影響同個節點的其他 Pod 的性能
而且大量同時 Build 會導致
整個 Region 不穩定

Solution:

專門運行一組 Builder Nodes 來跑 Job
根據 Jobs 數量呼叫 EKS API 進行自動擴縮容
節省成本並降低 CI/CD 的排隊等待時間

WebConf 2024 Taiwan
2024/12/27



建置方案預覽

了解 Zeabur 如何建置你的專案

Provider
The programing language or runtime detected in the source code
nodejs

Framework
The framework detected in the source code
vite

Package Manager
The package manager used to install the dependencies
unknown

Install Command
The command to install the dependencies

```
COPY package.json* tsconfig.json* .npmrc*
.
RUN yarn install
```

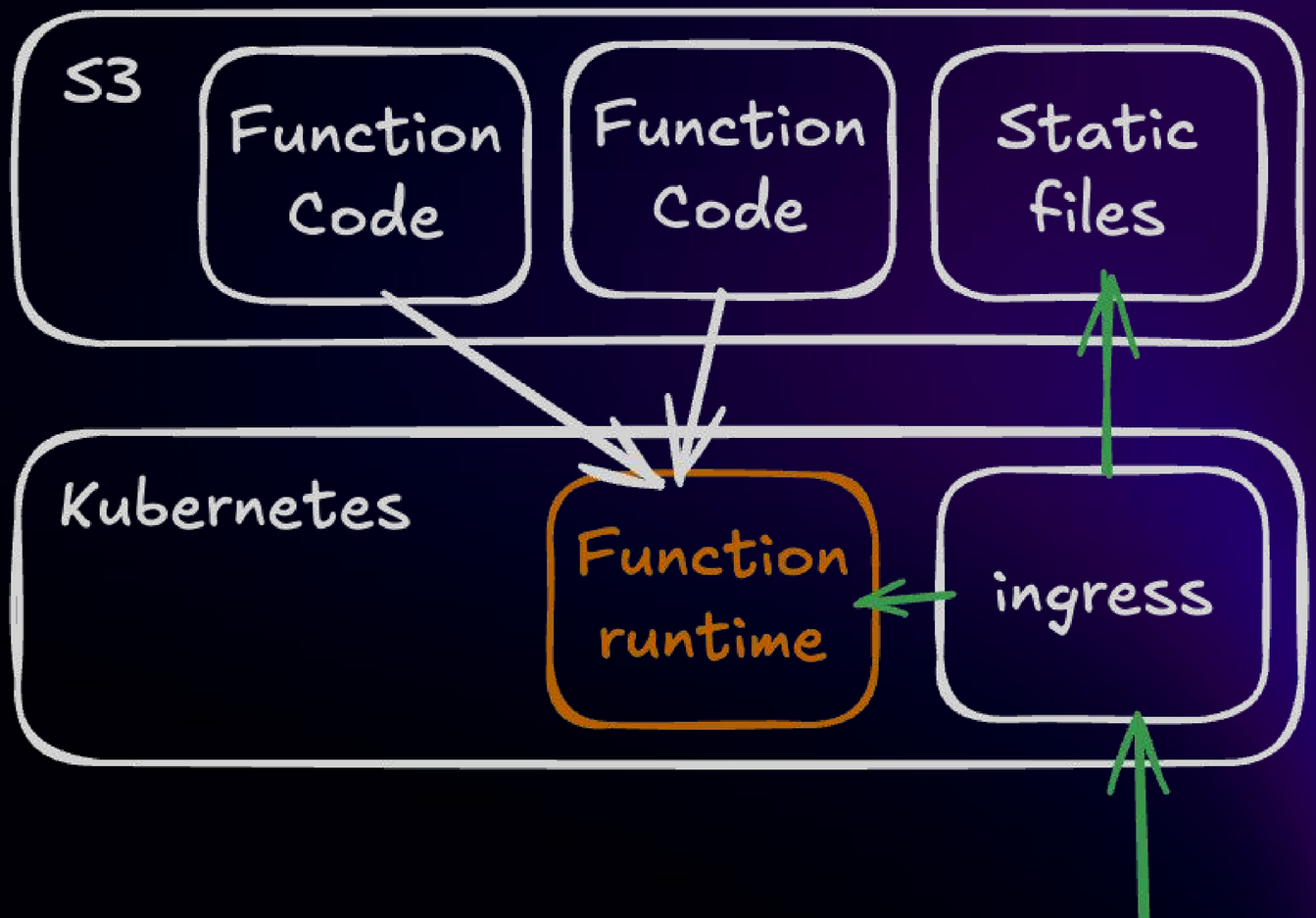
Build Command
The command to build the source code
yarn build

