Core Services Workshop

2019年4月12日

目录

① AWS基础知识

② IAM和VPC

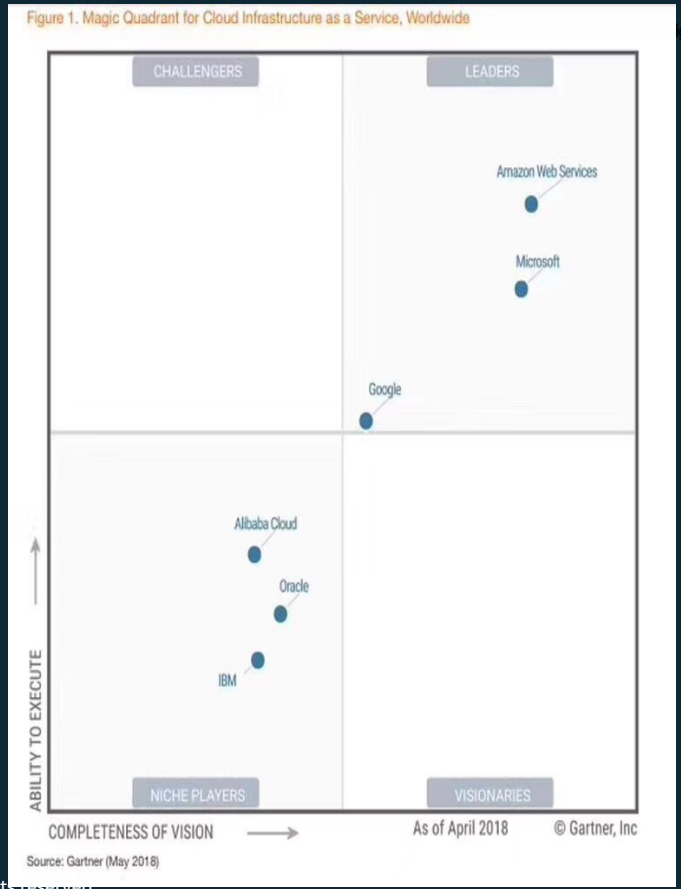
③ 计算服务EC2, AutoScaling和ELB

④ 对象存储服务S3+动手本地文件备份到S3

⑤ 容灾的的几个层次+容灾演示

AWS 基础知识分享

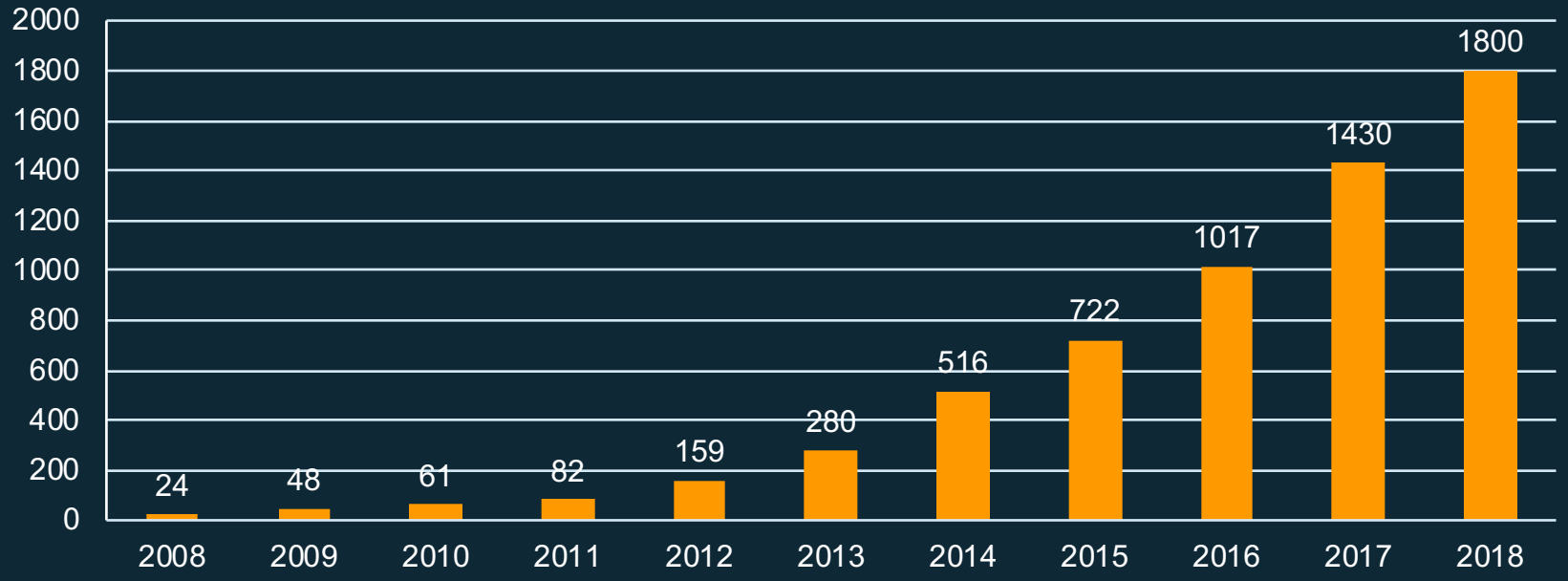
AWS引领云计算市场



Source:
https://www.gartner.com

AWS：基于客户需求的高速创新

AWS一直致力于将更多的服务与功能提供给不同行业及垂直领域的云服务需求， 已提供超过150种服务，横跨计算，存储，网络，数据库，数据分析，企业应用服务，自动化运维与管理，以及移动应用等领域。 自2006年诞生以来，AWS已累积发布了**6000多项**新服务与功能。



