



# AWS Well-Architected

AWS资深解决方案架构师  
Weiqiong Chen

A man with a beard and balding head, wearing a dark suit, stands in a blurred city street holding a large white sign. He is smiling slightly and looking towards the camera. The background is a soft-focus view of a city with buildings, trees, and other people.

*"Are you well  
Architected ? "*

*Werner Vogels*

# 什么是 AWS Well-Architected Framework ?



要素



设计原则



问题

# Well-Architected Framework 的五大要素



卓越运营



安全性



可靠性



性能效率



成本优化

# 设计原则



一般设计原则



各要素的具  
体设计原则

# 一般设计原则

停止猜测您的容量需求

进行生产级系统测试

实现自动化，使架构试验变得更容易

支持实现架构演进

利用数据驱动架构

通过实际演练不断改进



# 要素问题结构

## 基础

### REL 1: 如何管理您账户的 AWS 服务限制？

AWS 账户配置了默认的服务限制，以便防止新用户意外配置超出其需要的资源。

您应评估您的 AWS 服务需求并针对各个使用区域请求对相应限制进行适当的更改。

#### 最佳实践：

- 监控和管理限制：评估您在 AWS 上的预期使用情况，相应提高您的区域性限制，并支持使用量按计划增长。
- 设置自动监控：实施软件开发工具包等工具，让系统在使用量接近阈值时向您发送提醒。
- 注意固定的服务限制：注意无法更改的服务限制并根据这些限制设计架构。
- 确保您的服务限制与最高使用量之间有足够的宽裕度，以便能够进行故障转移。
- 跨所有相关账户和区域考虑服务限制。

