亚马逊云科技

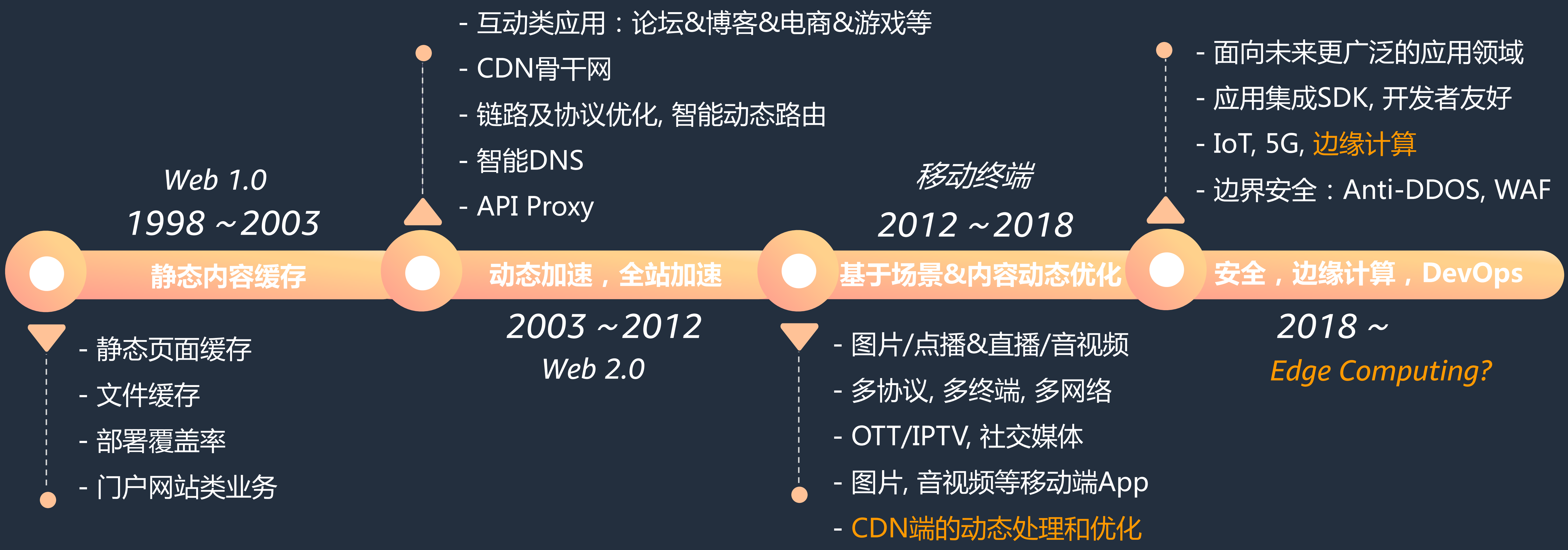
使用函数在 CloudFront 边缘进行自定义

Lambda@Edge 及 CloudFront Functions 介绍

郭道明 | 亚马逊云科技解决方案架构师

在 CDN 侧的边缘计算崭露头角

CDN 的技术发展之路



Web 1.0

1998 ~2003

静态内容缓存

- 静态页面缓存
- 文件缓存
- 部署覆盖率
- 门户网站类业务

- 互动类应用：论坛&博客&电商&游戏等
- CDN骨干网
- 链路及协议优化, 智能动态路由
- 智能DNS
- API Proxy

动态加速，全站加速

2003 ~2012

Web 2.0

移动终端

2012 ~2018

基于场景&内容动态优化

