
aws
INNOVATE
ONLINE CONFERENCE

aws INNOVATE
ONLINE CONFERENCE

分会场一：基础设施，卫星与安全

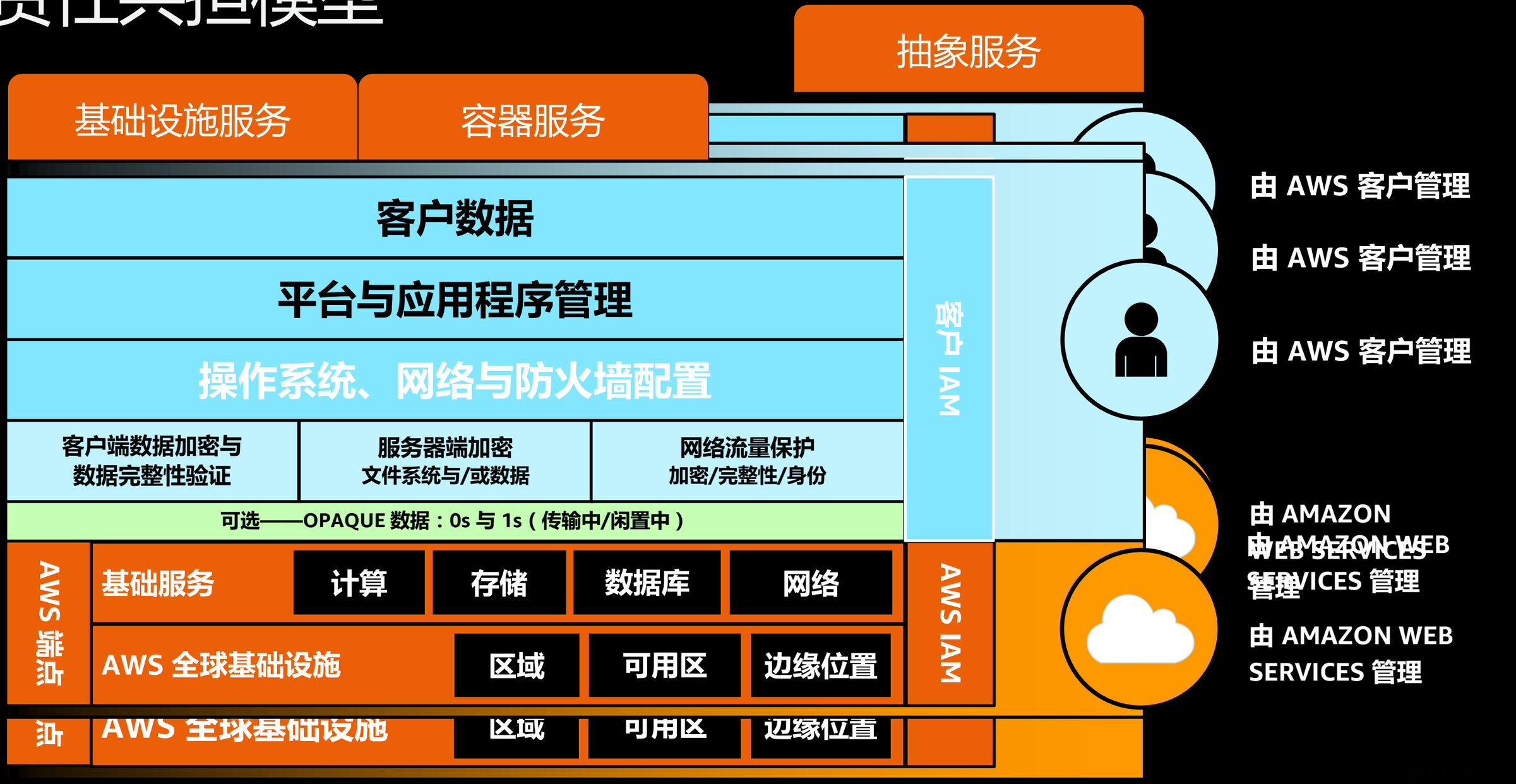
AWS 云上安全最佳实践

陈晓东，AWS 专业服务顾问

内容安排

- AWS 责任共担模型
- AWS 安全服务
- AWS 安全最佳实践

责任共担模型


抽象服务
基础设施服务
容器服务
客户数据
平台与应用程序管理
操作系统、网络与防火墙配置
客户端数据加密与
数据完整性验证
服务器端加密
文件系统与/或数据
网络流量保护
加密/完整性/身份
可选——OPAQUE 数据：0s 与 1s（传输中/闲置中）
客户 IAM
AWS 端点
基础服务
计算
存储
数据库
网络
AWS 全球基础设施
区域
可用区
边缘位置
AWS IAM
由 AWS 客户管理
由 AWS 客户管理
由 AWS 客户管理
由 AMAZON WEB SERVICES 管理
由 AMAZON WEB SERVICES 管理

AWS 安全解决方案

身份

AWS Identity and Access Management (IAM)

AWS Organizations

Amazon Cognito

AWS Directory Service

AWS Single Sign-On

检测控制

AWS CloudTrail

AWS Config

Amazon CloudWatch

Amazon GuardDuty

Amazon Virtual Private Cloud (Amazon VPC) flow logs

基础设施安全

Amazon EC2 Systems Manager

AWS Shield

AWS WAF

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

数据保护

AWS Key Management Service (AWS KMS)

AWS CloudHSM

Amazon Macie

AWS Certificate Manager (ACM)