## 要素区域

## 问题文本

## 问题背景

## 最佳实践

# 选择 Well Architected 的原因？



更快地构建和部署



做出明智决定



降低或缓解风险



学习 AWS  
最佳实践

# 一种服务于云之旅的机制



学习



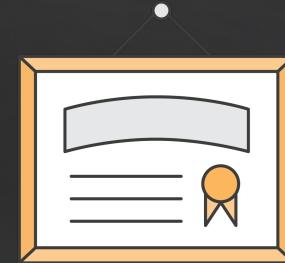
衡量



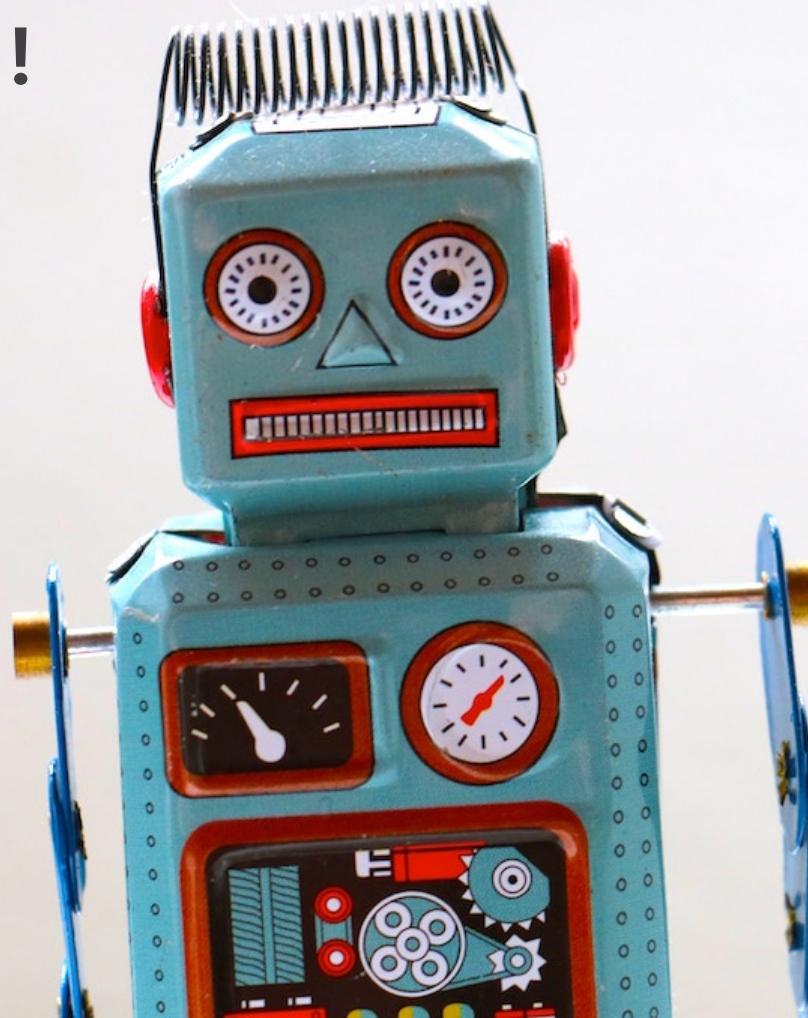
提高

# Well-Architected

## 卓越运营要素



# 实现完全自动化！



# 卓越运营 的设计原则



执行运营即代码

注释文档

频繁进行小型、可回滚的增量变更

经常改进运营流程

预测故障

从所有运营故障中吸取经验教训



# 卓越运营要素

准备

运营

演进

其他资源

卓越运营考虑事项和相  
应的重要 AWS 服务



- 您如何设计工作负载以便自己了解其状态？
- 您如何缓解部署风险？