你可以嘗試新增環境變數或者更改根目錄來修改配置。

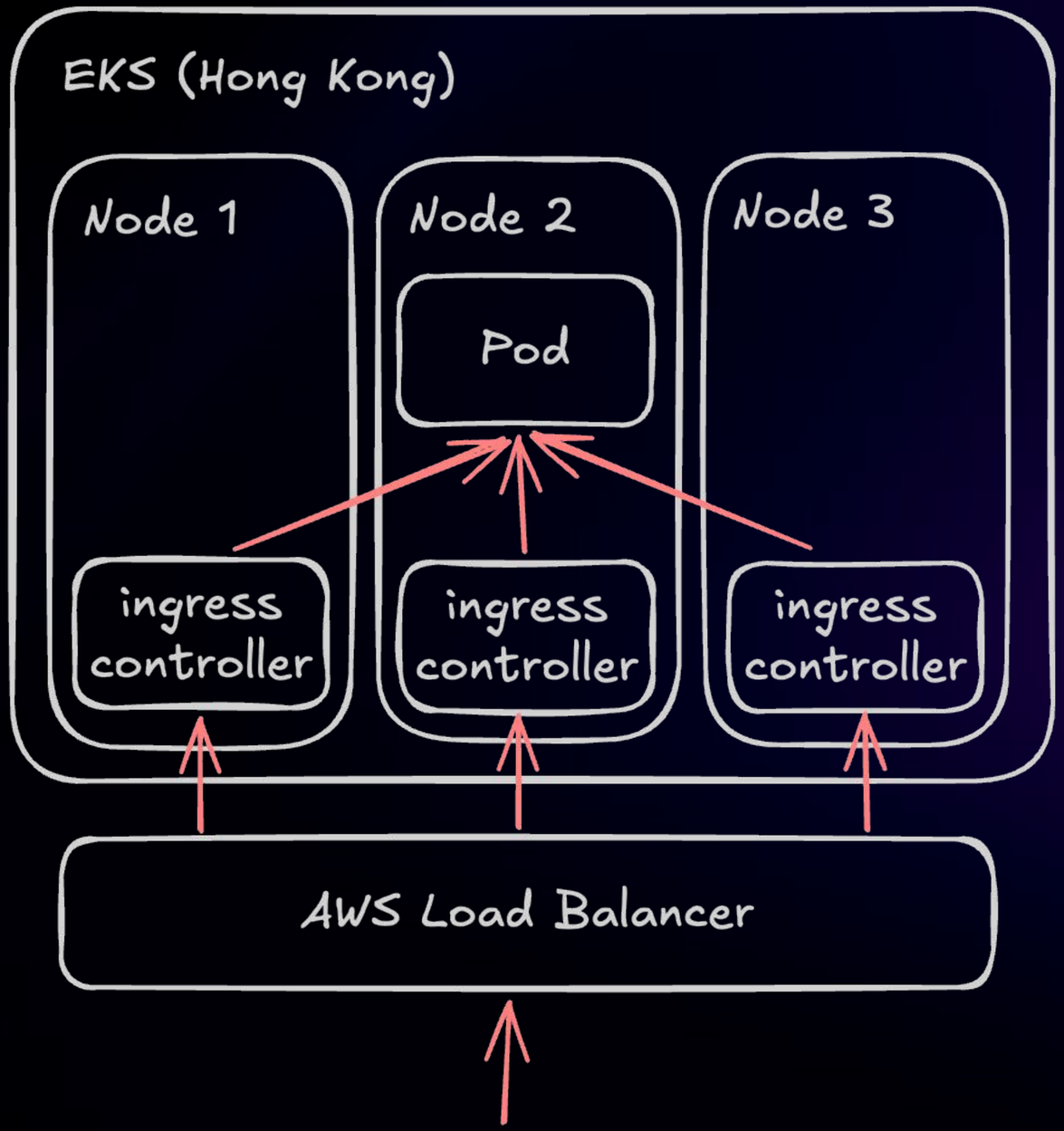
配置 部署

曾經走過的彎路

Serverless Mode

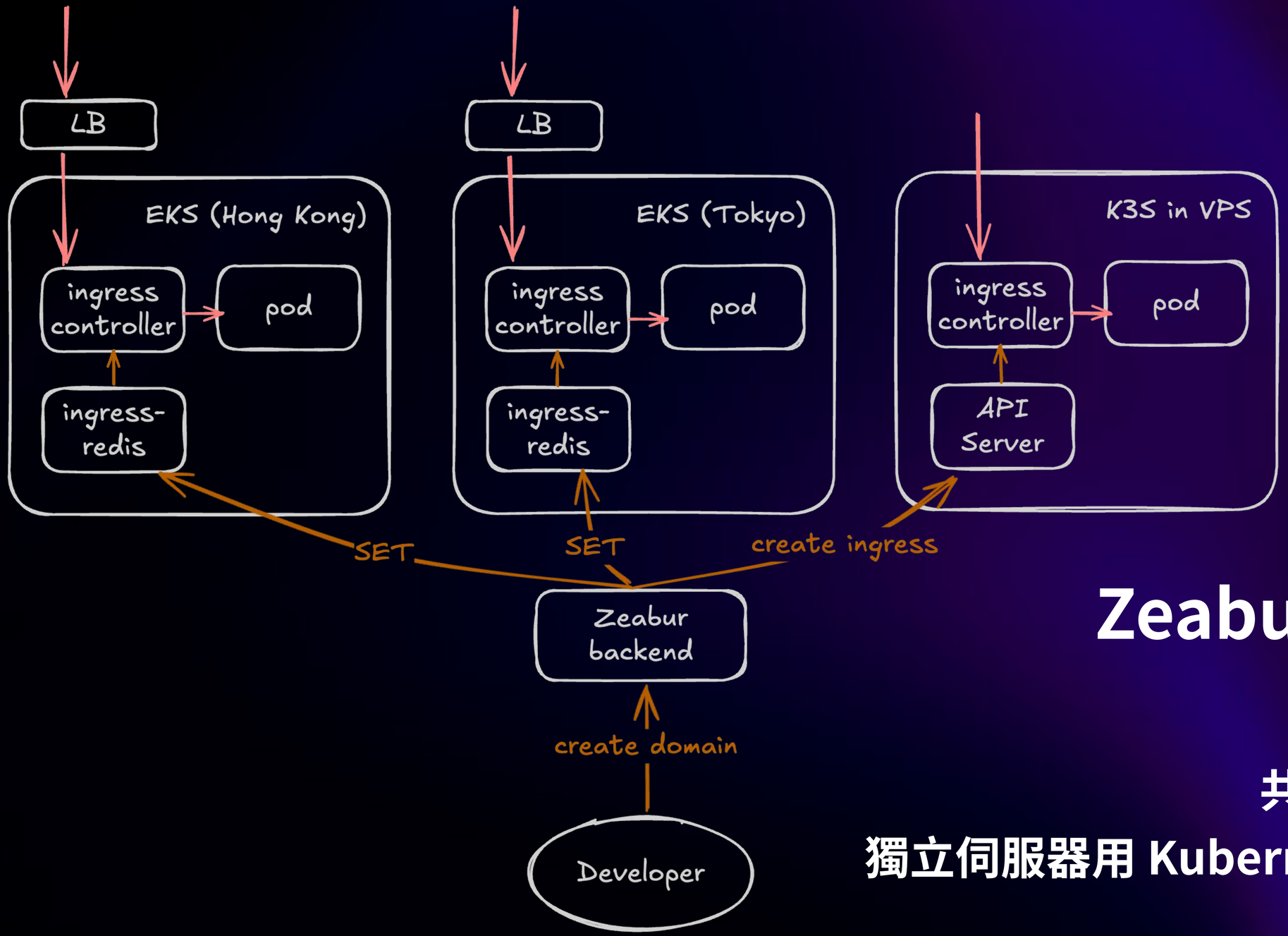


WebConf 2024 Taiwan
2024/12/27



基本 ingress 架構

Question:
ingress controller 怎麼知道
請求要發給哪個 Pod？



Zeabur 目前方案

共享集群用 Redis

獨立伺服器用 Kubernetes Resource

下一個問題

DDoS 攻擊 😨

主流 DDoS 攻擊類型

L4 傳輸層攻擊

消耗網路頻寬和連接資源

容易識別、清洗

大型公有雲的 L4 LB 預設有基礎防禦

L7 應用層攻擊

消耗 CPU、記憶體等計算資源

和普通請求沒有明顯差異

需要額外開啟和設定 WAF 規則等

主流 DDoS 攻擊類型

L4 傳輸層攻擊

消耗網路頻寬和連接資源

容易識別、清洗

大型公有雲的 L4 LB 預設有基礎防禦

如果是小廠 / VPS 的話呢？

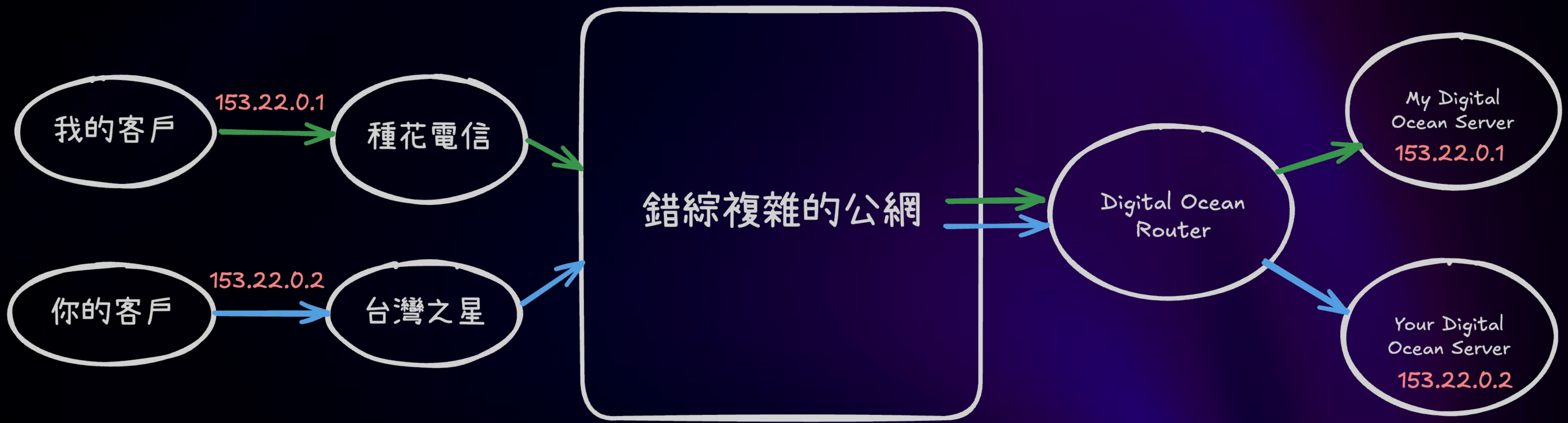
L7 應用層攻擊

消耗 CPU、記憶體等計算資源

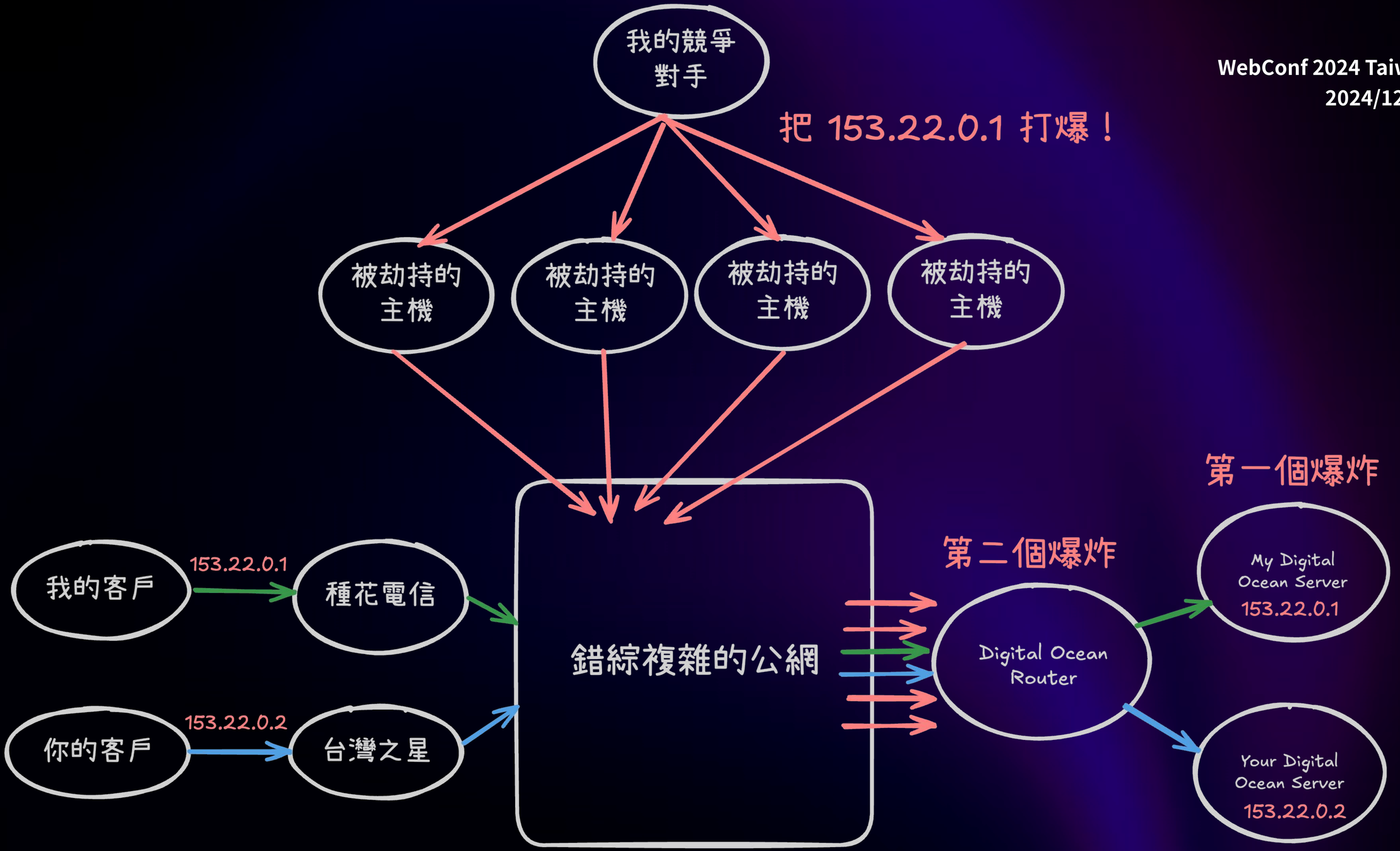
和普通請求沒有明顯差異

需要額外開啟和設定 WAF 規則等

WebConf 2024 Taiwan
2024/12/27



WebConf 2024 Taiwan
2024/12/27

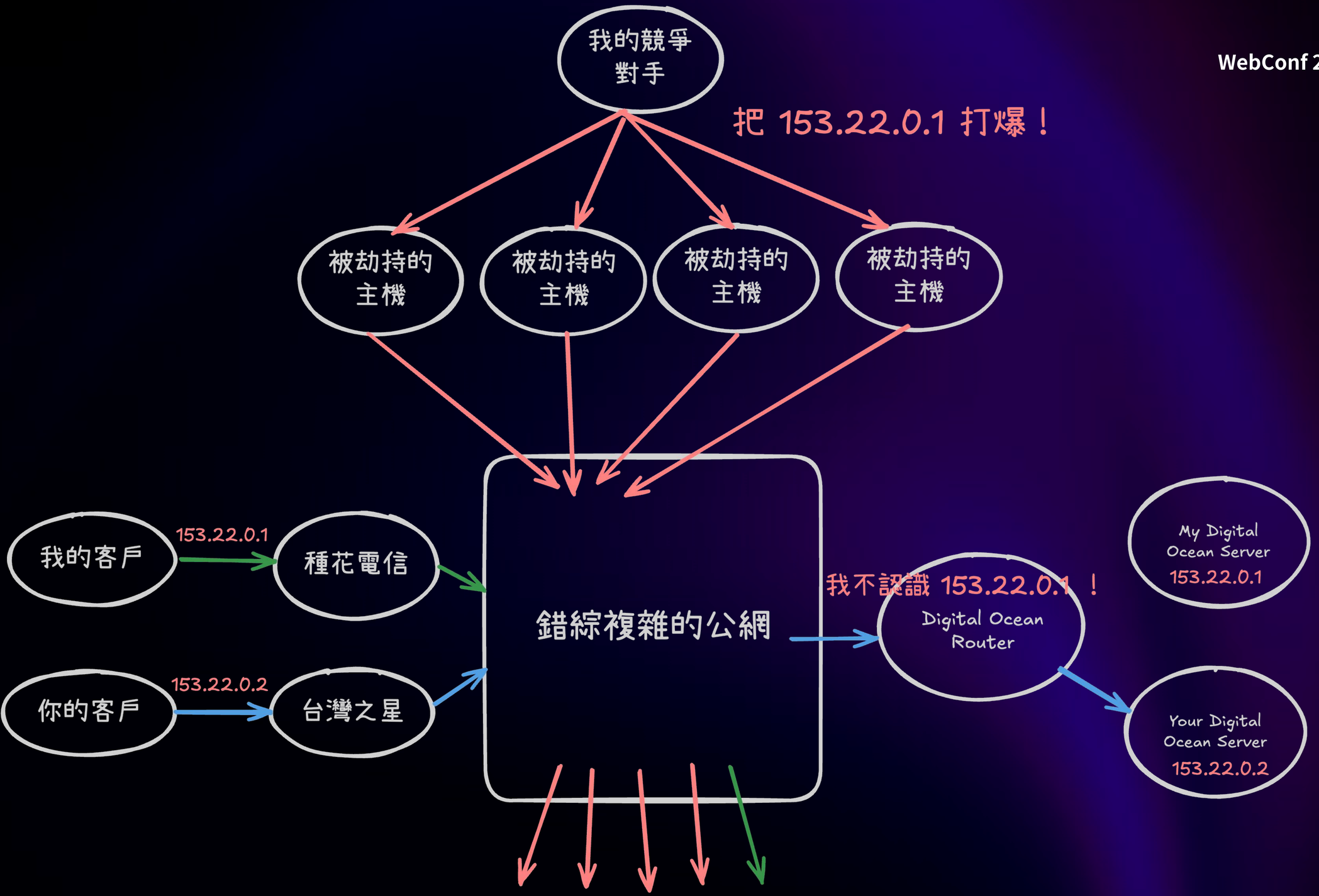


WebConf 2024 Taiwan
2024/12/27

最簡單粗暴的 DDoS 防禦策略

Blackhole Routing

黑洞路由


我的競爭對手
把 153.22.0.1 打爆！