Server side encryption

AWS Secrets Manager

事件响应

AWS Config rules

AWS Lambda

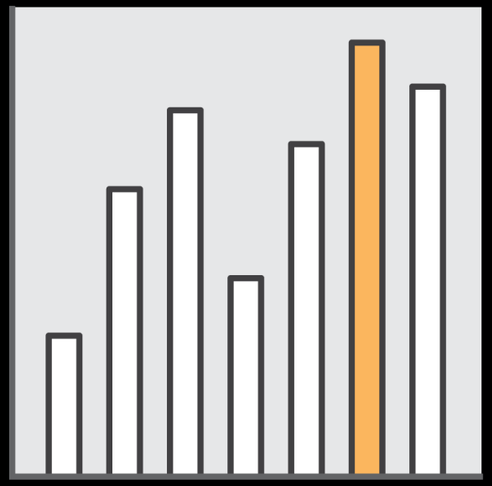
Amazon EC2 Systems Manager

账号与权限

aws INNOVATE
ONLINE CONFERENCE

AWS 账户

安全/资源边界

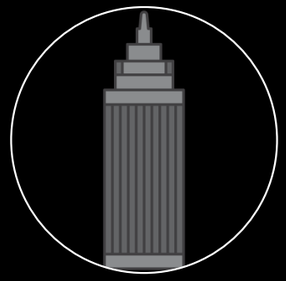


API 限制/约束

账单分离

账户模式

单一账户

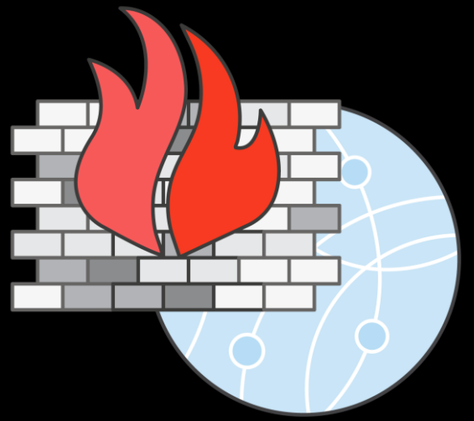


数千账户

为什么单一账户还不够？

多个团队

账单计费

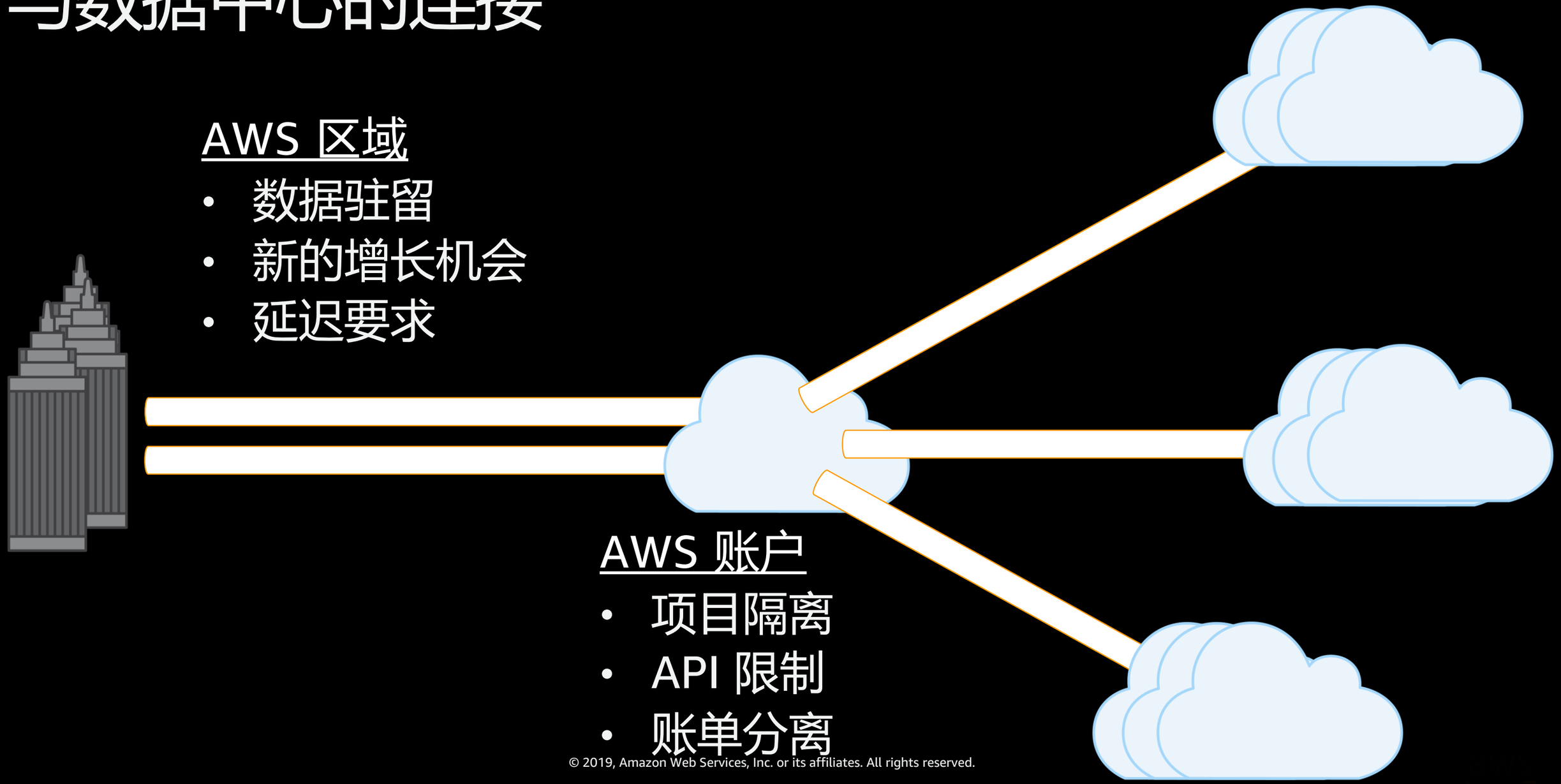


相互隔离

安全控制

业务流程

与数据中心的连接



AWS 区域

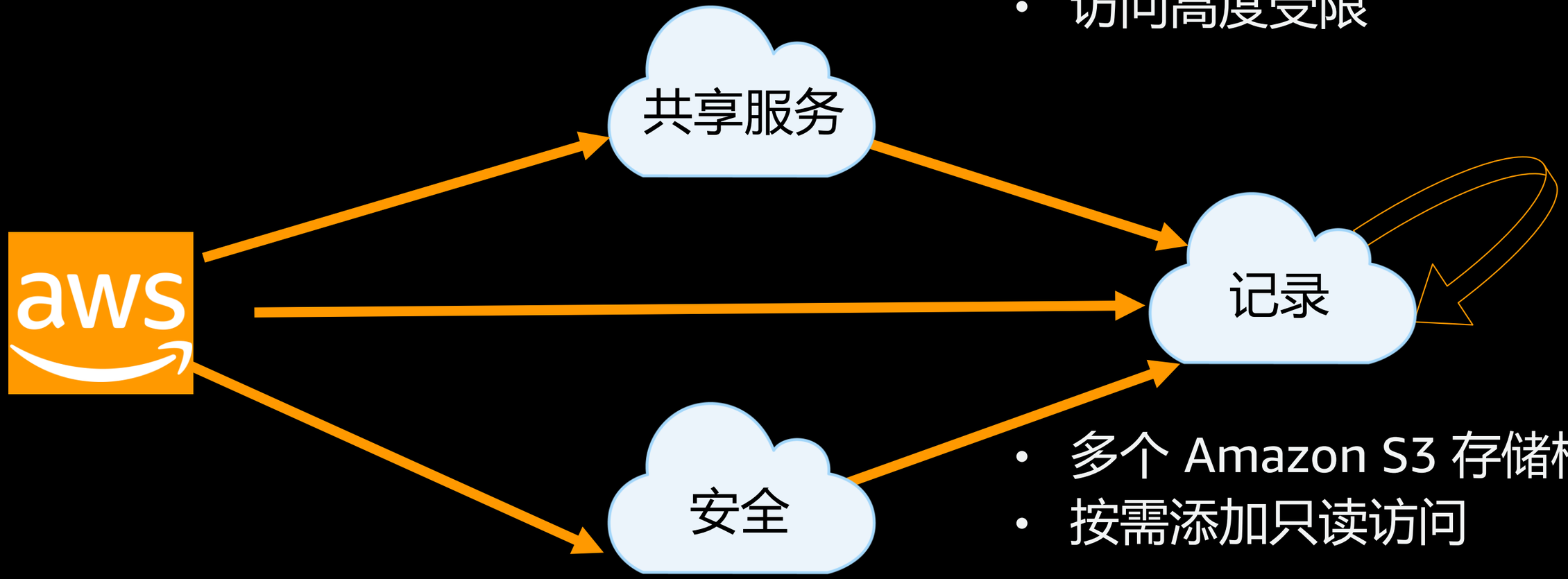
- 数据驻留
- 新的增长机会
- 延迟要求

AWS 账户