最可信的云平台，适用于全球化的合规性要求

SOC 1 / ISAE 3402	ISO 27001	FedRAMP
SOC 2	ISO 9001	ISO 27017
SOC 3	ISO 27018	PCI DSS Level 1
HIPAA	GxP	FIPS 140-2
CJIS	ITAR	G-Cloud 
DoD SRG Levels 2 & 4	FERPA	IT-Grundschutz 
MLPS Level 3 等保三级 	Section 508 / VPAT	MPAA
MTCS Tier 3 	NIST	Cloud Security Alliance
IRAP 	FISMA, RMF, and DIACAP	Cyber Essentials Plus 

aws

AWS为中国客户定制

中国区域

中国账户

中国定制
运营模式

7×24小时
中文支持中心

北京区域
宁夏区域

技术平台得到
等保三级认证

全国信息安全标准化委员会
TC260 工作组成员单位

数据中心联盟
全权会员单位

aws

天然享有“两地三中心”能力

可用区：

每个区域至少有两个可用区

每个可用区都由多个数据中心组成

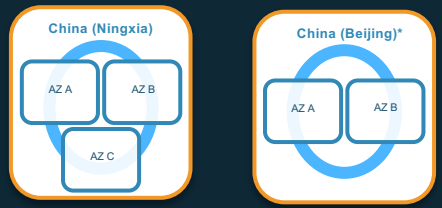
可用区之间地理与网络均独立设计与运营

可用区直接网络延时保持在3ms以下

可用区内延时保持在0.3ms以下

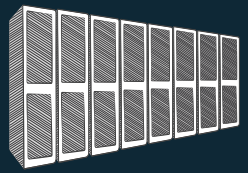
跨可用区的高可用部署

极低成本的城市圈级别的实时灾备方案

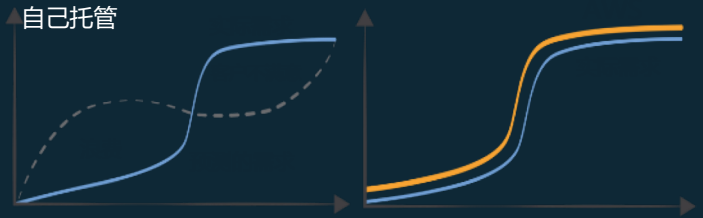


AWS 云在全球 22 个地理区域内运营着 69 个可用区，并宣布计划增加开普敦、雅加达和米兰这三个区域，同时再增加 9个可用区。

1. 按需付费，无需事先固定投资

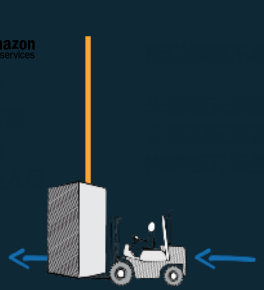


2. 无需猜测容量



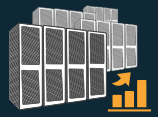
3. 增加创新： 更快的尝试并且低成本、低风险

4. 摆脱无差异化的，基础的体力劳动



5. 天然享有高可用属性

6. IT整体成本降低



51
Price Reductions

的

AWS IAM和VPC

责任共担模型

客户

客户内容

平台、应用、身份和权限管理

操作系统、网络和防火墙配置

客户端数据加密

服务器端
数据加密

网络流量保护

客户负责云
内部的安全

AWS 基础服务

计算

存储

数据库

网络

AWS 全球
基础设施

可用区

区域

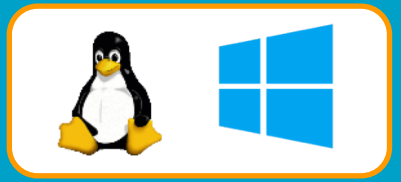
边缘站点

AWS负责云
本身的安全

不同层面的操作主体

应用
- 应用用户，应用管理员

操作系统
- 系统管理员，开发人员



Amazon Web Services
- 开发人员，SA，测试人员，软件 / 平台
- 与 AWS 资源的交互:
  - 部署 EC2 实例和 EBS 卷
  - 配置 ELB
  - 访问 S3 对象或 DynamoDB 中的数据
  - 与 SQS 队列交互
  - 发送 SNS 通知

aws

AWS 中的 AAA

Authenticate 认证	Authorize 授权	Audit 审计
IAM 用户名/密码 访问密钥 Access Key (+ 多因子认证 MFA) 联邦	IAM 策略	CloudTrail

AWS Identity and Access Management (IAM)