## 准备

### AWS Config 和 AWS Config 规则

可用于为工作负载创建标准，并在投入生产之前确定环境是否符合这些标准。

## 卓越运营考虑事项和相 应的重要 AWS 服务



- 您如何了解工作负载的运行状况？
- 您如何了解自己的运营状况？

## 运营

### Amazon CloudWatch

它可供您监控工作负载的运行状况



卓越运营考虑事项和相  
应的重要 AWS 服务



- 如何改进运营？

## 演进

**Amazon Elasticsearch Service (Amazon ES)**

它可供您分析日志数据，以便快速安全地获取可行见解

# 其他资源

卓越运营要素

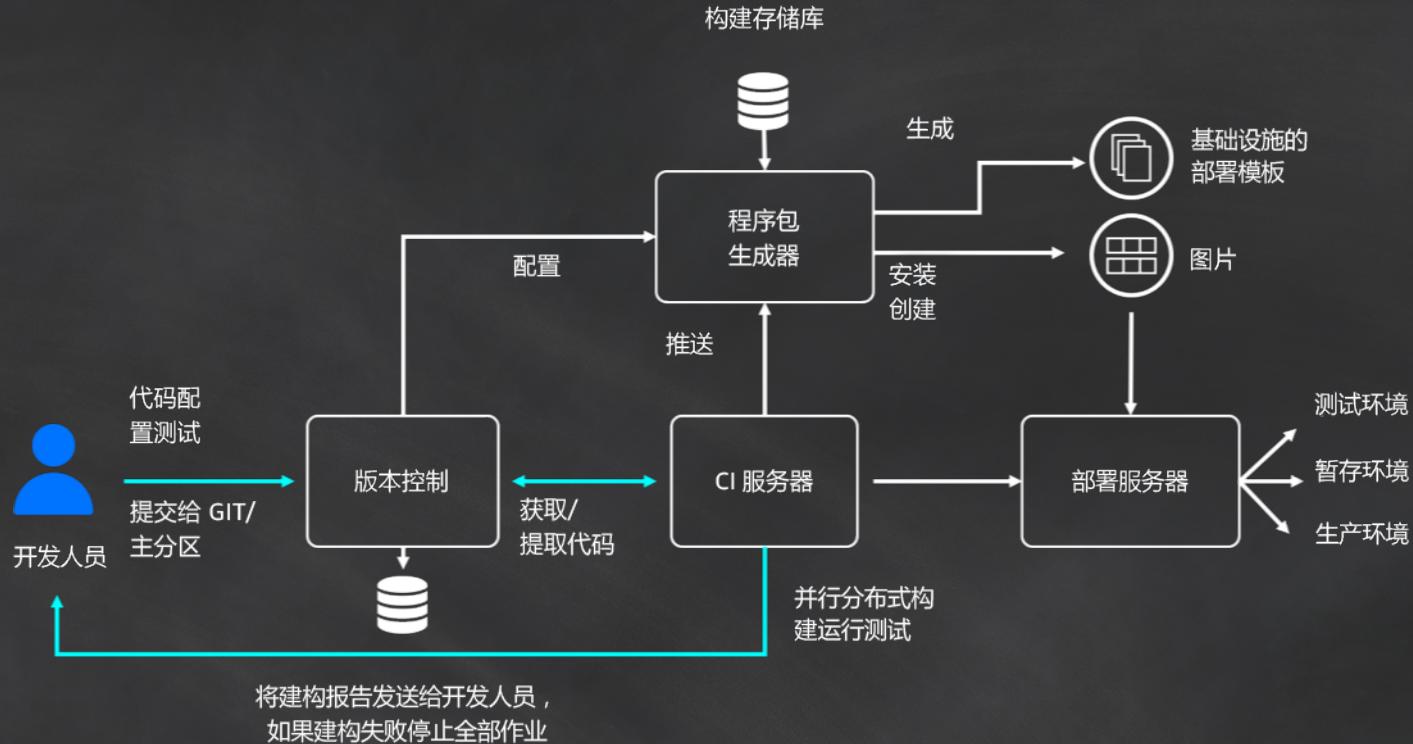


## 开发运营

<https://aws.amazon.com/devops/>

来自 AWS re:Invent 2018 的视频：  
通过容器化工作负载实现卓越运营  
<https://www.youtube.com/watch?v=rtk3rRdAZ6s>