- 项目隔离
- API 限制
- 账单分离

日志账户

- 单一事实来源
- 单一安全位置
- 访问高度受限



- 多个 Amazon S3 存储桶
- 按需添加只读访问

监管账户

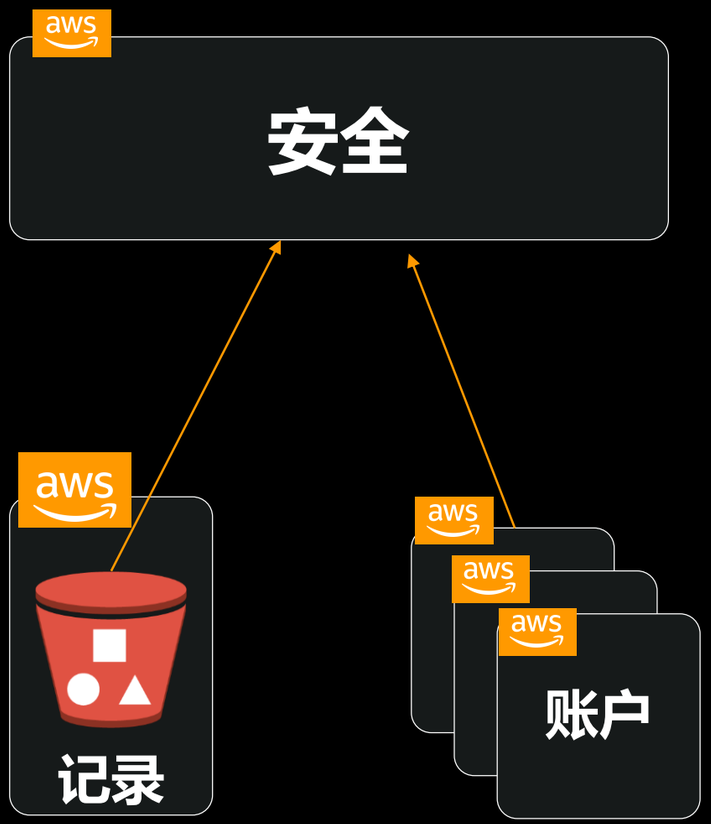
AWS Trusted Advisor

AWS Config

- 信任但需要验证
- 所有账户需要集中的窗口

- 通知而非强制执行
- 监管账户
- 选择工具

安全账户



- 安全账户用于实现 SecOps
  - 处理日志
  - 安全工具
  - 事件管理
  - 安全审计

共享服务账户

- AWS Direct Connect
- DNS 服务器
- 堡垒机
- 网络监控
- 构建 AMI

- 区分业务关键服务
- 更多访问限制
- 减少风险范围

沙箱账户

- 团队创新

- 无 Direct Connect 连接
- 多租户
- 限制性权限
- 无限制伸缩

沙箱账户

各业务部门

- 学习与实验

- 无 Direct Connect 连接
- 单租户
- 完全权限
- 受限伸缩