- 图片/点播&直播/音视频
- 多协议, 多终端, 多网络
- OTT/IPTV, 社交媒体
- 图片, 音视频等移动端App
- CDN端的动态处理和优化

- 面向未来更广泛的应用领域
- 应用集成SDK, 开发者友好
- IoT, 5G, 边缘计算
- 边界安全：Anti-DDOS, WAF

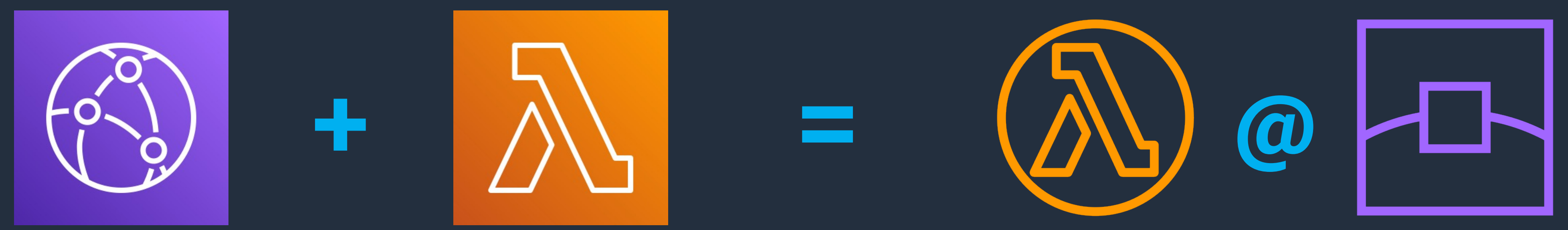
安全，边缘计算，DevOps

2018 ~

Edge Computing?

什么是 Lambda@Edge

在 CDN 侧自定义您的业务逻辑



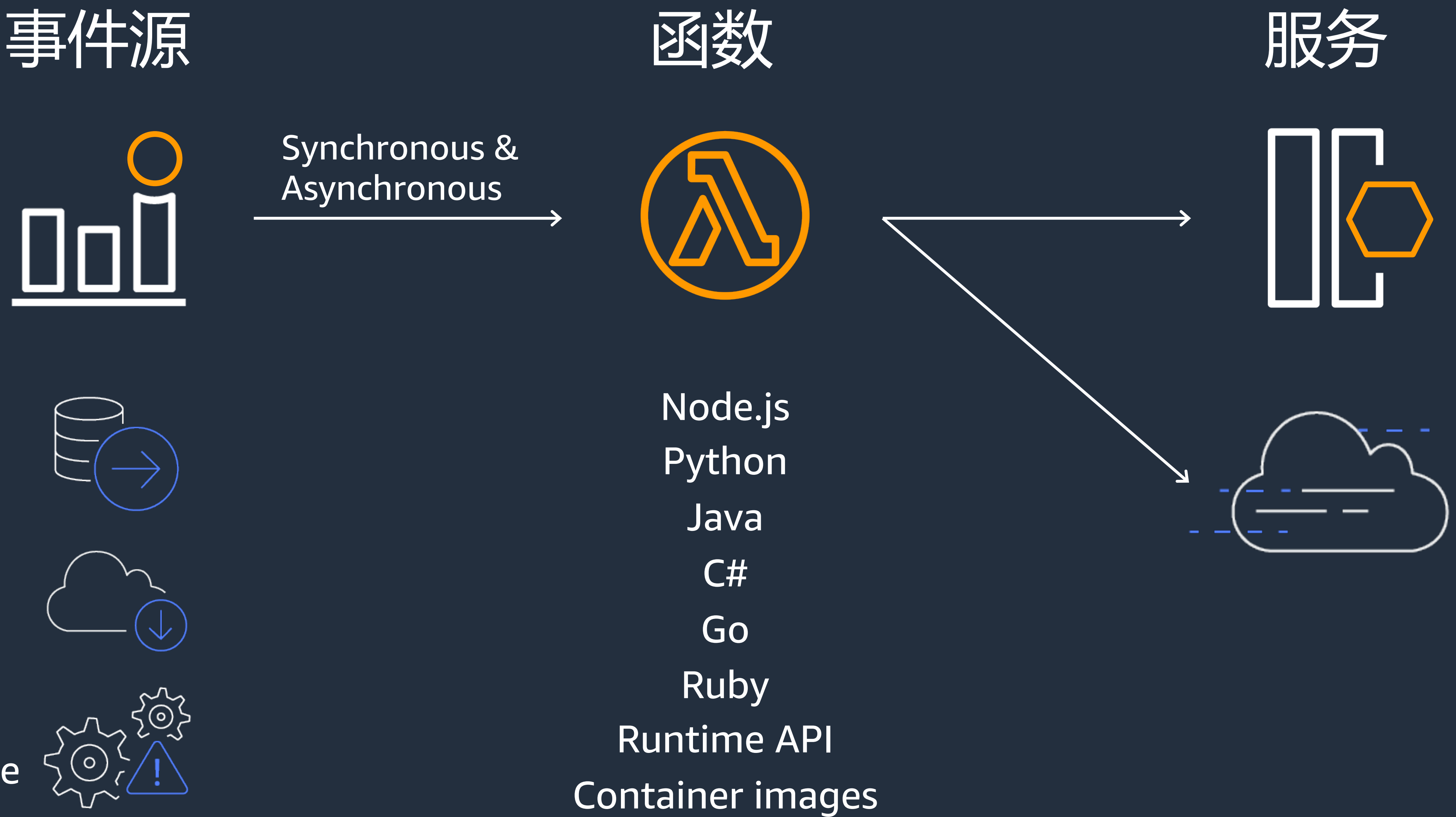
Amazon CloudFront + AWS Lambda = Lambda function @ Edge location