- *四个重要概念：用户 **users**, 组 **groups**, 角色 **roles**, 权限 **permissions/策略Policy***

- 控制
  - 集中式
  - 细粒度的 APIs, 资源和管理控制台

- 安全
  - 默认安全（拒绝）
  - 可加守门员策略

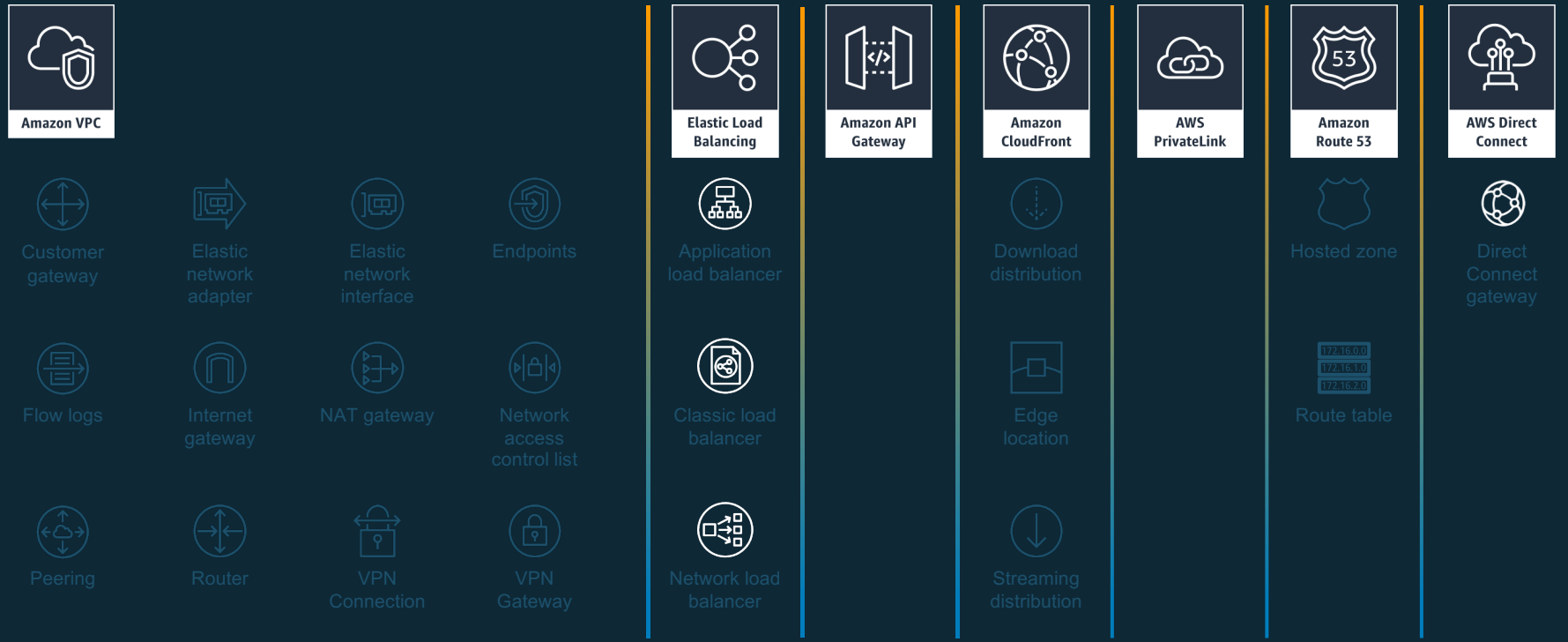
IAM 策略

- JSON 格式
- 语句（权限）定义:
  - Principal 主体
  - Action 操作
  - Resource 资源
  - Condition 条件

```
{
 "Statement":[{
   "Effect":"effect",
   "Principal":"principal",
   "Action":"action",
   "Resource":"arn",
   "Condition":{
     "condition":{
       "key":"value" }
     }
   }
  ]
 }
```


aws

Our networking & content delivery business



网络构建模块

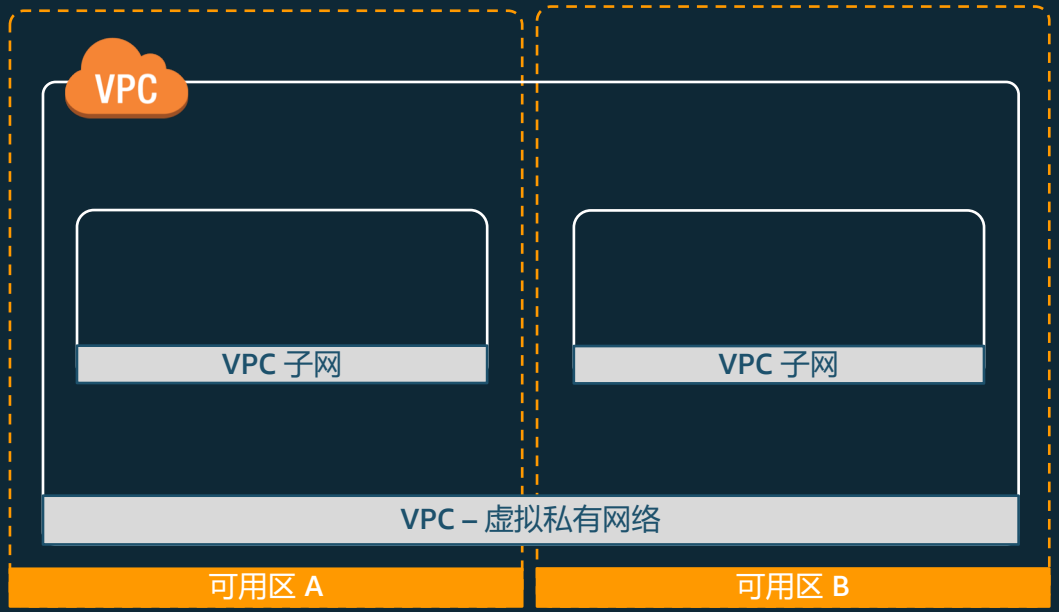
Amazon 虚拟私有网络 (VPC)