被劫持的主機
被劫持的主機
被劫持的主機
被劫持的主機
我的客戶
153.22.0.1
種花電信
你的客戶
153.22.0.2
台灣之星
錯綜複雜的公網
我不認識 153.22.0.1 ！
Digital Ocean Router
My Digital Ocean Server
153.22.0.1
Your Digital Ocean Server
153.22.0.2

所以，為什麼 Shared Cluster 只用 AWS、GCP？

因為便宜的 VPS 沒辦法讓多個使用者共用 IP
否則一被 DDoS 大家一起掛😢

主流 DDoS 攻擊類型

L4 傳輸層攻擊

消耗網路頻寬和連接資源

容易識別、清洗

大型公有雲的 L4 LB 預設有基礎防禦

L7 應用層攻擊

消耗 CPU、記憶體等計算資源

和普通請求沒有明顯差異

需要額外開啟和設定 WAF 規則等

前提是你的 L7 交給他們負責！

Load balancers

Your AWS account has the following quotas related to Application Load Balancers.

Name	Default	Adjustable
Application Load Balancers per Region	50	Yes
Certificates per Application Load Balancer (excluding default certificates)	25	Yes
Listeners per Application Load Balancer	50	Yes
Target Groups per Action per Application Load Balancer	5	No
Target Groups per Application Load Balancer	100	No
Targets per Application Load Balancer	1,000	Yes