# 运营即代码



# Well-Architected

## 安全性要素



# 什么是安全性？

在创造商业价值的同时，通过风险评估和缓解策略  
保护信息、系统和资产的能力。

# 安全性的 设计原则



实施强大的身份验证基础

实现可追溯性

在所有层面应用安全机制

自动实施最佳安全防护实践

保护动态数据和静态数据

限制对数据的访问

做好应对安全性事件的准备



# 安全性要素

身份与访问管理

检测性控制

基础设施安全性

数据保护

事件响应

其他资源

安全性考虑事项和相应  
的重要 AWS 服务



- 您如何管理凭证和身份验证？
- 您如何控制人员访问？

## 身份与访问管理

**AWS Identity and Access Management (IAM)**

安全地控制对 AWS 服务和资源的访问

**AWS Organizations**

基于策略管理多个 AWS 账户

**AWS Secrets Manager**

在整个生命周期内轻松轮换、管理和检索数据库凭证、  
API 密钥和其他密钥

## 安全性考虑事项和相应的重要 AWS 服务



- 您如何检测和调查安全事件？
- 如何抵御新出现的安全威胁？

## 检测性控制

### AWS CloudTrail

让您对 AWS 账户实现监管、合规性和运营/风险审计

### Amazon GuardDuty

提供智能威胁检测和持续监控，用于保护您的 AWS 账户和工作负载

### VPC 流日志

捕获有关传入和传出您的 VPC 中网络接口的 IP 流量的信息。

## 安全性考虑事项和相应的重要 AWS 服务



- 如何保护网络？
- 如何保护计算资源？

## 基础设施安全性

### Amazon Virtual Private Cloud (VPC)

AWS 中预置的一个逻辑隔离的部分，让您可以在自己定义的虚拟网络中启动 AWS 资源

### Amazon Cloud Front 和 AWS Shield

CloudFront 是一个全球内容分发网络，可以安全地为观看者提供数据、视频、应用程序和 API，并与 AWS Shield 集成以实现 DDoS 缓解。

### AWS WAF – Web 应用程序防火墙

保护您的 Web 应用程序免受常见 Web 漏洞威胁，确保可用性和安全性

安全性考虑事项和相应  
的重要 AWS 服务



- 如何保护您的静态数据？
- 如何保护传输中的数据？

## 数据保护

### AWS Key Management Service (KMS)

轻松地创建和控制用于加密数据的密钥

### AWS Certificate Manager

轻松地预置、管理和部署用于 AWS 服务的 SSL/TLS 证书

## 安全性考虑事项和相应的重要 AWS 服务



### - 您如何响应事件？

## 事件响应

### AWS Lambda

使用我们的无服务器计算服务来运行代码，无需预置或管理服务器，这样您就可以扩展对事件的编程式自动响应

### AWS Support

使用支持工程师帮助改变您的实验团队规模，通过获得工具和专业知识组合来支持业务关键应用程序。

# 其他资源

## 安全性要素



### AWS Marketplace

利用行业中的软件和规则集补充您的防御层以构建额外的弹性

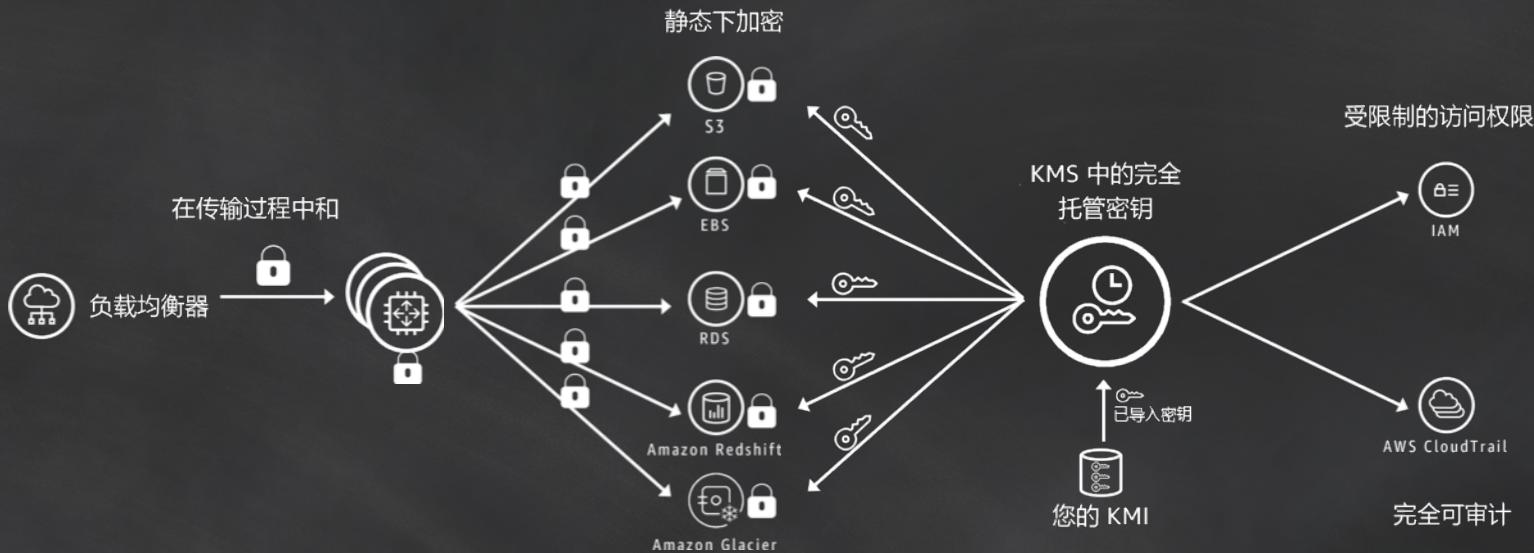