- 构建您自己的网络

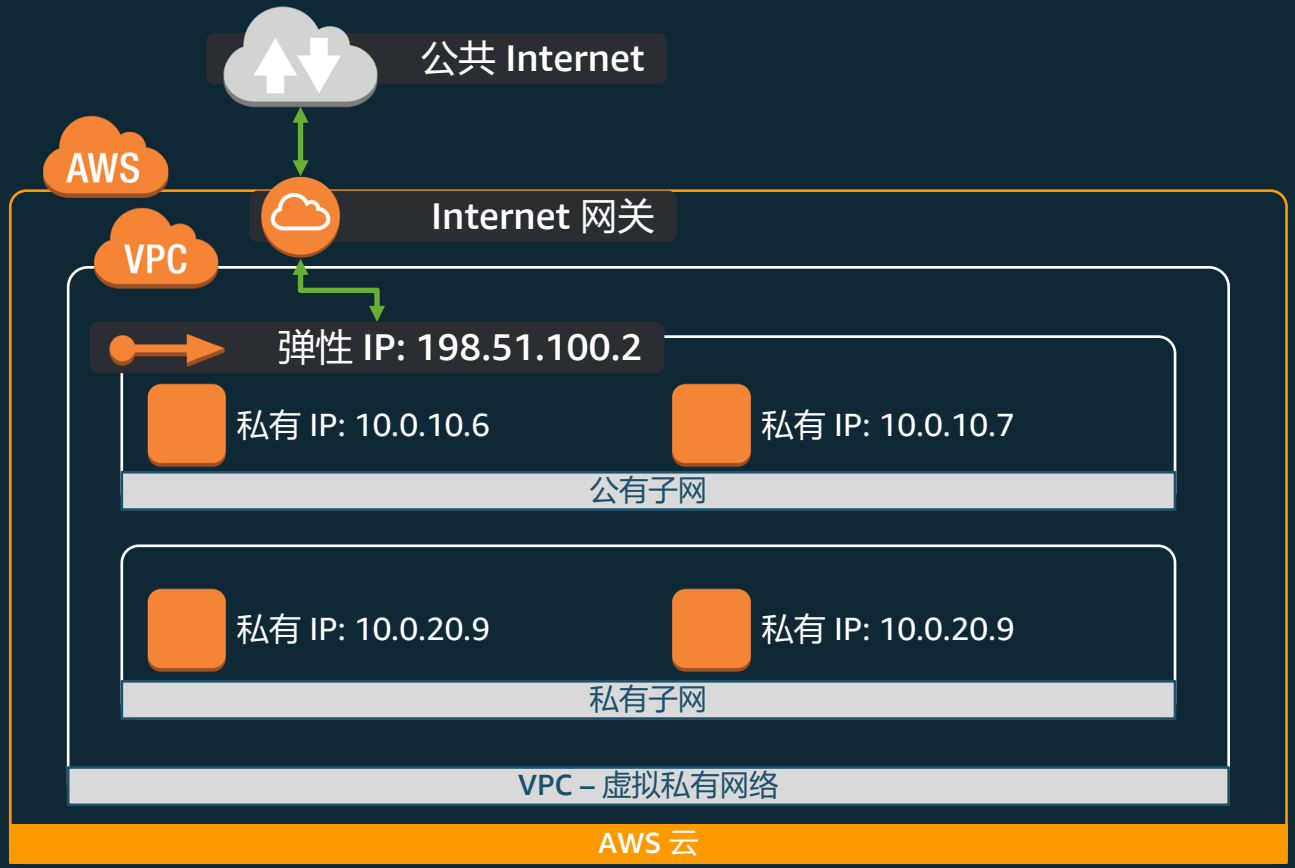
网络构建模块

Amazon 虚拟私有网络 (VPC)

