



Amazon CloudFront Extensions

CloudFront 拓展功能

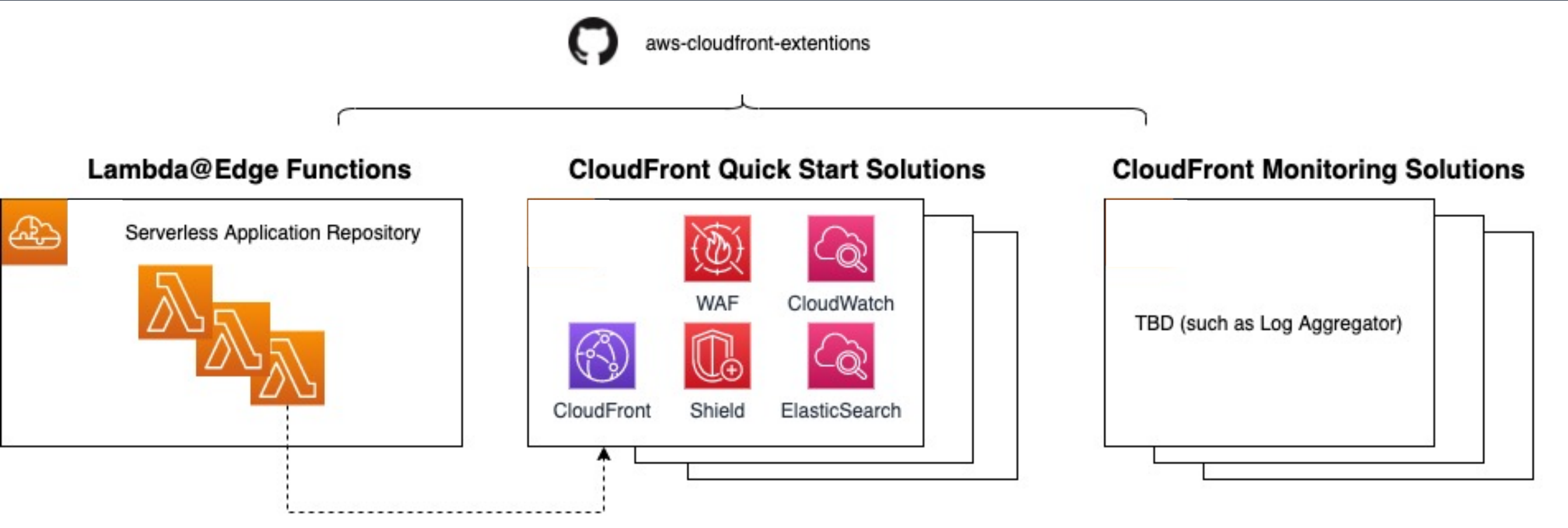
吕宁，亚马逊云科技 解决方案架构师

目录

- CloudFront Extensions 介绍
 - Lambda@Edge 和 CloudFront Function 合集
 - WAF & Shield 自动化部署
 - CloudFront 监控
- 动手实验
 - 通过 Cognito 实现鉴权功能