### AWS 白皮书

从范围涉及安全性最佳实践、工作负载和合规性特定主题的全系列技术 AWS 白皮书中了解相关技术

### AWS 安全初始账户设置

<https://aws.amazon.com/answers/security/aws-secure-account-setup/>

# 普适加密



# Well-Architected 性能效率要素



# 性能效率 的设计原则



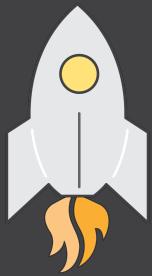
普及先进技术

数分钟内实现全球化部署

使用无服务器架构

提升实验频率

软硬件协同编程



# 性能效率要素

选择

检查

监控

权衡

其他资源

## 性能效率考虑事项和相 应的重要 AWS 服务



- 如何选择表现最好的架构？
- 如何选择数据库解决方案？

## 选择

### Auto Scaling

确保您有足够的实例来满足需求并保持响应能力的关键。

### Amazon EBS

提供各种存储方案（例如 SSD 和预配置每秒输入/输出操作 [预置 IOPS]），支持您根据自身用例进行优化。

### Amazon RDS

提供各种数据库功能（例如预置 IOPS 和只读副本），让您可以根据自己的使用场景进行优化。

## 性能效率考虑事项和相 应的重要 AWS 服务



- 如何改进工作负载以便利用  
新的版本？

## 检查

AWS 网站上的 AWS 博客和新增功能部分  
关于新发布的功能和服务的学习资源。

## 性能效率考虑事项和相 应的重要 AWS 服务



- 如何监控资源以便确保其性能符合预期？

## 监控

### Amazon CloudWatch

提供指标、告警和通知，您可以将它们与现有监控解决方案集成，并与 AWS Lambda 一起使用以便触发操作

## 性能效率考虑事项和相 应的重要 AWS 服务



- 如何使用权衡机制来提高性能？

## 权衡

Amazon ElastiCache、Amazon CloudFront 和  
AWS Snowball

有些服务可供您提高性能

Amazon RDS 中的只读副本  
允许您扩展包含大量读取操作的工作负载

# 其他资源

## 性能效率要素



来自 AWS re:Invent 2018 的视频：扩展到第一个 1000 万用户 (ARC205-R1)

<https://www.youtube.com/watch?v=Ma3xWDXTxRg>

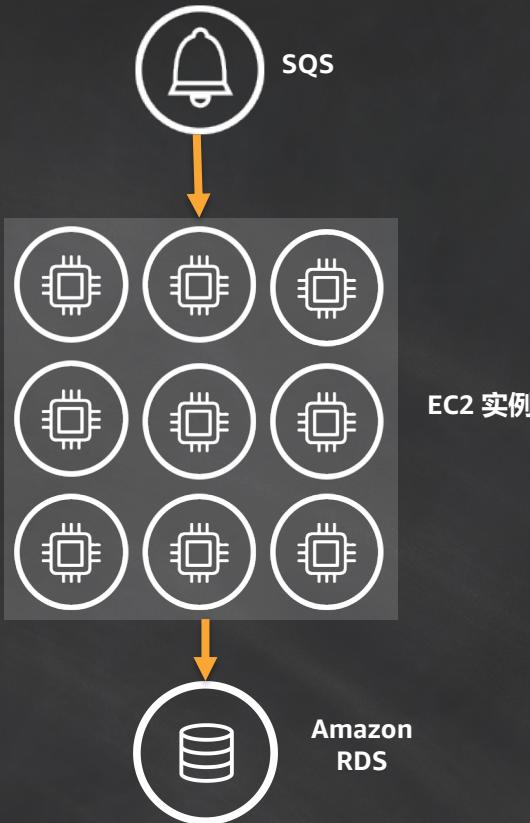
来自 AWS re:Invent 2018 的视频：Amazon EC2 实例和性能优化最佳实践 (CMP307-R1)

<https://www.youtube.com/watch?v=W0PKclqP3U0>

# 通过缓存实现数据库优化



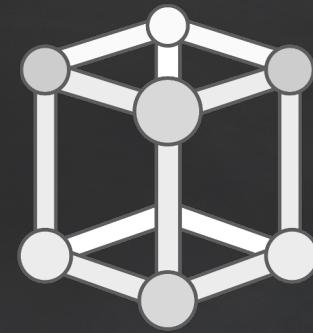
良好



更好



# Well-Architected 可靠性要素



“

故障是注定的，每种产品长期  
使用后最终都会发生故障。

”

*Werner Vogels*  
*CTO – Amazon.com*



# 什么是可靠性？

“可靠性要素包含系统从基础设施或服务中断中恢复、动态获取计算资源以满足需求以及减少诸如配置错误或暂时性网络问题等中断的能力。”