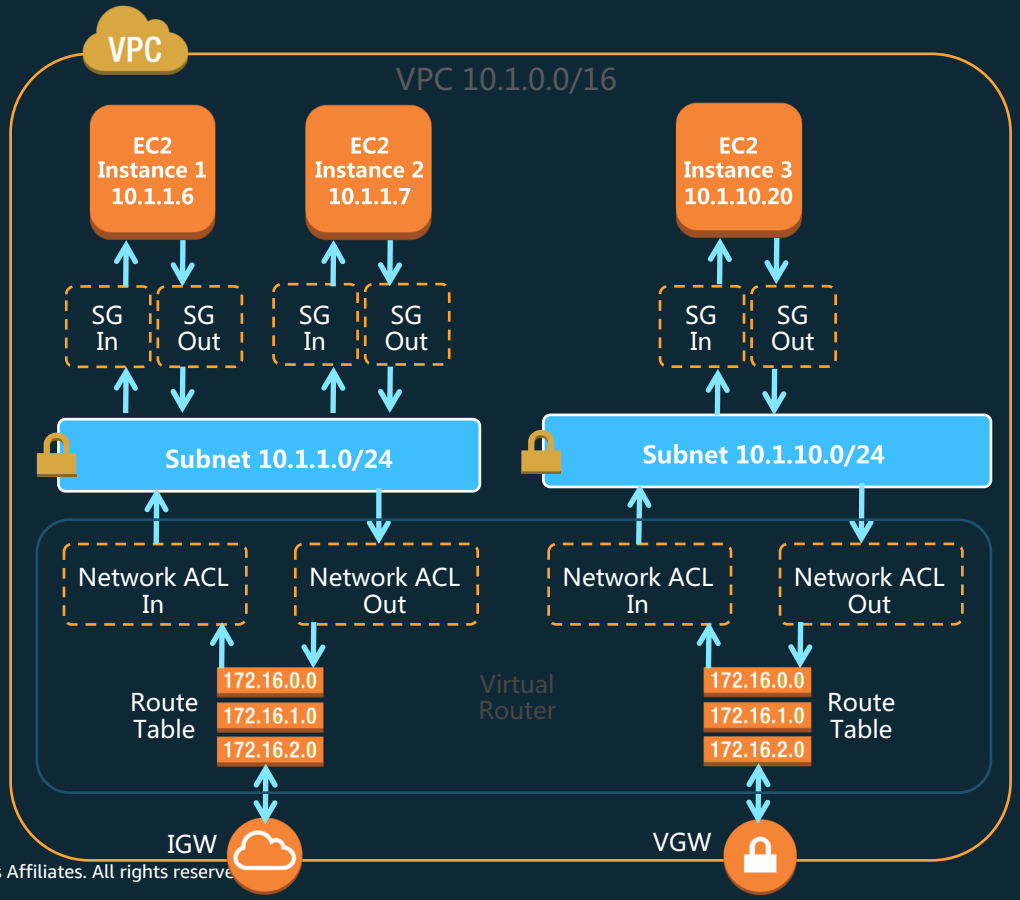
- 构建您自己的网络
- 创建您自己的子网



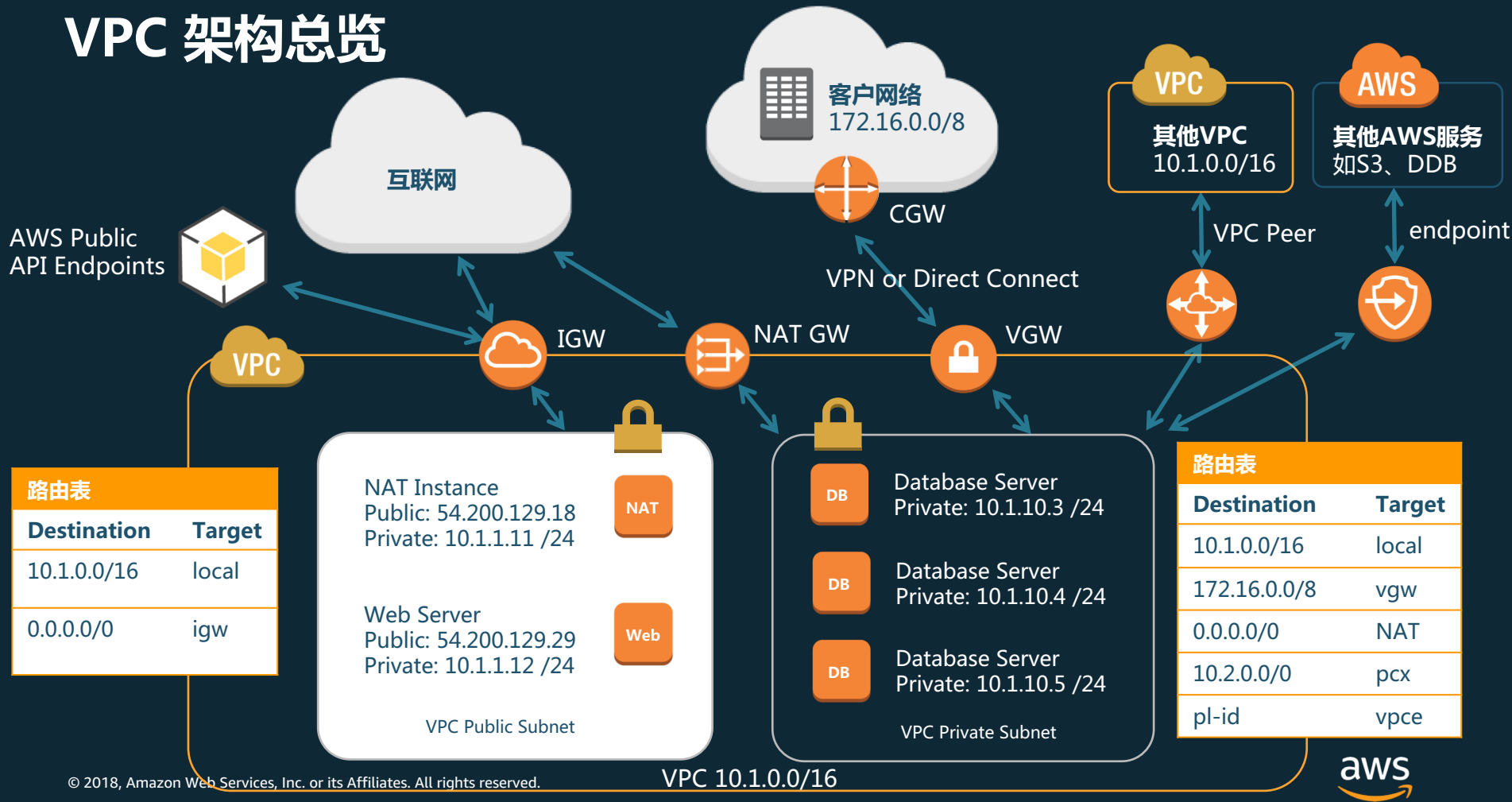
VPC 网关 – Internet 网关 (IGW)