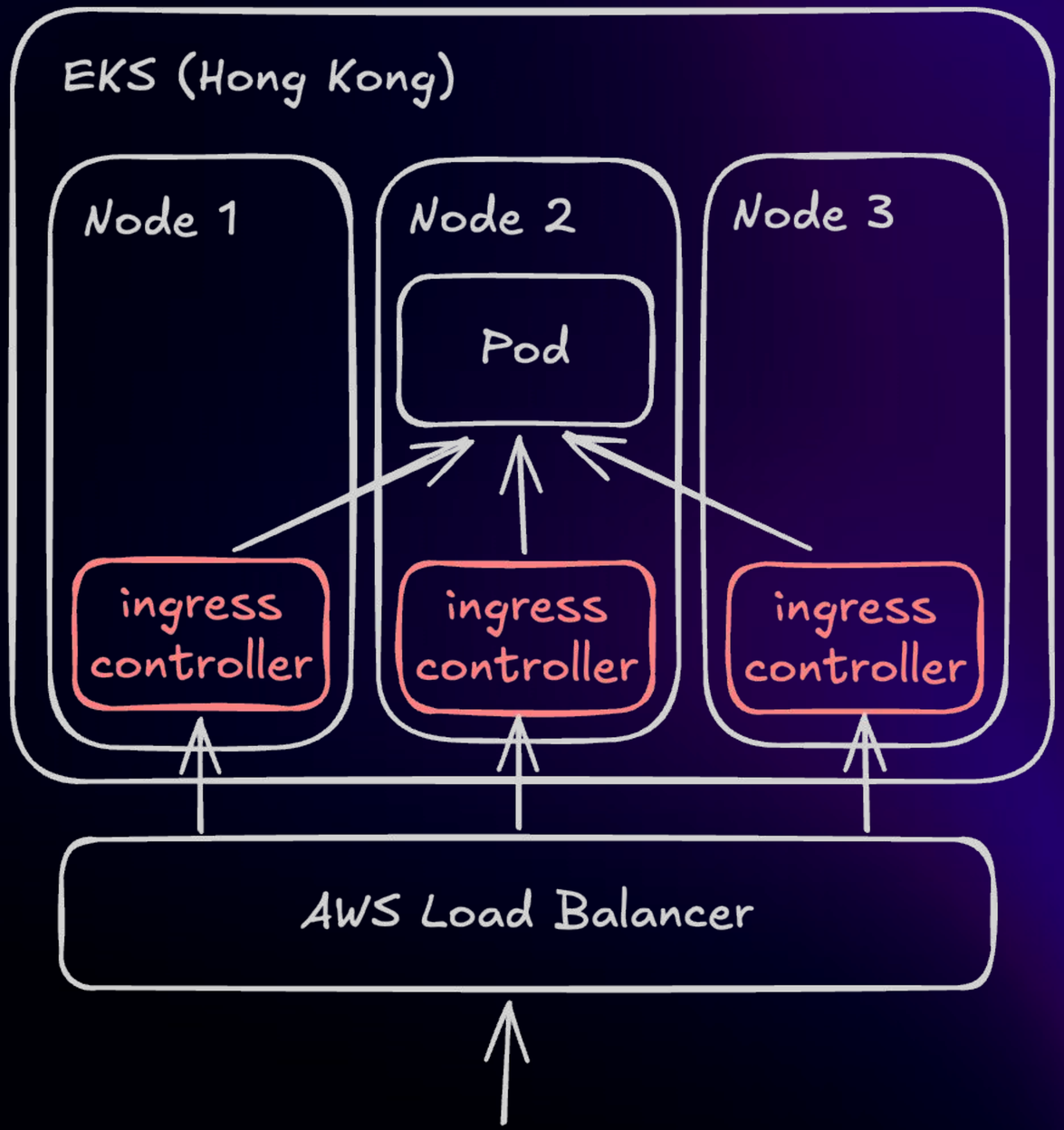
ps. 可以申請提高 quota 到 ... 100（？？

URL maps

The limits documented here cannot be increased.

Item	External Application Load Balancer	Internal Application Load Balancer
URL maps	Quota This quota is per project.	Quota This quota is per project.
Host rules, path matchers per URL map	Limit: 1000	Limit: 2000
Path rules or route rules per path matcher	Limit: 1000	Limit: 1000
Hosts per host rule	Limit: 1000	Limit: 1000
Predicates per path matcher †	Limit: 1000	Limit: 1000

只能說，公有雲的 ALB 不是設計來給 PaaS 這種場景使用的 🤣


EKS (Hong Kong)
Node 1
Node 2
Node 3
Pod
ingress controller
ingress controller
ingress controller
AWS Load Balancer

Control subnet traffic with network access control lists

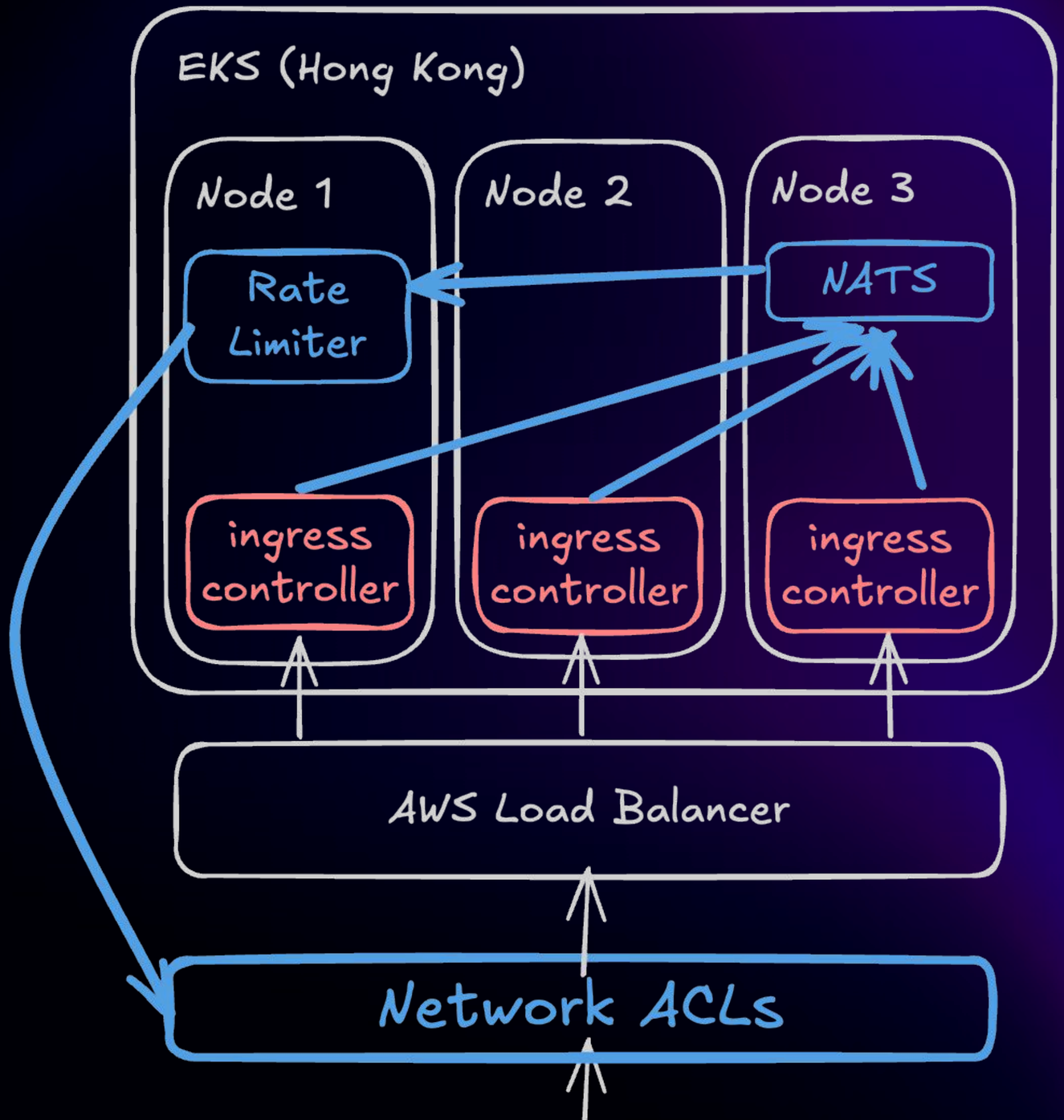
A *network access control list (ACL)* allows or denies specific inbound or outbound traffic at the subnet level. You can use the default network ACL for your VPC, or you can create a custom network ACL for your VPC with rules that are similar to the rules for your security groups in order to add an additional layer of security to your VPC.

There is no additional charge for using network ACLs.