# 可靠性 的设计原则



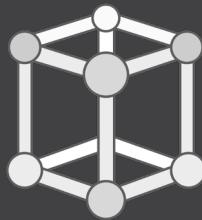
测试恢复过程

自动从故障中恢复

横向扩展以提高聚合系统的可用性

无需预估容量

变更管理自动化



## 可靠性要素

基础

变更管理

故障管理

其他资源

## 可靠性考虑事项和相应的重要 AWS 服务



- 您如何管理服务限制？
- 如何管理您的网络拓扑？

## 基础

### AWS IAM

您可以通过它安全地控制对 AWS 产品和资源的访问

### Amazon VPC

让您在 AWS 云中部署一个私有隔离的部分，并在这个虚拟网络中启动 AWS 资源

### AWS Trusted Advisor

让您能够了解服务限制

## 可靠性考虑事项和相应的重要 AWS 服务



- 您的系统如何适应需求变化？
- 如何监控您的资源？

## 变更管理

### AWS CloudTrail

记录您账户的 AWS API 调用，并向您发送日志文件以供事后审计

### Amazon Auto Scaling

是一项服务，可为已部署的工作负载提供自动化需求管理

### Amazon CloudWatch

让您能够发出关于指标的提醒（包括自定义指标），并获得日志记录功能，可用于聚合您的资源中的日志文件。

## 可靠性考虑事项和相应的重要 AWS 服务



- 如何备份数据？
- 如何规划灾难恢复？

## 故障管理

### AWS CloudFormation

提供用于创建 AWS 资源的模板，并以有序和可预测的方式预置这些模板

### Amazon S3

提供高度持久的服务来保留备份

### Amazon Glacier

提供高度持久的存档

# 其他资源

## 可靠性要素



### 容许故障：错误注入和服务可靠性

<https://www.youtube.com/watch?v=wrY7XoOnysg&t=6s>

### 如何管理我的 AWS 服务限制？

<https://aws.amazon.com/premiumsupport/knowledge-center/manage-service-limits/>

### AWS 灾难恢复

<https://aws.amazon.com/disaster-recovery>

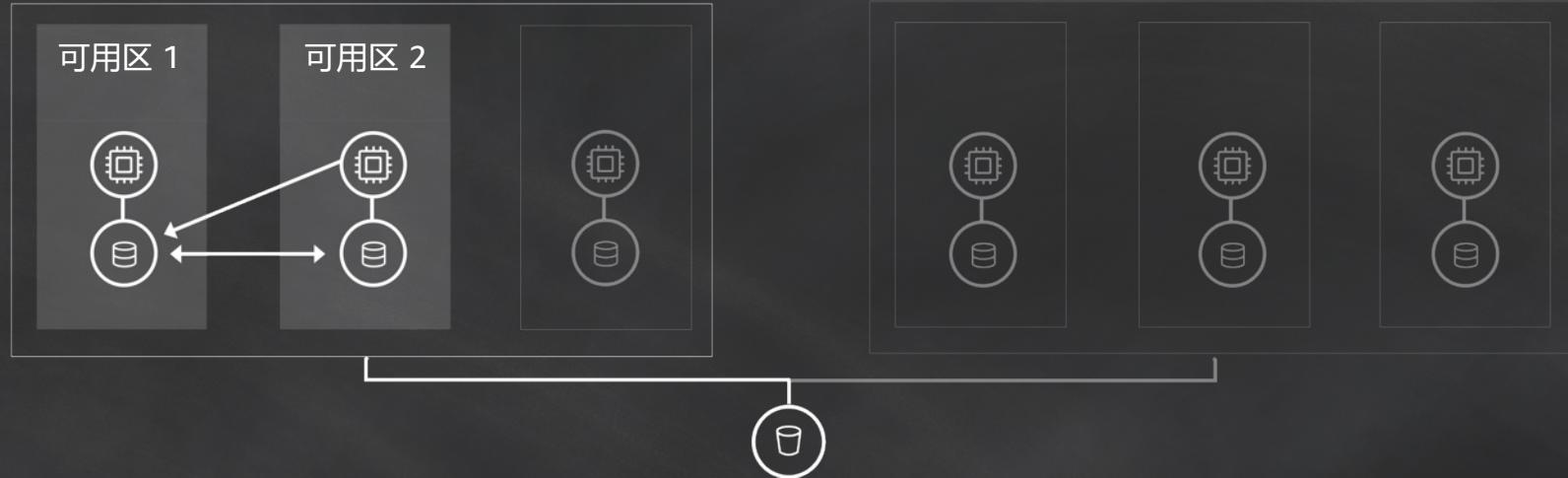
# 可用性 +

区域 1



# 可用性 ++

区域 1



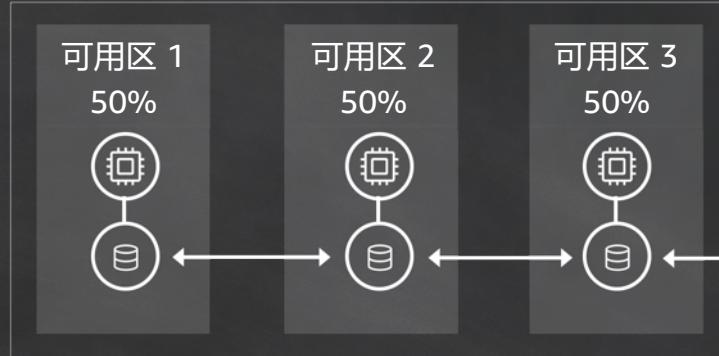
# 可用性 + + +

区域 1

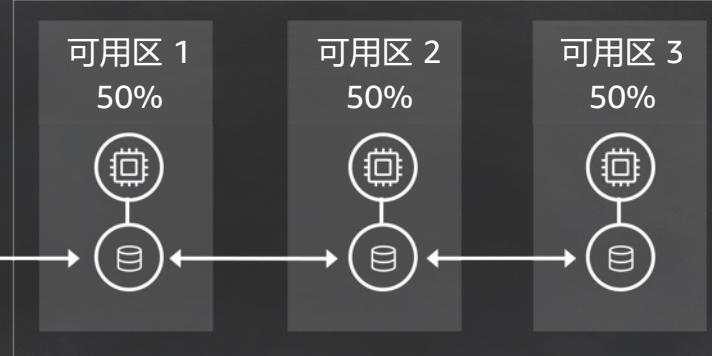


# 可用性 + + + + +

区域 1