- You PROGRAM Amazon CloudFront with Lambda@Edge

AWS Lambda 无服务器计算服务

Serverless Function, 功能即服务, 事件驱动

无需部署和管理服务器 | 按需自动扩展 | 按实际用量付费 | 自带高可用和容错机制



事件源

函数

服务

Synchronous &
Asynchronous

Changes in
data state

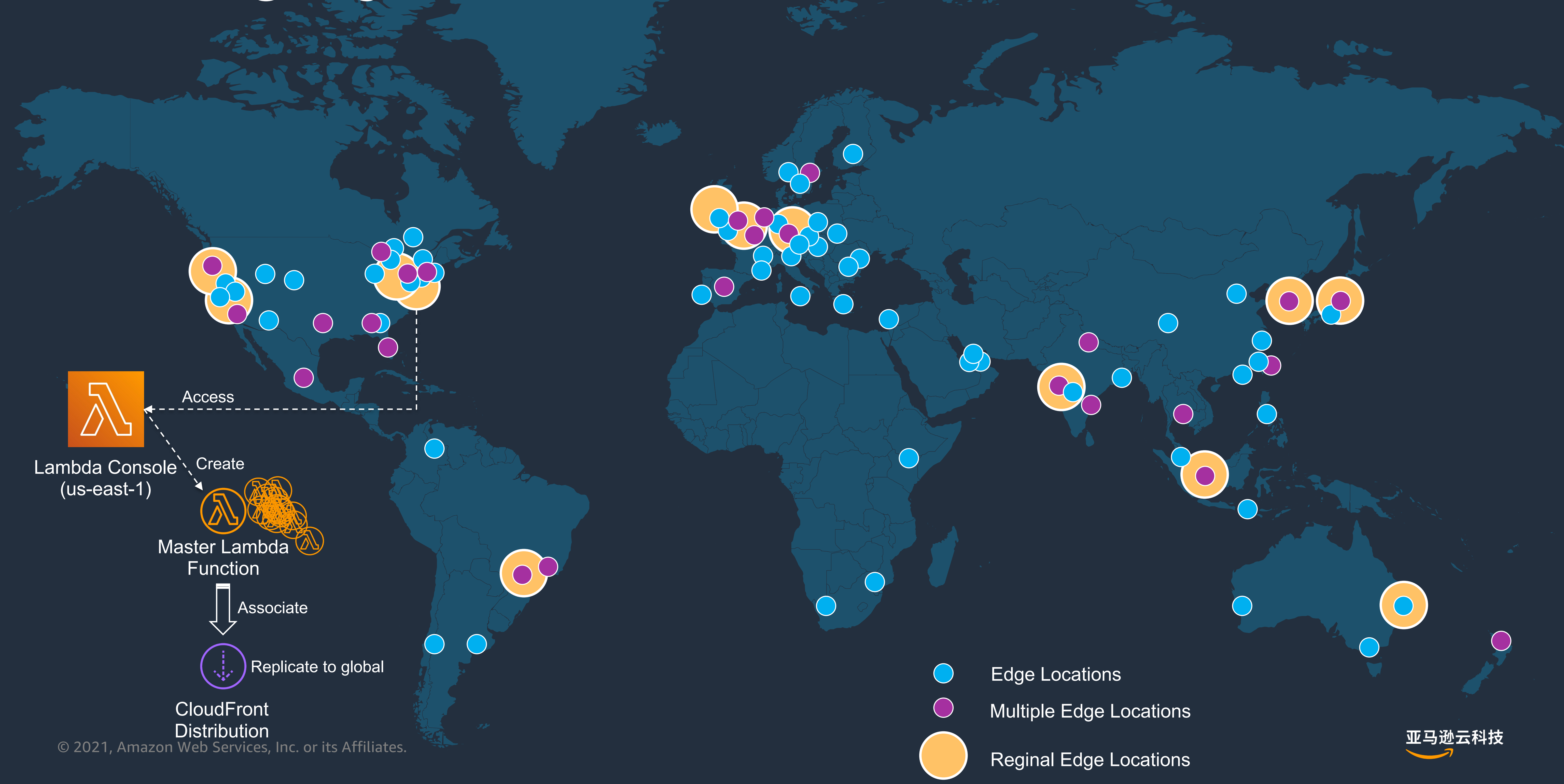
Requests to
endpoints

Changes in
Resource state

Node.js
Python
Java
C#
Go
Ruby
Runtime API
Container images

亚马逊云科技

lambda@Edge: 编写一次，复制至全球各地运行



Access

Lambda Console
(us-east-1)