CloudFront Extensions 介绍

CloudFront Extensions 介绍



24 Lambda@Edge
9 CFF

WAF & Shield
自动化部署

CloudFront
监控

Lambda@Edge & CFF 合集

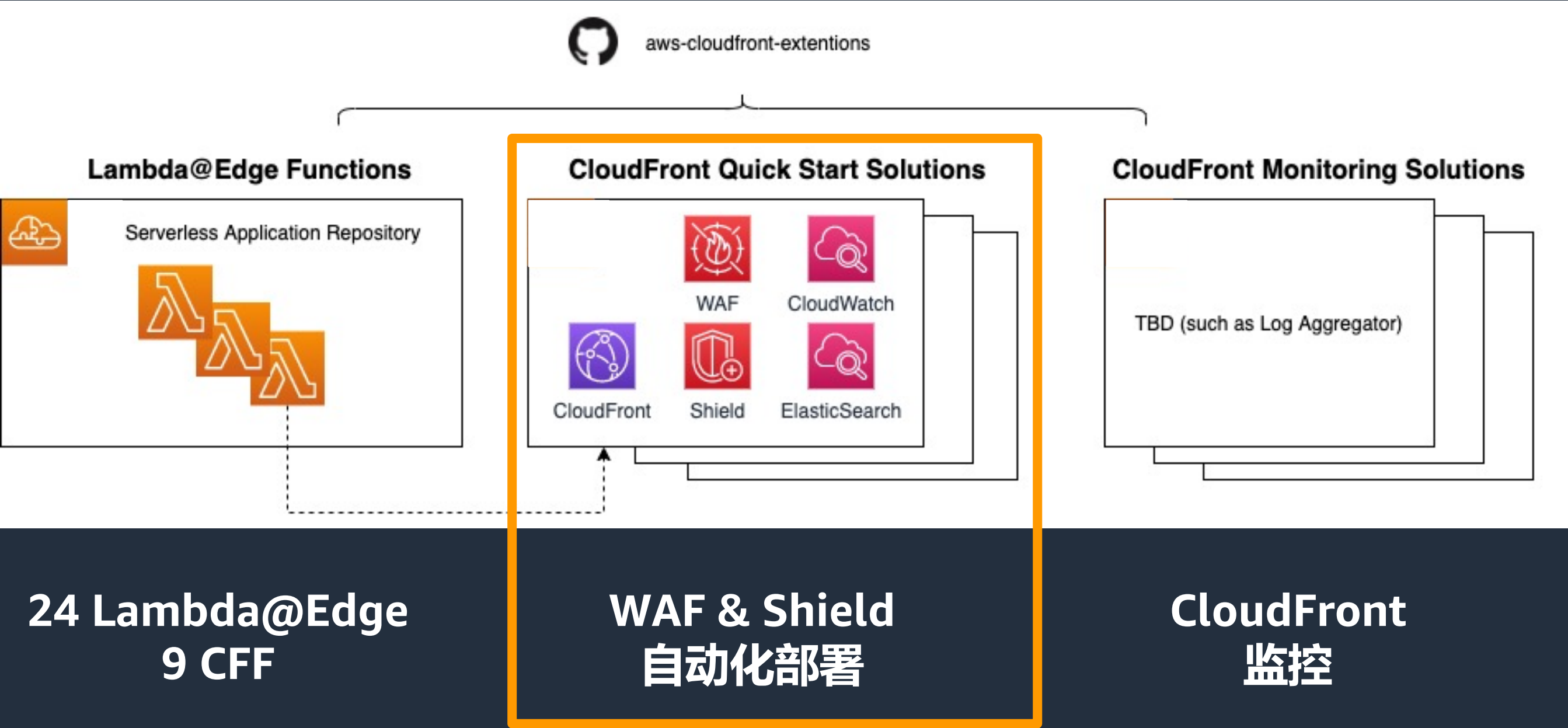
Lambda@Edge

Name	Description	Deployment Type	Deploy
Authentication by Cognito	Integrate with Cognito to provide authentication service.(Workshop)	SAR , SAM	Deploy
Adding security header	Add security header into response after successful authentication, this function will add 'strict-transport-security' to force browser using HTTPS.	SAR , SAM	Deploy

CloudFront Function

Name	Description	Deploy
Add Security Headers	Add several response headers to enable web browsers security features.	Deploy
Cross Origin Resource Sharing	Support CORS(Cross Origin Resource Sharing) by CloudFront Function.	Deploy
Add Cache Control Headers	Add a Cache-Control header for the browser so that content can be cached locally in the browser.	Deploy

CloudFront Extensions 介绍



WAF & Shield 自动化部署

Rules (9)

EditDeleteAdd rules ▼

Find rules

< 1 > ⚙

<input type="checkbox"/>	Name	Action	Priority
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	Use rule actions	0
<input type="checkbox"/>	AwsCloudfrontWafStackWhitelistRule	Allow	1
<input type="checkbox"/>	AwsCloudfrontWafStackBlacklistRule	Block	2
<input type="checkbox"/>	AwsCloudfrontWafStackHttpFloodRegularRule	Block	3
<input type="checkbox"/>	AwsCloudfrontWafStackScannersProbesRule	Block	5
<input type="checkbox"/>	AwsCloudfrontWafStackIPReputationListsRule	Block	6
<input type="checkbox"/>	AwsCloudfrontWafStackBadBotRule	Block	7
<input type="checkbox"/>	AwsCloudfrontWafStackSqlInjectionRule	Block	20
<input type="checkbox"/>	AwsCloudfrontWafStackXssRule	Block	30