沙箱账户

各开发者

SDLC 账户

- 受保护 Root
- 基础网络
- 安全控制
- AWS IAM 联动
- 基础 AWS IAM 角色

非生产

- 受保护 Root
- 基础网络
- 安全控制
- AWS IAM 联动
- 基础 AWS IAM 角色

预生产

- 受保护 Root
- 基础网络
- 安全控制
- AWS IAM 联动
- 基础 AWS IAM 角色

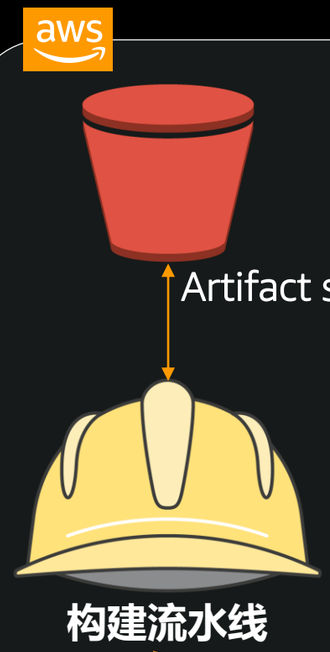
生产

- 受保护 Root
- 基础网络
- 安全控制
- AWS IAM 联动
- 基础 AWS IAM 角色

灾难恢复

CI/CD 账户

- 主机 CI/CD 流水线
- 执行混沌工程



步骤

构建 Artifact

为各个账户

- AssumeRole
- 部署 AWS CloudFormation
- 部署应用程序

CICD 账户

部署 AWS IAM 角色 | AWS CloudFormation | AWS CodeDeploy

业务开发

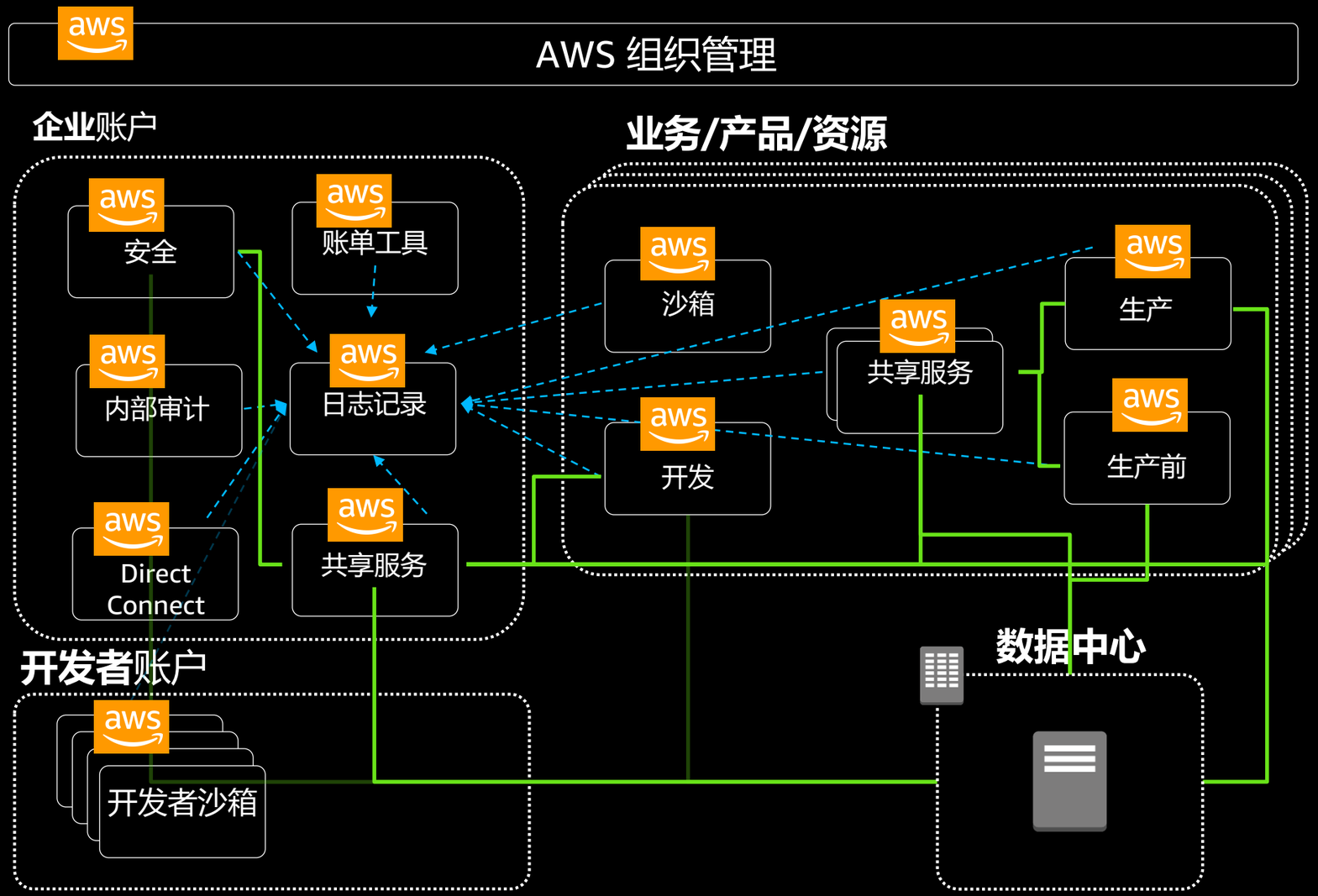