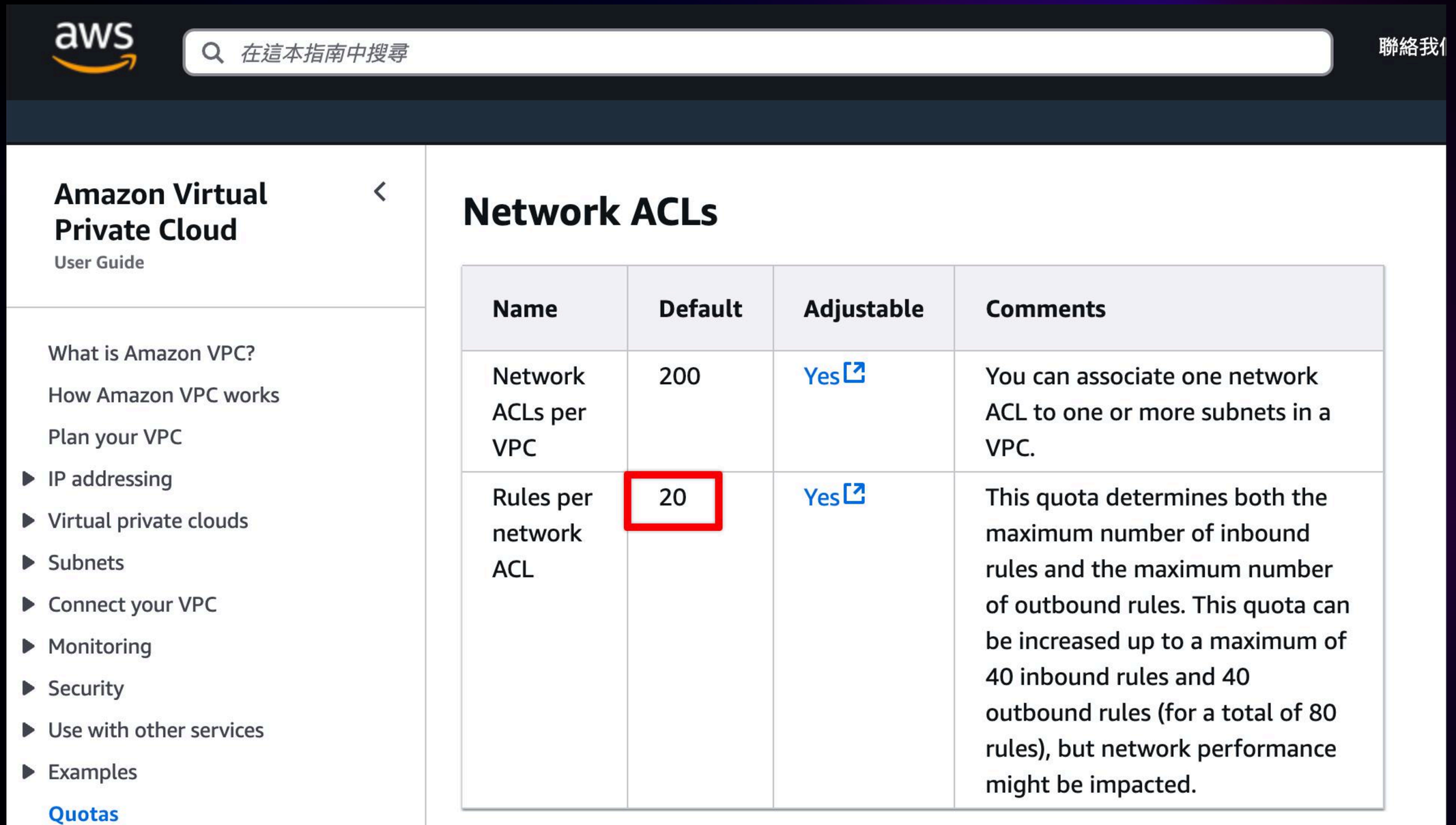
The following diagram shows a VPC with two subnets. Each subnet has a network ACL. When traffic enters the VPC (for example, from a peered VPC, VPN connection, or the internet), the router sends the traffic to its destination. Network ACL A determines which traffic destined for subnet 1 is allowed to enter subnet 1, and which traffic destined for a location outside subnet 1 is allowed to leave subnet 1. Similarly, network ACL B determines which traffic is allowed to enter and leave subnet 2.

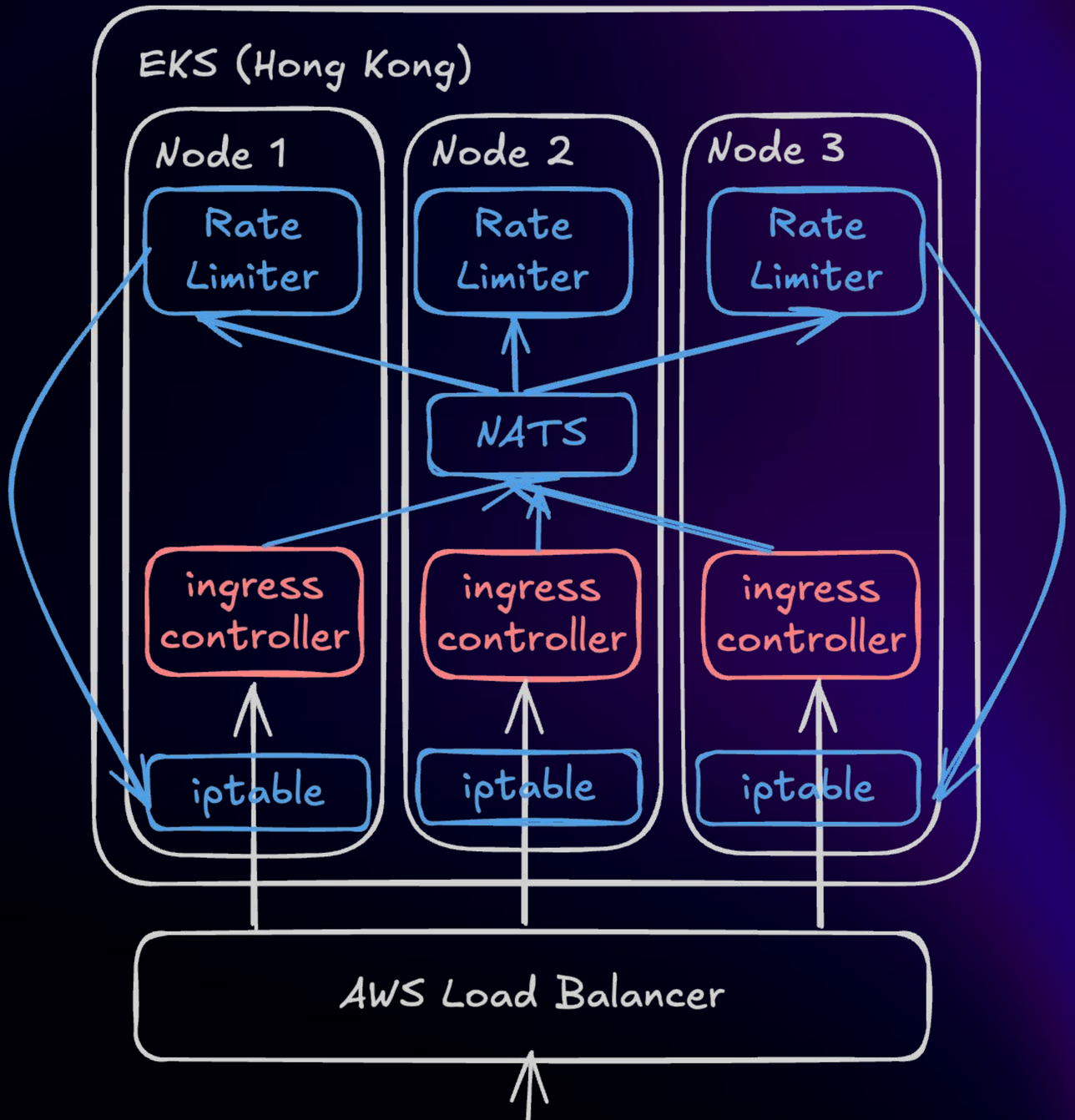
Related resources

VPC Peering Guide
Amazon VPC Transit Gateways
Amazon EC2 Developer Guide


EKS (Hong Kong)
Node 1
Node 2
Node 3
Rate Limiter
NATS
ingress controller
ingress controller
ingress controller
AWS Load Balancer
Network ACLs

順利擋了一陣子，直到 ...


aws
在這本指南中搜尋
聯絡我
Amazon Virtual Private Cloud
User Guide
What is Amazon VPC?
How Amazon VPC works
Plan your VPC
IP addressing
Virtual private clouds
Subnets
Connect your VPC
Monitoring
Security
Use with other services
Examples
Quotas
Network ACLs
Name
Default
Adjustable
Comments
Network ACLs per VPC
200
Yes
You can associate one network ACL to one or more subnets in a VPC.
Rules per network ACL
20
Yes
This quota determines both the maximum number of inbound rules and the maximum number of outbound rules. This quota can be increased up to a maximum of 40 inbound rules and 40 outbound rules (for a total of 80 rules), but network performance might be impacted.


EKS (Hong Kong)
Node 1
Node 2
Node 3
Rate Limiter
Rate Limiter
Rate Limiter
NATS
ingress controller
ingress controller
ingress controller
iptable
iptable
iptable
AWS Load Balancer

免費子網域 Generated subdomain

mywebsite.zeabur.app

你不用花錢買網域，在 Zeabur 按一下就可以用

自定義網域 Custom Domain

mywebsite.com

你要自己付錢買網域，然後 DNS 指向 Zeabur


- Zeabur
回報為不安全的網站: 已封鎖瀏覽
危險
https://[redacted].zeabur.app
此網站已回報為不安全網站
裝載 [redacted].zeabur.app
Microsoft 建議您不要繼續瀏覽此網站。該網站已回報至 M
其可能包含試圖竊取個人或財務資訊的網路釣魚威脅。
上一步
其他資訊
網路釣魚網站可能會冒充受信任的網站來誘騙您洩露個人或財務資訊。

publicsuffix / list

Type / to searc

Code Issues 25 Pull requests 9 Actions Projects Wiki Security Insights

Add "zeabur.app" #1865

Merged **simon-friedberger** merged 1 commit into `publicsuffix:master` from `pan93412:add-zeabur` on May 10

Conversation 4 Commits 1 Checks 1 Files changed 1

pan93412 commented on Oct 1, 2023 • edited Contributor

Public Suffix List (PSL) Pull Request (PR) Template

Each PSL PR needs to have a description, rationale, indication of DNS validation and syntax checking, as well as a number of acknowledgements from the submitter. This template must be included with each PR, and the submitting party MUST

	免費子網域	自定義網域
彈性共享集群	事情開始複雜起來了 ... 1. DNS 誰管理 2. SSL 誰管理 3. DNS 指向哪裡 4. DNS 和 SSL 的方案是否 scalable	
專用伺服器		

	免費子網域	自定義網域
彈性共享集群	DNS 我們管理 Cert 我們管理 指向集群的 Ingress LB 的 IP	DNS 客戶管理 Cert 我們管理 指向集群的 Ingress LB 的 IP
專用伺服器	DNS 我們管理 Cert 我們管理 指向客戶的 VPS 的 IP	DNS 客戶管理 Cert 我們管理 指向客戶的 VPS 的 IP

Does Cloudflare limit the number of DNS records a domain can have?