VPC 安全控制



VPC 架构总览



路由表

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	igw

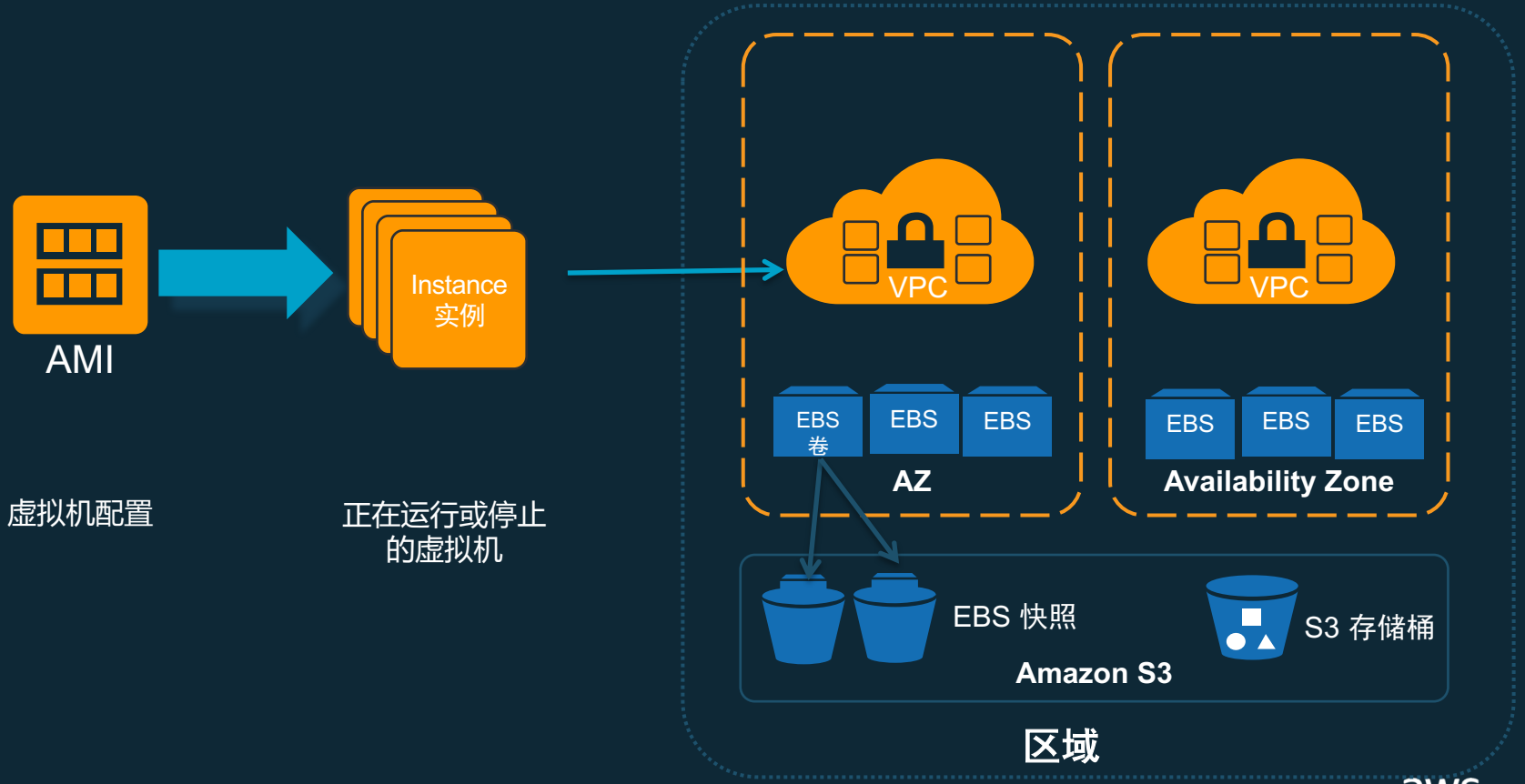
路由表

Destination	Target
10.1.0.0/16	local
172.16.0.0/8	vgw
0.0.0.0/0	NAT
10.2.0.0/0	pcx
pl-id	vpce