WAF 规则

WAF & Shield 自动化部署

Protections

Delete protections

Configure protections ▼

Add resources to protect

< 1 >

<input type="checkbox"/>	Name	AWS resource	Resource type	Status	Application layer (lay...
<input type="checkbox"/>	ShieldProtectionForCloudFront	↗	Cloudfront distrib...	✔ OK	CloudFront-Web-WAF ↗

Protection groups

Delete protection groups

Edit

Create protection group

< 1 >

<input type="checkbox"/>	Name	Pattern	Status	Resource type	Aggregation
<input type="checkbox"/>	ProtectionGroupForCloudFront	Arbitrary	<div><div>✔ OK</div></div>	-	Max

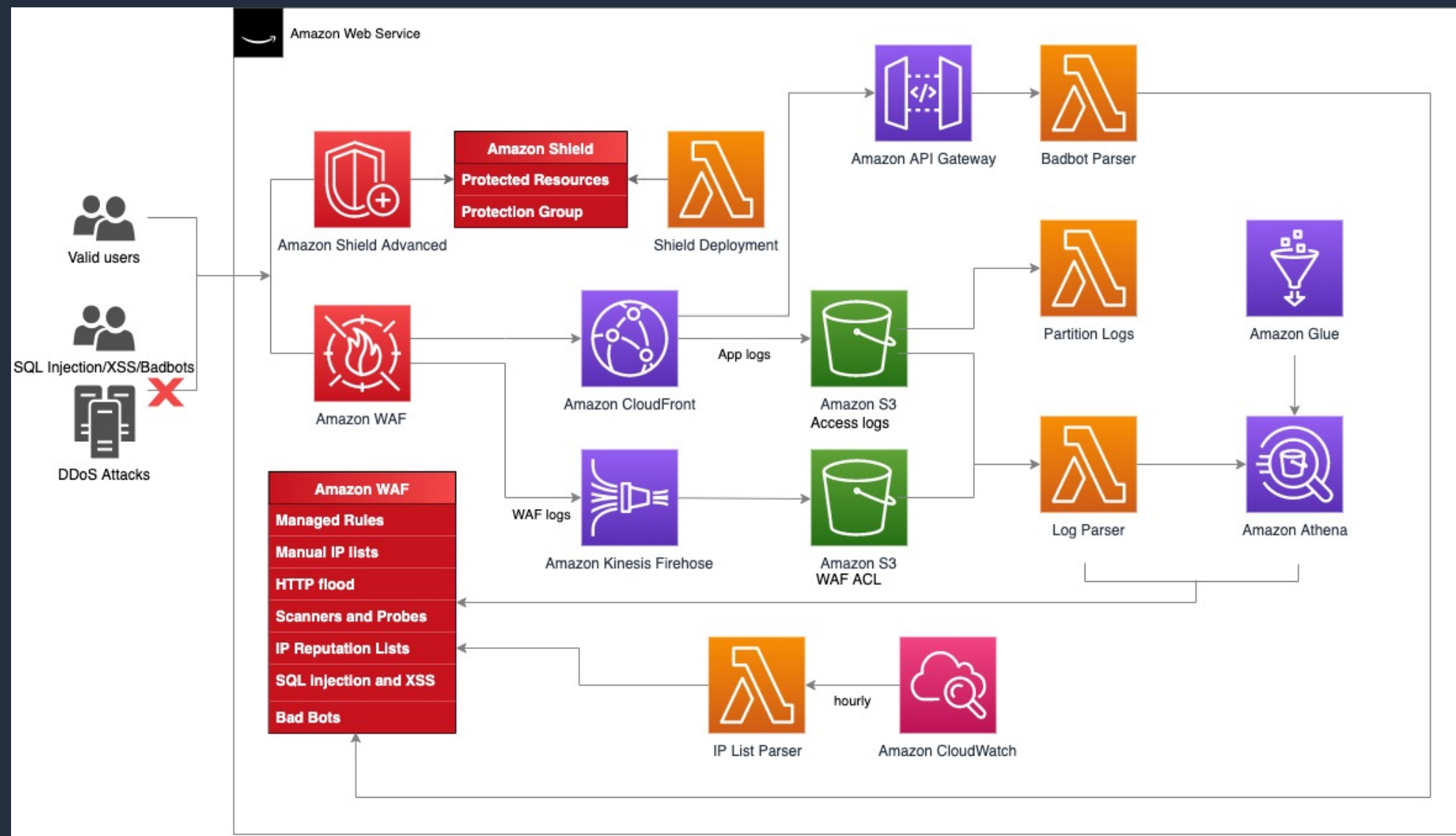
Shield 保护组

WAF & Shield 自动化部署

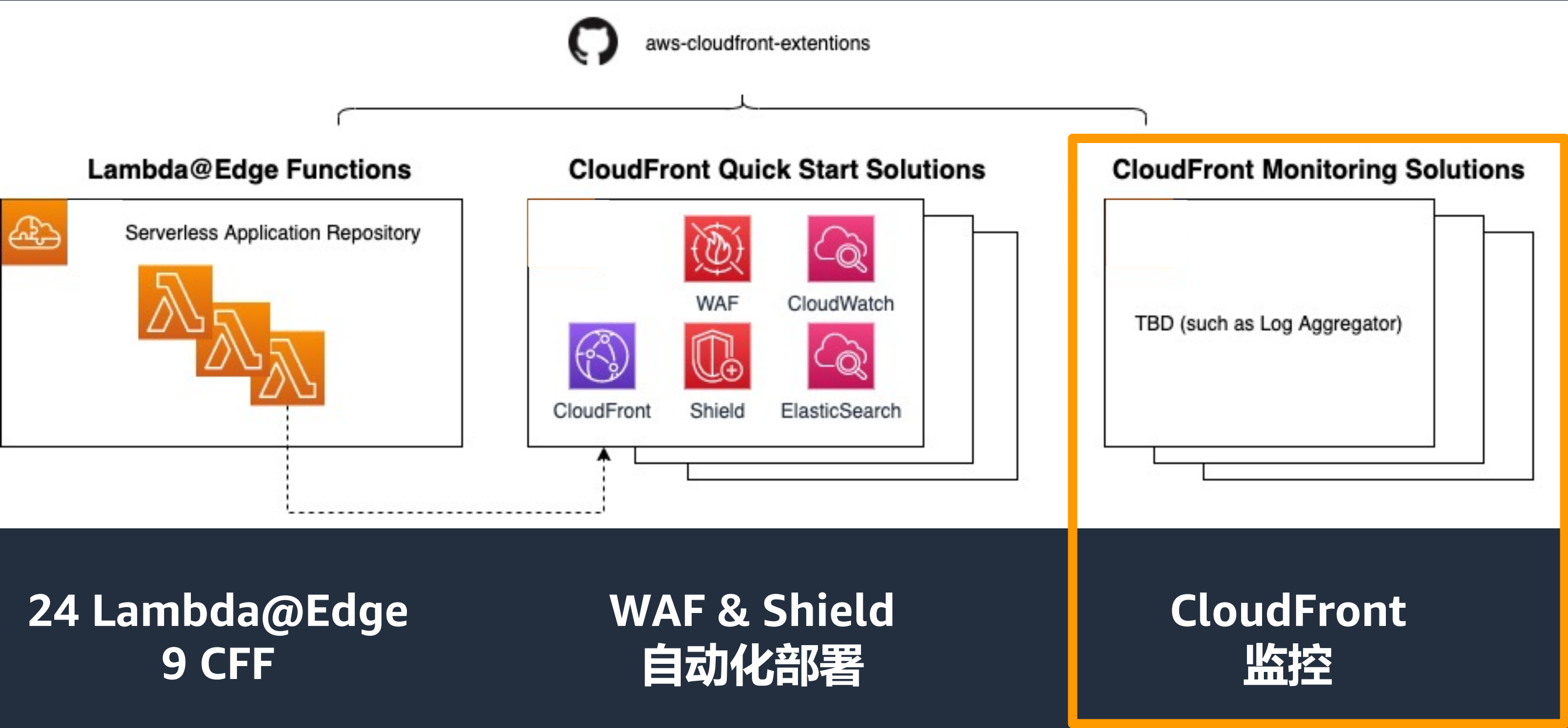
本方案可保护您的
CloudFront 免于如下攻击

- DDoS
- 爬虫
- 有风险的IP
- SQL 注入攻击
- XSS攻击

[Demo video](#)



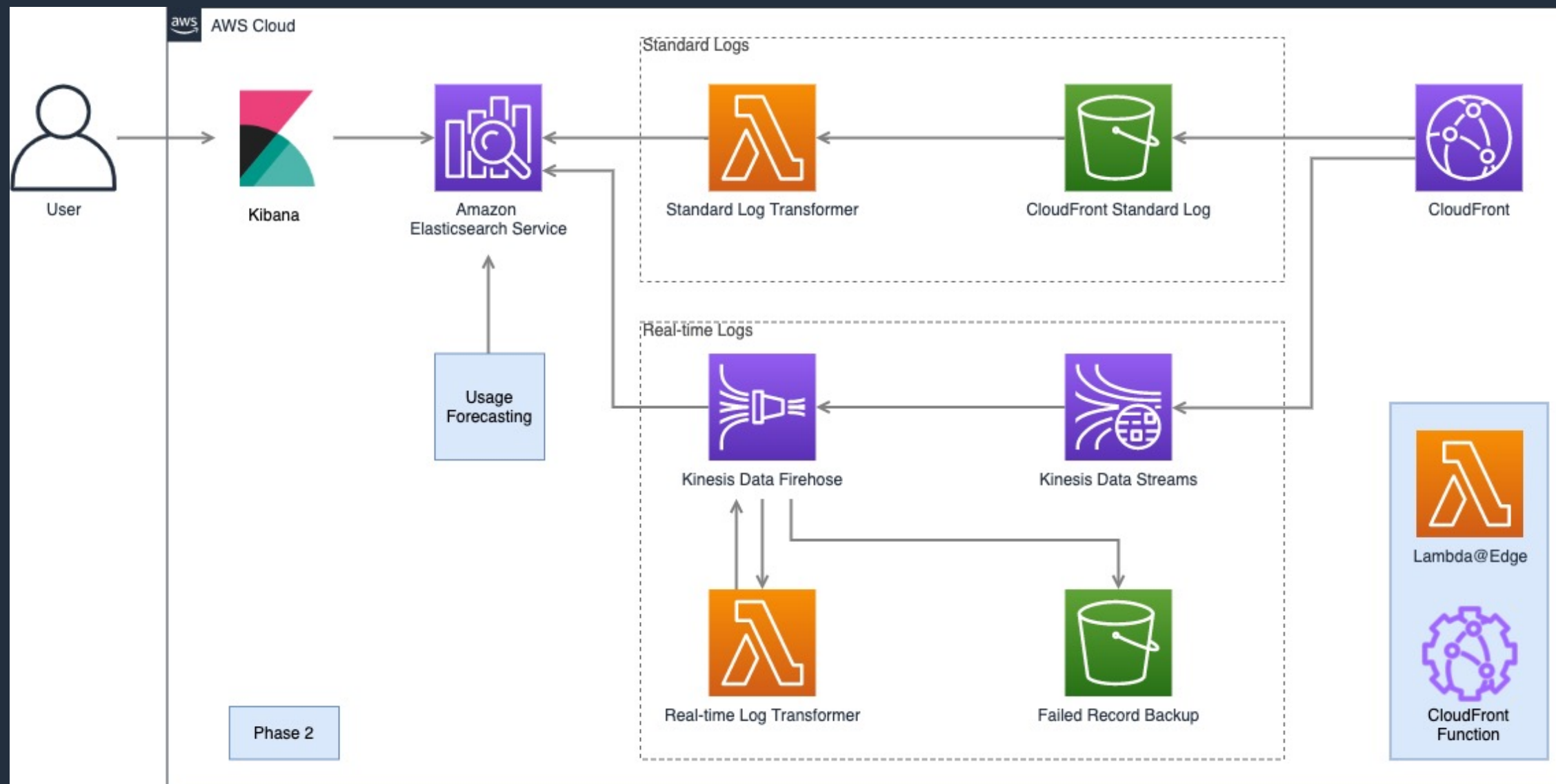
CloudFront Extensions 介绍



CloudFront 监控

[Dashboard 示例](#)