Yes. All customers have a limit on the number of DNS records they can create.

- Free zones created before `2024-09-01 00:00:00 UTC`: 1,000
- Free zones created on or after `2024-09-01 00:00:00 UTC`: 200
- Pro: 3,500
- Business: 3,500
- Enterprise: 3,500

CloudFlare DNS (3500??)

Billable item	Type	Unit price
Hosted public zone	Personal Edition	USD 7 per year
	Enterprise Standard Edition	USD 29 per Year
	Enterprise Ultimate Edition	USD 81 per Year

Alibaba DNS

(for .zeabur.app) only

Maximum number of DNS records	100,000	The maximum number of Domain Name System (DNS) records that can be added for a domain name. If you want to add more DNS records, submit a ticket.

Lets Encrypt

New Certificates per Registered Domain

A registered domain is, generally speaking, the part of the domain you purchased from yo
instance, in `www.example.com`, the registered domain is `example.com`. In `new.blog.e`
domain is `example.co.uk`. We use the Public Suffix List to identify registered domains.

Limit

Up to 50 certificates can be issued per registered domain every 7 days. This is a global lim
regardless of which account submits them, count towards this limit. The ability to issue ne
registered domain refills at a rate of 1 certificate every 202 minutes.

Overrides

Question: Why not wildcard?

ZeroSSL

WebConf 2024 Taiwan
2024/12/27

ZeroSSL Pricing Plans

Pay Monthly  Pay Yearly Save 20%

Free

No credit card required

$0 per month

Get Free SSL

- 3 90-Day Certificates
- ✗ 90-Day Wildcards

Basic

Basic package with unlimited 90-day certificates.

$10 per month billed yearly

Sign Up

- ∞ 90-Day Certificates
- ✗ 90-Day Wildcards

MOST POPULAR

Premium

Advanced features and more access to 1-year certifiates

$50 per month billed yearly

Sign Up

- ∞ 90-Day Certificates
- ∞ 90-Day Wildcards

Business

All-inclusive package with SSL checks, wildcards and more.