③

计算服务: EC2相关服务

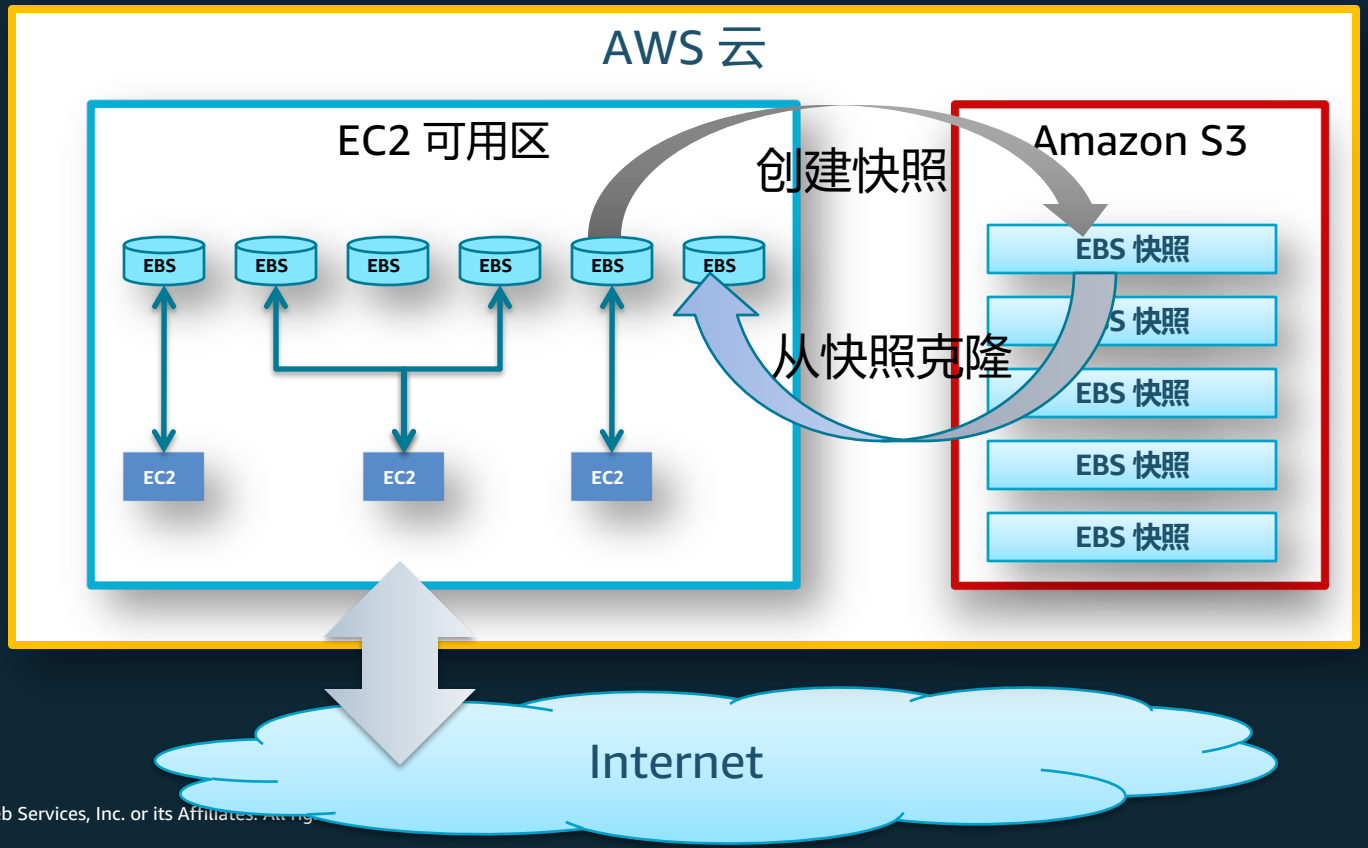
EC2 术语



虚拟机配置

正在运行或停止的虚拟机

EBS 快照



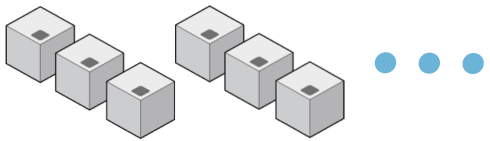
购买选项一览

按需实例
On-Demand

按使用量付费

正常的小时费率

无承诺用量



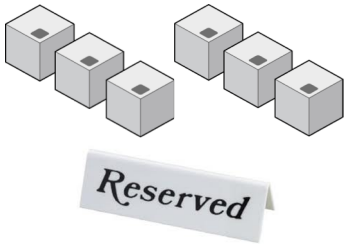
预留实例
Reserved

支付低额预付费用

预留实例资源

保证更低的小时费率

可销售或修改预留

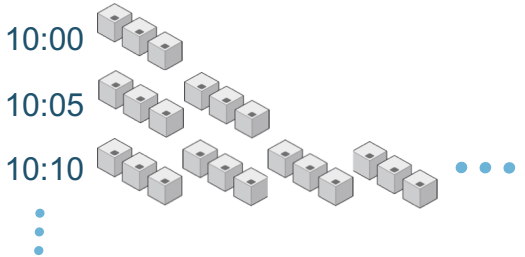


竞价实例
Spot

为您所需的竞价：Bid what you like—您出价高于现价时您的竞价实例开始运行

相比按需实例节约高达 90% 的费用

可运行大量的实例



aws

AWS计算服务

Amazon EC2

云中的弹性 虚拟服务器

Amazon ECS

Docker 容器集群管理

Auto Scaling

自动缩放 EC2 容量

Elastic Load Balancing

动态 流量分发

Amazon EKS

高可用的 Kubernetes服务

Amazon Fargate

无需管理服务器或集群运行容器

Amazon LightSail

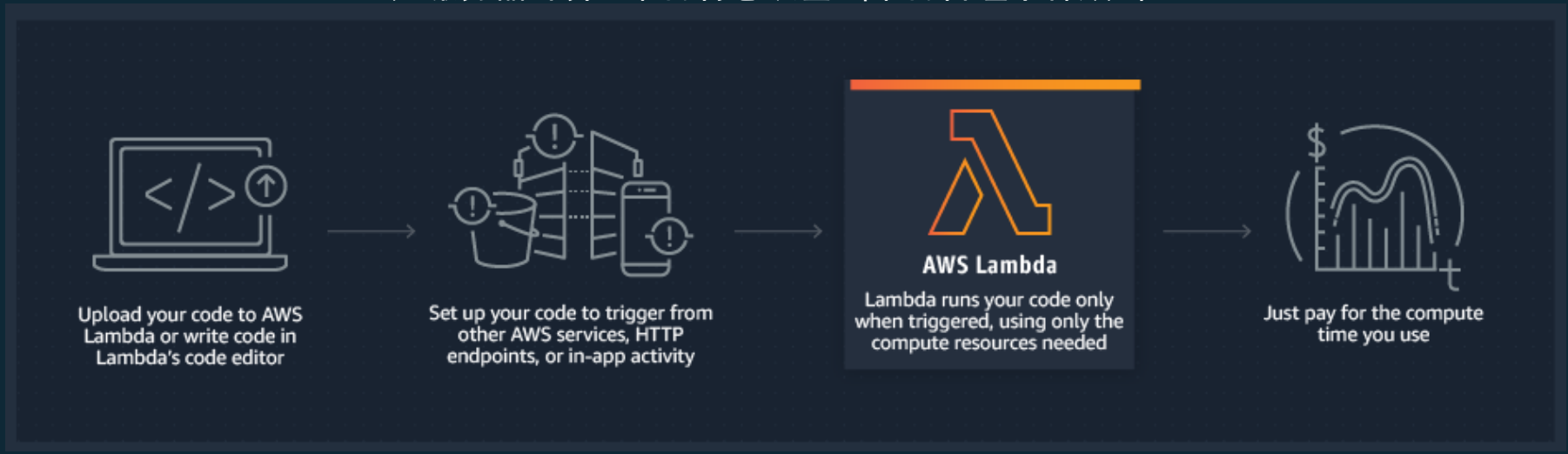
提供快速启动项目 一切资源

AWS Batch

完全托管的 批处理服务

Lambda: 无服务器、事件驱动的计算服务

无服务器计算：架构将您从基础架构管理中释放出来



专注开发，而不需要服务器管理

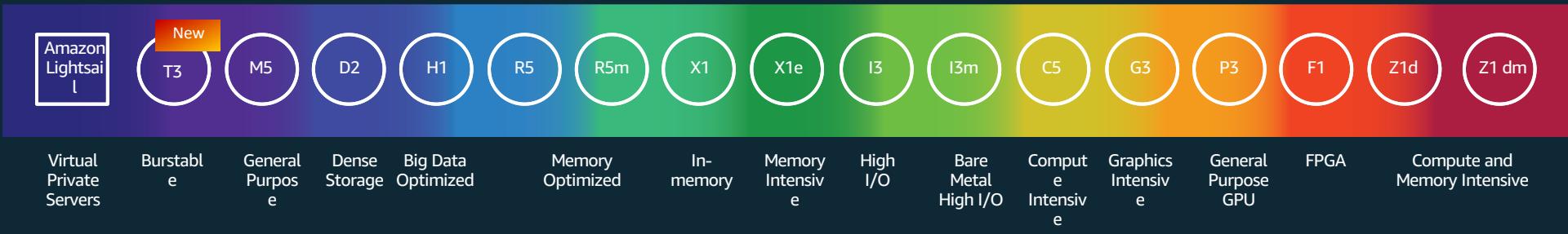