Create

Master Lambda
Function

Associate

Replicate to global

CloudFront
Distribution

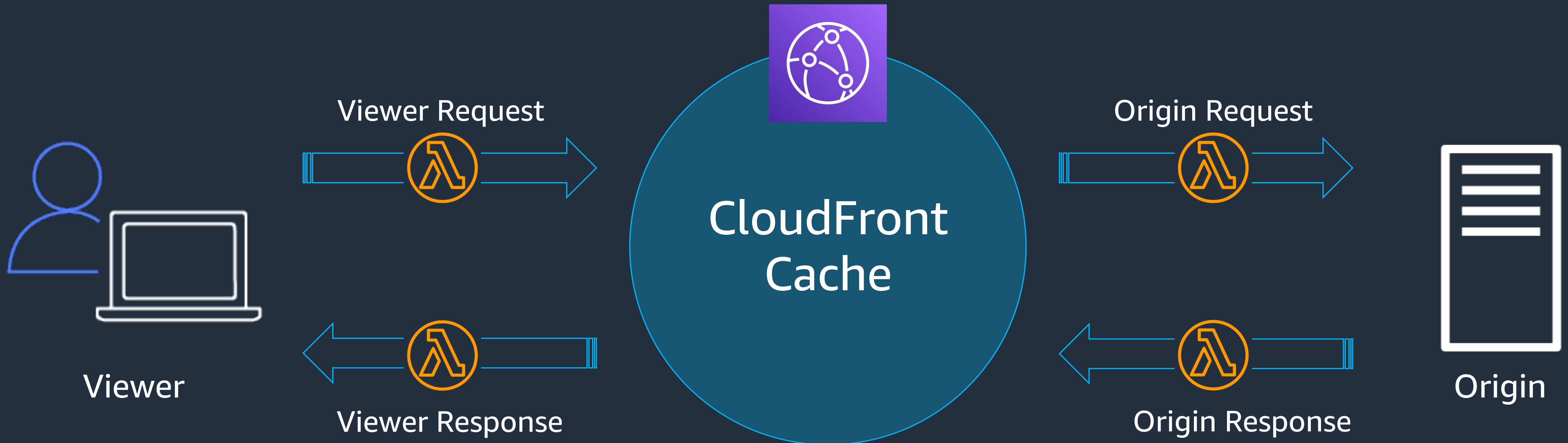
● Edge Locations

● Multiple Edge Locations

● Reginal Edge Locations

通过 CloudFront 触发 Lambda@Edge

事件触发架构



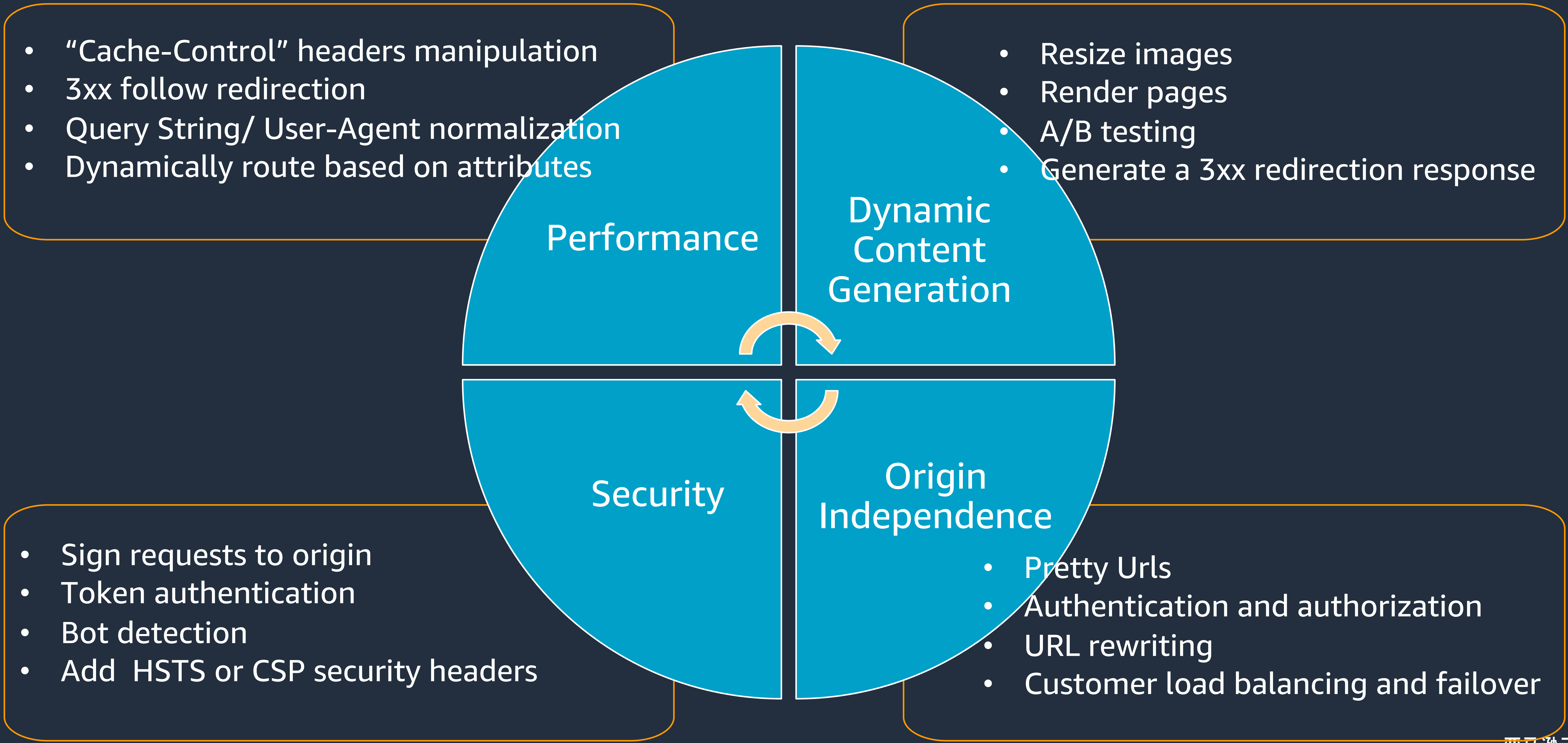
Viewer events

- Triggered for every viewer request
- Cache key can be modified
- Response is not cached

Origin events

- Triggered only for cache misses
- Cache key cannot be modified
- Response can be cached

Lambda@Edge 使用场景



Performance

- “Cache-Control” headers manipulation
- 3xx follow redirection
- Query String/ User-Agent normalization
- Dynamically route based on attributes

Dynamic Content Generation

- Resize images
- Render pages
- A/B testing
- Generate a 3xx redirection response

Security

- Sign requests to origin
- Token authentication
- Bot detection
- Add HSTS or CSP security headers