$100 per month billed yearly

Sign Up

- ∞ 90-Day Certificates
- ∞ 90-Day Wildcards

Enterprise

Need more?
Reach out to get an offer

Custom Pricing

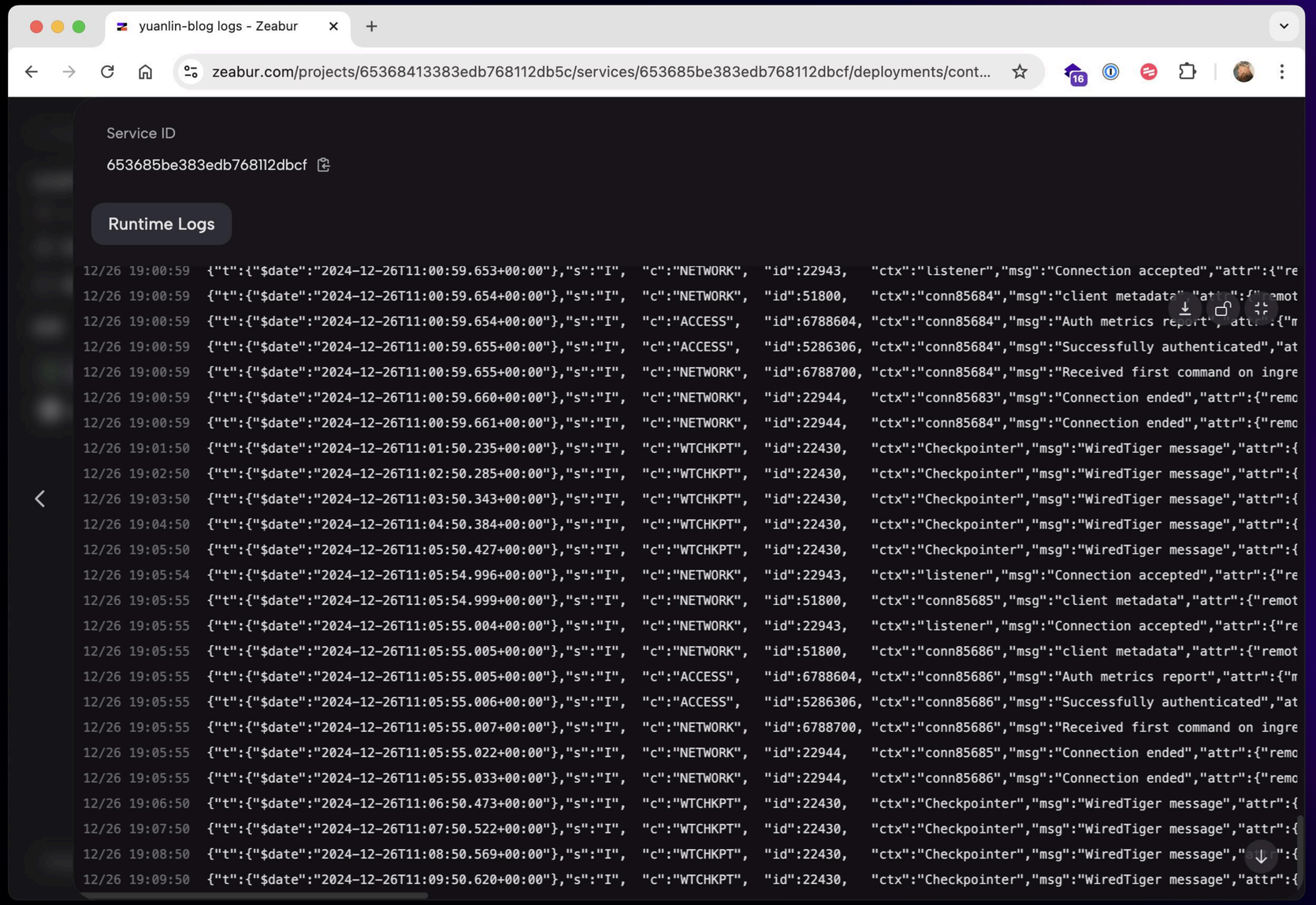
Tailored to your needs

Contact Us

- ✓ 90-Day Certificates
- ✓ 90-Day Wildcards

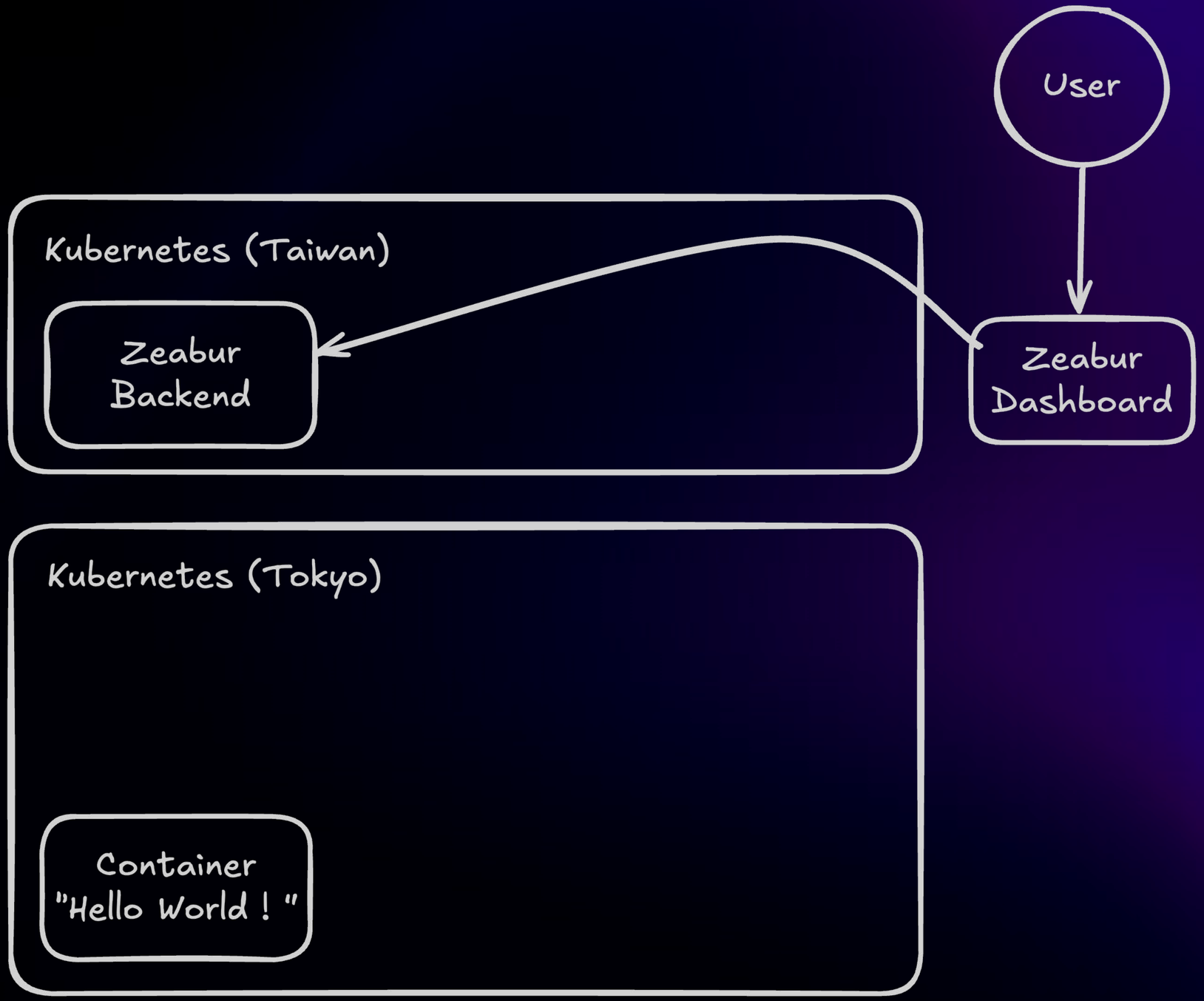
WebConf 2024 Taiwan
2024/12/27

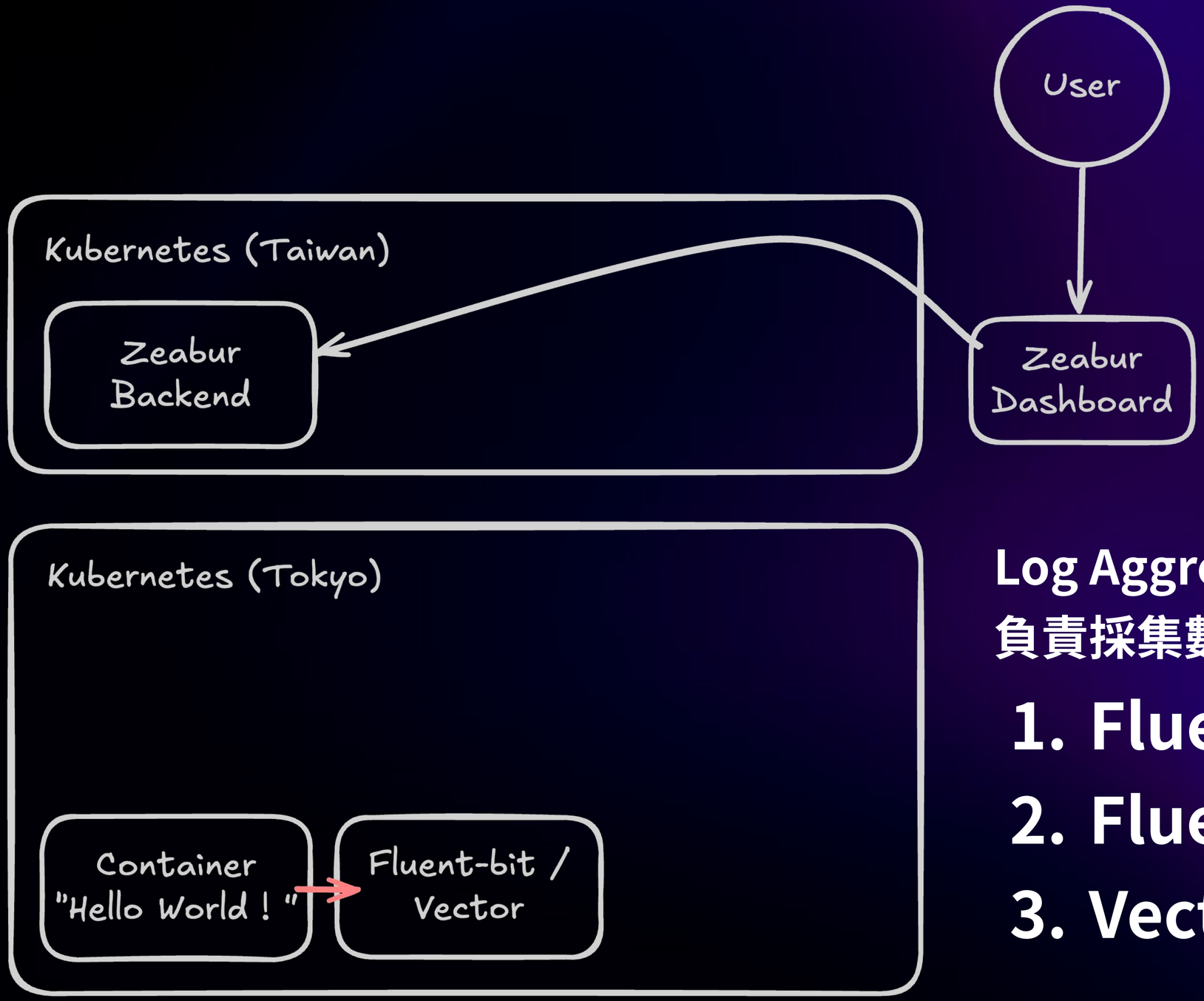
WebConf 2024 Taiwan
2024/12/27



PaaS 最重要的功能之一

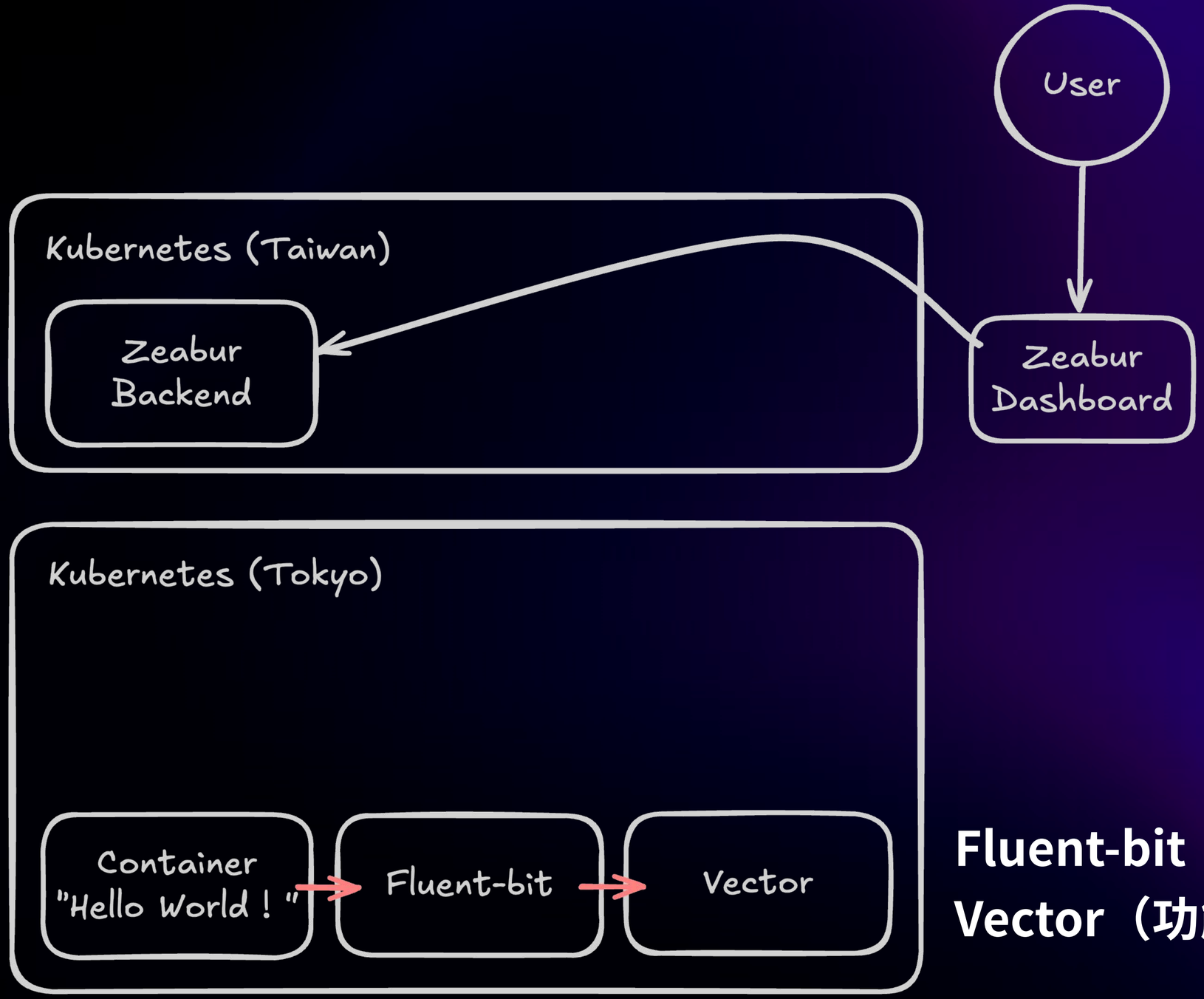
Runtime Logs


User
Kubernetes (Taiwan)
Zeabur Backend
Zeabur Dashboard
Kubernetes (Tokyo)
Container "Hello World ! "