[设计文档](#)



动手实验

动手实验



开始前的准备

部署CloudFront Extensions

部署Lambda@Edge实现Cognito鉴权

部署Lambda@Edge实现根据设备类型返回相应内容

贡献

参考资料

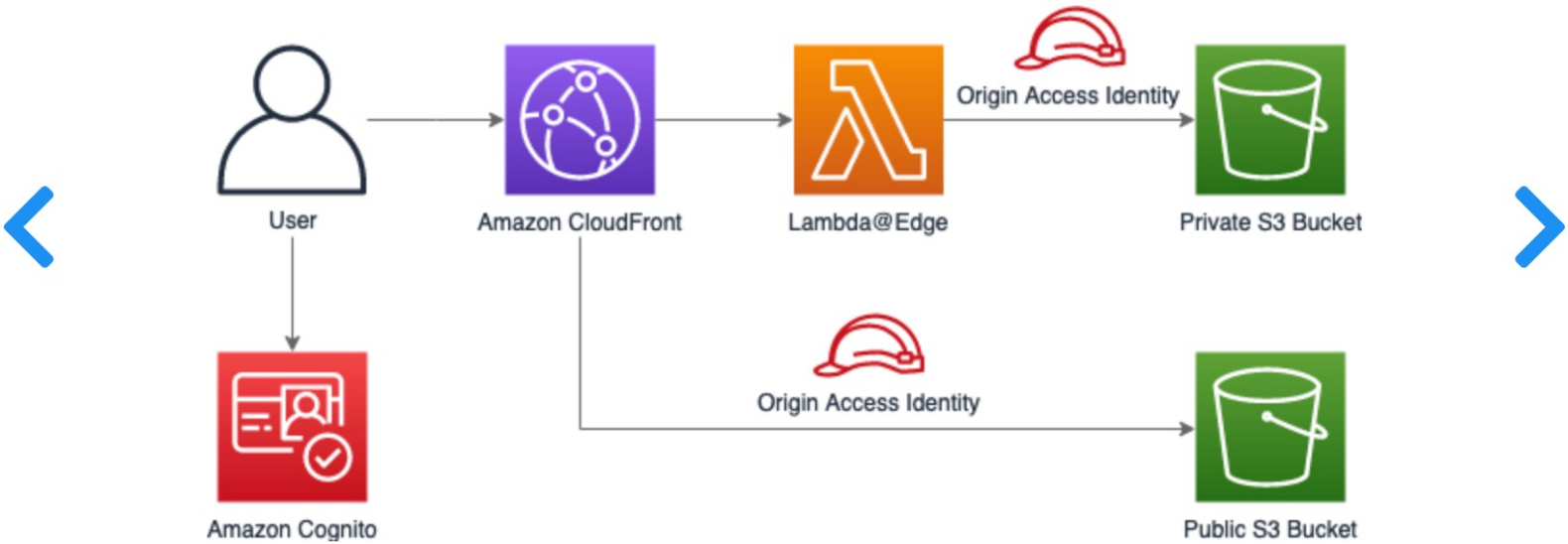
清理

Chinese

CloudFront Extensions workshop > ...

在本章中, 您将会在SAR (Serverless Application Repository) 中查找并部署一个已发布的无服务器应用。此应用会在您的网站上实现Amazon Cognito鉴权功能。

如下是本实验的架构图



包含如下两个S3桶

- 私有S3桶: 包含私有内容, 用户需要通过Amazon Cognito登录后才能访问此内容
- 公有S3桶: 包含本次实验的网站资源, 用户无需登录即可通过CloudFront访问此资源

[Workshop链接](#)



谢谢