区域 2



# Well-Architected

## 成本优化要素



# 关闭未使用的实例



# 成本优化 的设计原则



采用消费模式

衡量整体效率

不再将钱投入数据中心运营

对支出进行分析和归因

使用托管服务降低拥有成本



## 成本优化要素

了解支出情况

具有成本效益的资源

供需匹配

持续优化

其他资源

成本优化考虑事项和相关的重要 AWS 服务



- 您如何管理使用情况？
- 如何监控使用情况和成本？

## 了解支出情况

**AWS Cost Explorer**  
让您能够查看和跟踪使用详情

**AWS Budget**  
当您的使用量或开支超出实际或预计的预算金额通知您

## 成本优化考虑事项和相关的重要 AWS 服务



- 您在选择服务时如何评估成本？
- 您如何规划数据传输费用？

## 具有成本效益的资源

### Cost Explorer

检查您在一段时间内的 AWS 资源消费规律，根据规律尽量采用预留实例

### Amazon CloudWatch 和 Trusted Advisor

帮助您正确地选择资源规模

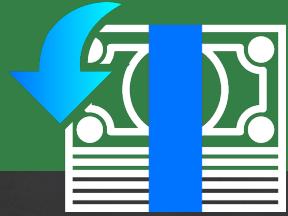
### RDS 上的 Amazon Aurora

消除数据库许可成本

### AWS Direct Connect 和 Amazon CloudFront

优化数据传输

## 成本优化考虑事项和相关的重要 AWS 服务



- 您如何将资源供应与需求匹配？

### 供需匹配

#### Auto Scaling

让您能够添加或删除资源以匹配实际需求，而不会超支

成本优化考虑事项和相关的重要 AWS 服务



## - 如何评估新服务？

## 持续优化

AWS 新闻博客和新增功能  
关于新发布的功能和服务的学习资源

### AWS Trusted Advisor

检查您的 AWS 环境，为您寻找节省开支的机会，包括停用或释放未使用的或闲置的资源，或是采用一部分的预留实例容量取代按需实例。

# 其他资源

## 成本优化要素



### AWS 简单月度成本计算器

帮助客户和潜在客户更加高效地估计其每月 AWS 账单。

### AWS 总体拥有成本 (TCO) 计算器

通过减少对大规模资本支出的需要并提供按使用量付费模型，  
帮助您降低总拥有成本 (TCO)

# 了解您的成本

每项服务的成本是多少？

每个小时的成本是多少？

标记至关重要

项目 = IronMan 使用了哪些资源？

部门 = Accounts 的支出是多少？

按您的使用量显示成本！无需等待账单！

# 框架白皮书包含问答

<https://aws.amazon.com/well-architected/>





谢谢 !