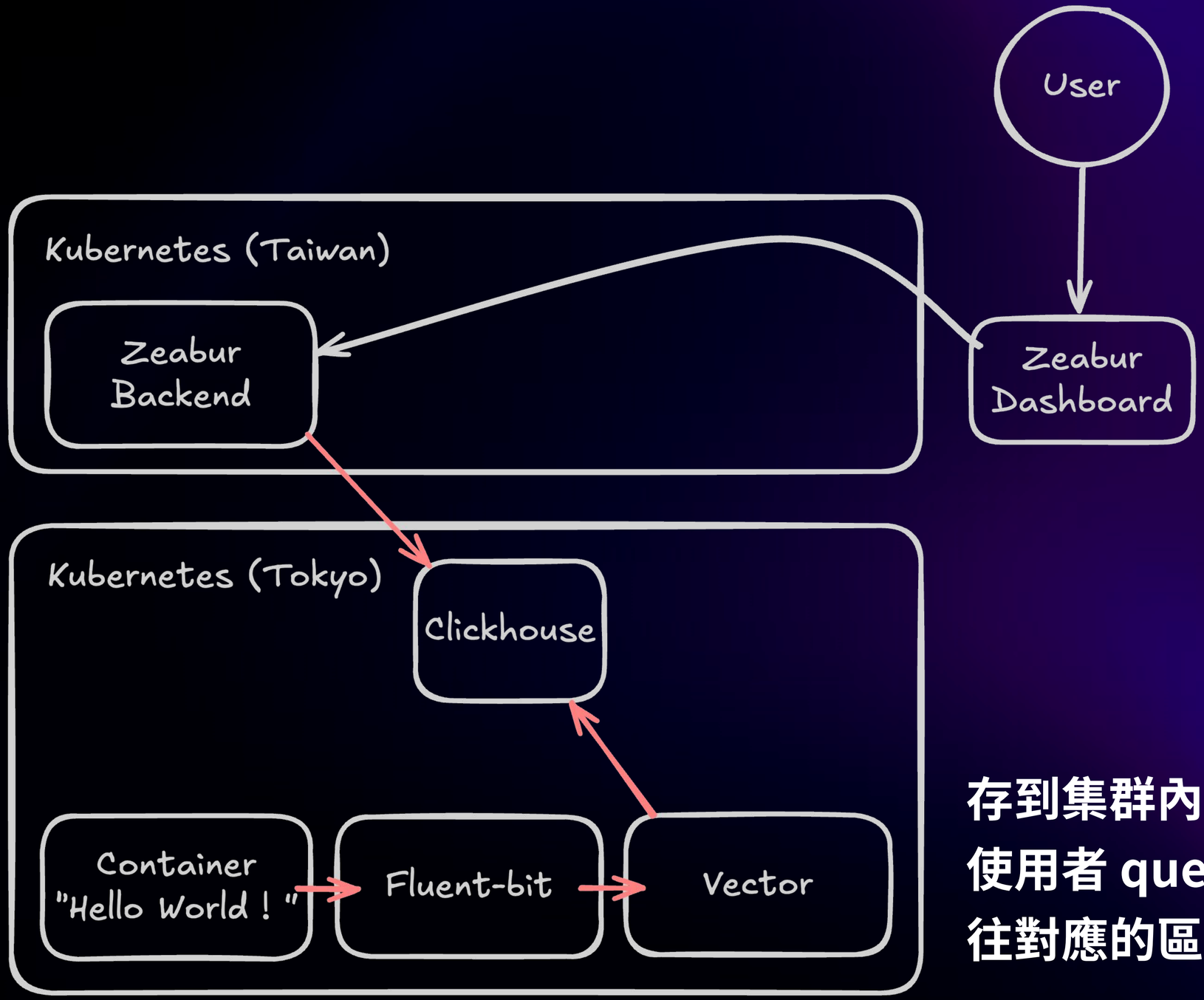


Log Aggregator
負責採集數據、過濾、分流 ...

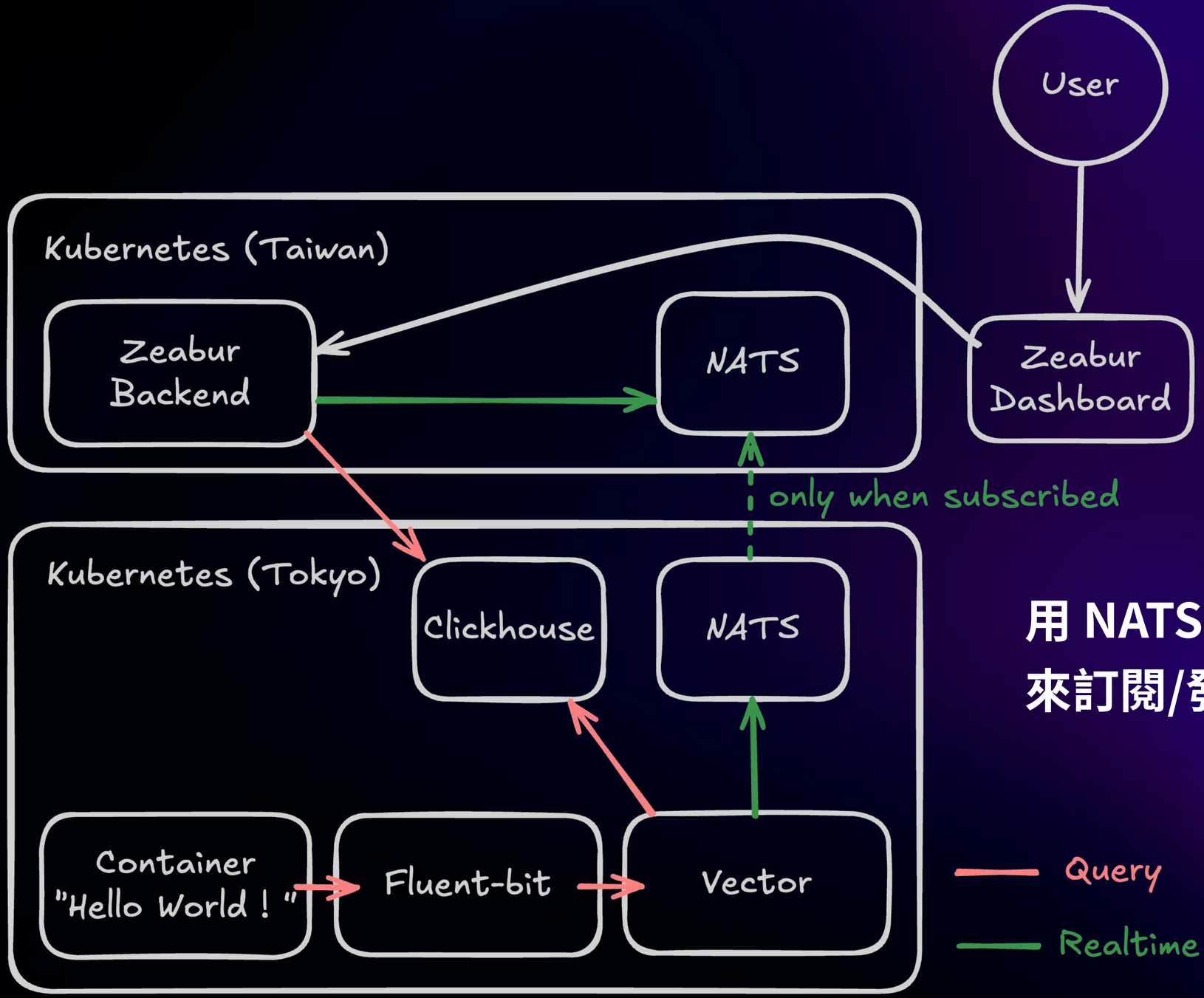
1. Fluentd
2. Fluent-bit
3. Vector



Fluent-bit（性能比較好）負責採集
Vector（功能比較強）負責限速、分流



存到集群內的 Clickhouse
使用者 query 的時候從 Zeabur 後端往對應的區域查詢



用 NATS（基於 Go 寫的 MQ）
來訂閱/發布 Realtime logs

總結

當年選題目的時候想的太簡單了 🤣

踩到了許多 Scalability 相關的坑

（無論是技術角度 & 商業/成本角度）

WebConf 2024 Taiwan
2024/12/27

Thanks！

以上就是今天的分享 😀

掃描 QRCode
免費領取一個月 Zeabur 付費會員 👉