代码设置成由各种触发条件激活运行

代码按需要运行并可持续扩展

只需按照使用的时间付费

Amazon Lambda：https://aws.amazon.com/lambda/

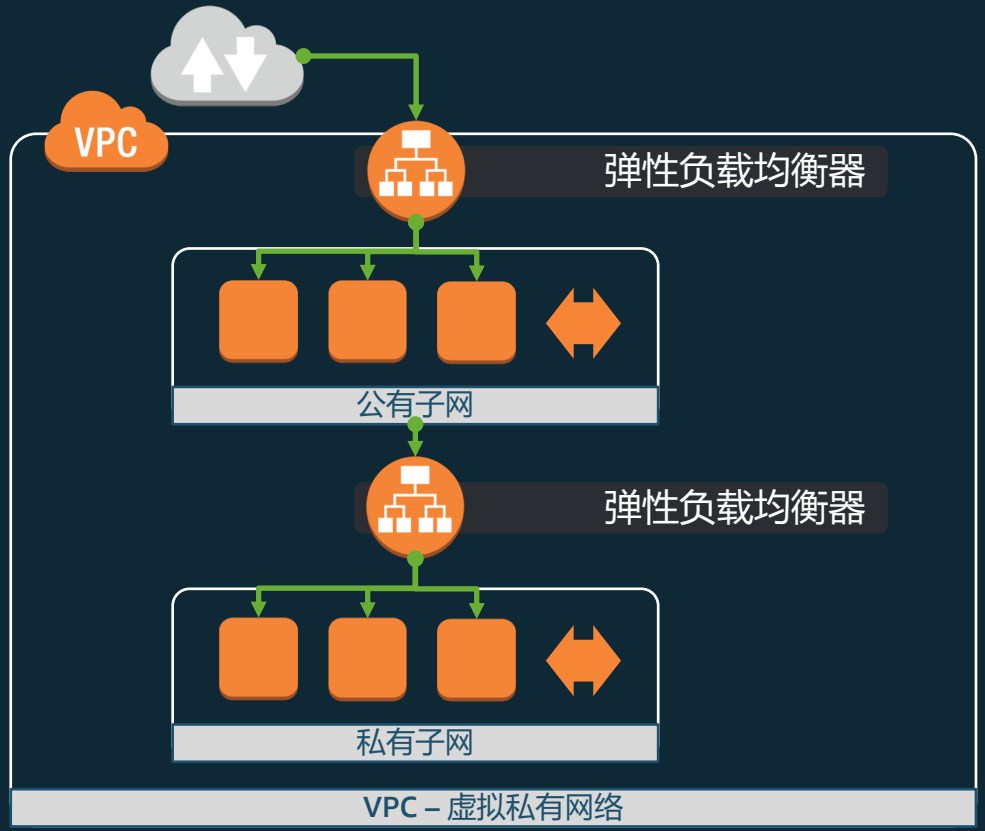
EC2 实例: 丰富的实例类型



EC2 Elastic Graphics
- 支持EC2实例的图形加速

EC2 Fleet
- 简化算力预估
- 超大规模集群
- 根据需求弹性伸缩

连接到实例： 负载均衡器



三种负载均衡器

Elastic Load Balancing 支持三种负载均衡器：Application Load Balancer、网络负载均衡器 (新) 和 Classic Load Balancer。选择能满足您需求的负载均衡器类型。 了解哪种负载均衡器更适合您

应用程序负载均衡器

创建

如果您使用 HTTP 和 HTTPS 流量的 Web 应用程序需要灵活的功能集，请选择应用程序负载均衡器。应用程序负载均衡器在请求级别运行，面向包括微服务和容器在内的应用程序架构提供高级路由功能和可见性功能。

了解更多信息 >

网络负载均衡器

创建

当您需要超高性能、大规模终止 TLS 连接的能力、集中部署证书的能力以及对应用程序使用静态 IP 地址时，请选择网络负载均衡器。网络负载均衡器在连接级别运行，每秒钟能够安全地处理数百万个请求，同时维持超低延迟。

了解更多信息 >

Classic Load Balancer

上一代

用于 HTTP、HTTPS 和 TCP

创建

当您在 EC2-Classic 网络中运行现有应用程序时，请选择 Classic Load Balancer。

了解更多信息 >

THANK YOU