Origin Independence

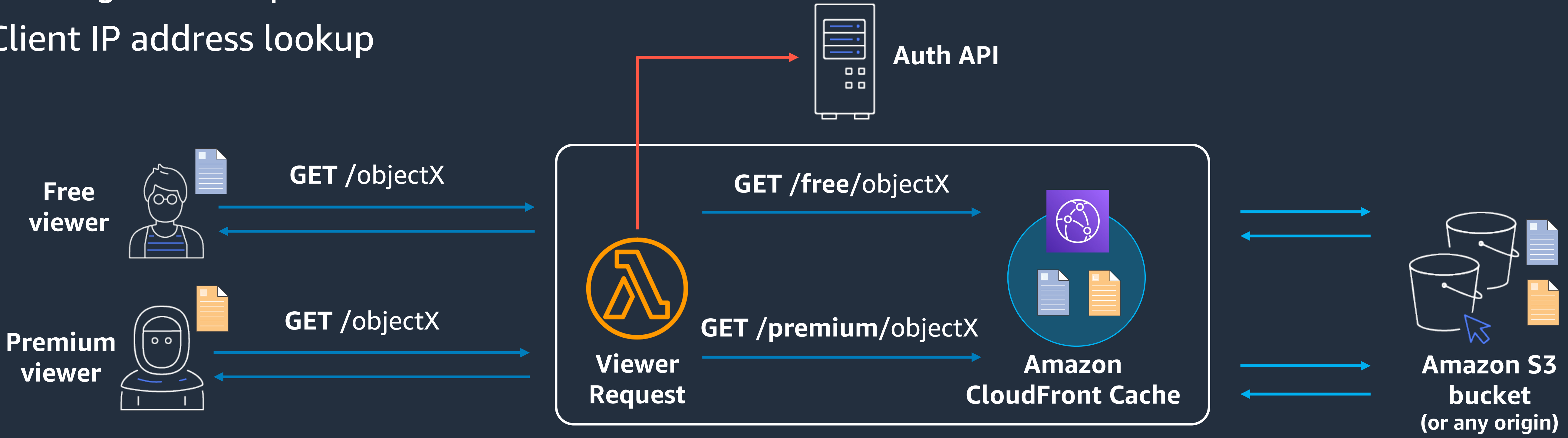
- Pretty Urls
- Authentication and authorization
- URL rewriting
- Customer load balancing and failover

典型示例 1：认证鉴权

- **Event trigger: Viewer Request**

The classification condition is based on unique properties of the viewer:

- Authentication/authorization condition
- User-Agent lookup
- Client IP address lookup

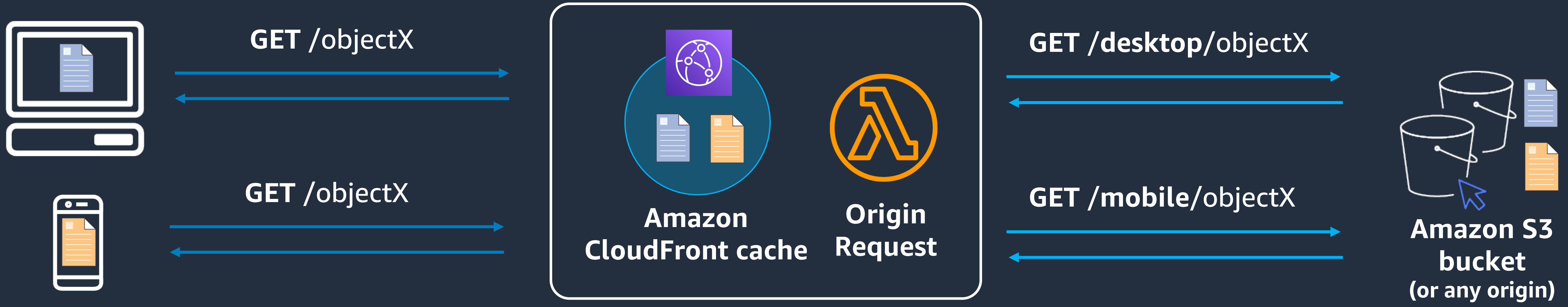


典型示例 2：分类型交付内容

- **Event trigger: Origin Request**

The classification condition can be a part of the cache key, for example:

- CloudFront-Is-[Desktop|Mobile]-Viewer
- CloudFront-Viewer-Country
- any other header, cookie, or query string

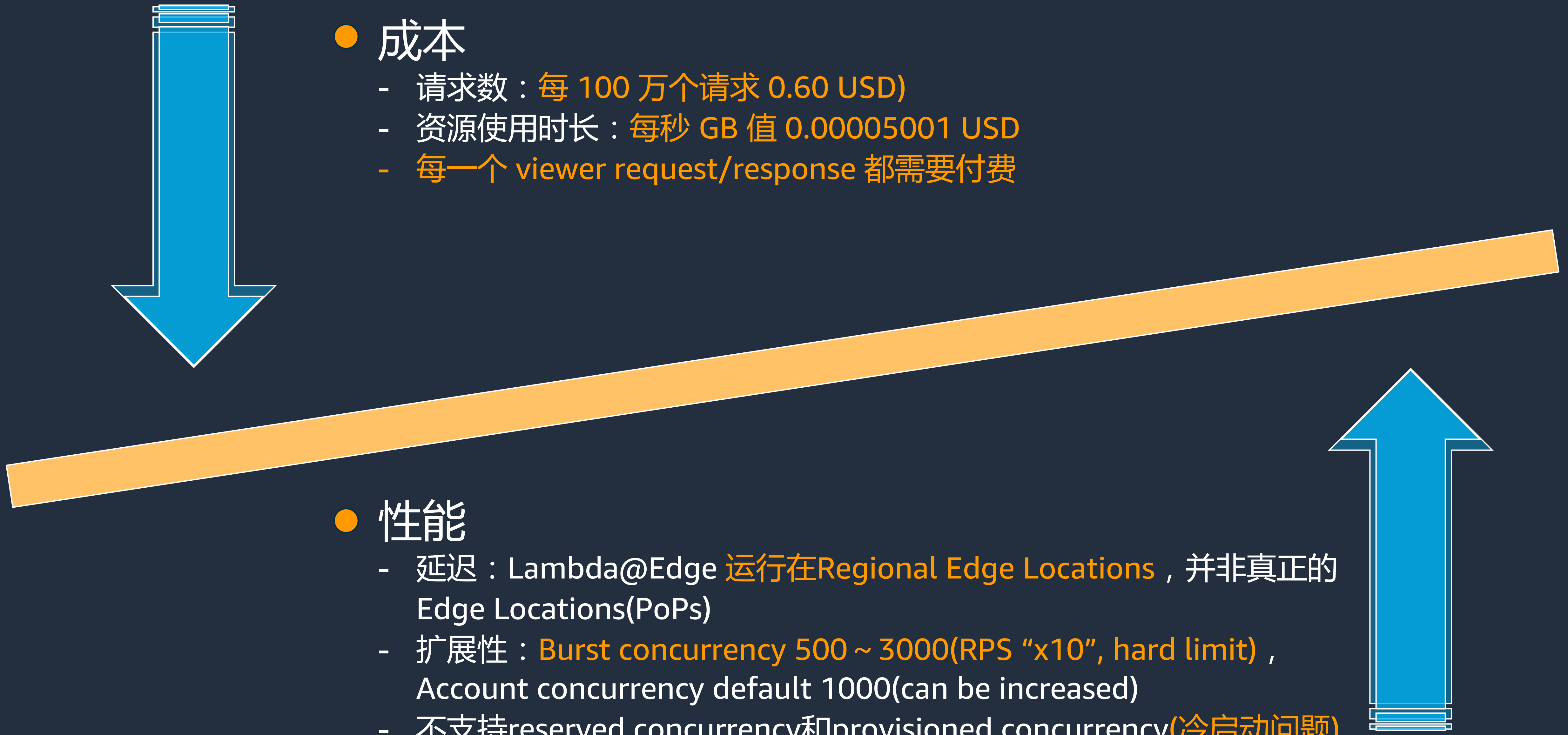


Demo: Lambda@Edge

根据特定的国家编码返回 L@E 的自定义页面

关于 Lambda@Edge 成本和性能的一些思考

降低成本，提高性能



- 成本
  - 请求数：每 100 万个请求 0.60 USD)
  - 资源使用时长：每秒 GB 值 0.00005001 USD
  - 每一个 viewer request/response 都需要付费

- 性能
  - 延迟：Lambda@Edge 运行在Regional Edge Locations，并非真正的 Edge Locations(PoPs)
  - 扩展性：Burst concurrency 500 ~ 3000(RPS “x10”, hard limit)，Account concurrency default 1000(can be increased)
  - 不支持reserved concurrency和provisioned concurrency(冷启动问题)

CloudFront Functions

Lambda@Edge 的有效补充

CloudFront Functions 的由来

积极倾听客户的反馈

Today 55% of all Lambda@Edge functions:

- Viewer-facing code that needs to run on every request
- Latency-sensitive, simple functions with very low execution durations
- Prone to unpredictable spikes in traffic

For viewer request and response functions, customers asked us for:

Better Performance

Easier scaling

Lower cost

Better Dev Experience

CloudFront Functions 的独特之处

New purpose-built serverless scripting feature for running lightweight JavaScript code at the 225+ CloudFront edge locations

Ultra Performant

Sub millisecond start times

Instantly Scalable

Handle millions of requests per second

Highly Secure

Uses the highest security standards

Cost Effective

Fraction of Lambda@Edge price

Developer Friendly

Streamlined workflow and APIs

CloudFront Functions 特性介绍

Native to CloudFront

Functions can be created, tested and deployed using the CloudFront console

Global service

Deploy from any AWS region

Centralized logs and metrics

All logs and metrics are centralized in US-East-1

Geo-location and device header data

Make decisions on where users are located and devices they use

Test against CloudFront

Immediate feedback if the function will work in production

CloudFront Functions 使用场景

适合简单业务逻辑处理以及轻负载运算

- **Cache key normalization** - Transform HTTP request attributes (URL, headers, cookies, query strings) to construct CloudFront cache key in a more optimal way, leading to an improved cache hit ratio.
- **Header manipulation** - Insert, modify or delete any HTTP headers (e.g. True-Client-IP, CORS, or HSTS headers).
- **URL redirects/rewrites** - Redirect users to other pages or seamlessly direct requests to different paths on the origin server.
- **Request authorization** - Create and validate user generated tokens, such as HMAC tokens or JSON web tokens (JWT). Implement access control by inspecting an AUTH header to determine if the request should be allowed or denied access.

不适合复杂业务逻辑处理及高负载运算

- **Long running** - Workloads that take several milliseconds to seconds to complete.
- **Adjustable Memory or CPU** – Workloads that require large CPU or memory footprint.
- **Dependency on 3rd party libraries** – Including the AWS SDK which is required for integrations with other AWS services (e.g., S3, DynamoDB).
- **Networks calls** – Workloads that need to call external services or end points for data processing.

Continue to use Lambda@Edge for these types of workloads

CloudFront Functions 和 Lambda@Edge 的不同之处

	Lambda@Edge	**CloudFront Functions**
Programming Languages	Node.JS and Python	JavaScript (ECMAScript 5.1 compliant)
Event sources supported	viewer-request, origin-request, origin-response, viewer-response	viewer-request, viewer-response
Execution Location	13 CloudFront Regional Edge Caches	225+ CF edge locations
Scale	10,000 RPS per region(can be raised)	10+ million RPS
Function execution time	up to 30 seconds	Up to 1ms (may be reduced)
Network access	Yes	No
File system access	Yes	No
Max memory	128 MB(View) - 10240 MB(Origin)	2MB
Max function and included libraries size	1MB(view request/response),50MB(origin request/response)	40KB (may be reduced)
Function logging and metrics	Yes (distributed in REC)	Yes (Centralized in us-east-1)

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions.html

Demo: CloudFront Functions

根据不同的国家编码重定向至不同的 Web 站点

Lambda@Edge 和 CloudFront Functions 代码参考样例

Lambda@Edge

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html

https://github.com/awslabs/aws-cloudfront-extensions

CloudFront Functions

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/functions-example-code.html

https://github.com/aws-samples/amazon-cloudfront-functions

亚马逊云科技

Thank You!

Q&A