部署 AWS IAM 角色 | AWS CloudFormation | AWS CodeDeploy

业务预生产

部署 AWS IAM 角色 | AWS CloudFormation | AWS CodeDeploy

业务生产

多账户方法



组织: 账户管理

记录: 集中式日志

安全: AWS Config 规则与安全工具

共享服务: Directory、DNS、限制监控

账单工具: 成本监控

沙箱: 实验

开发: 开发

生产前: 预生产/预发布

生产: 生产

利用 AWS IAM 实现多租户资源隔离

- AWS IAM 能够为您提供资源隔离
- 在 AWS IAM 策略中设置标记条件与资源名称

- 会带来资源开销
- 并非100%覆盖

- 策略模板与自动化

条件

Action: ec2:TerminateInstances
Condition:
StringEquals:
"ec2:ResourceTag/app-id": "123"

资源名称

Action: iam:PassRole
Resource: arn:aws:iam::*:Role/123*

基础架构安全

aws INNOVATE
ONLINE CONFERENCE

什么是安全组

- 安全组
  - 在实例级别运行
  - 仅支持允许规则（白名单）
  - 有状态
  - 每个安全组最多 50 条规则，最多支持5个组
  - 默认禁止所有入站，允许所有出站
  - 安全组的源可以是安全组

CIDR 和安全组源示例

Name	Group ID	Group Name	VPC ID	Description
org-portal_webtier_elb_dev	sg-a3c4d9c6	org-portal_webtier_elb_dev	vpc-a9b143cc	org-portal_webtier_elb_dev
org-portal_webtier_dev	sg-b2c4d9d7	org-portal_webtier_dev	vpc-a9b143cc	org-portal_webtier_dev

Security Group: sg-b2c4d9d7

Description | **Inbound** | Outbound | Tags

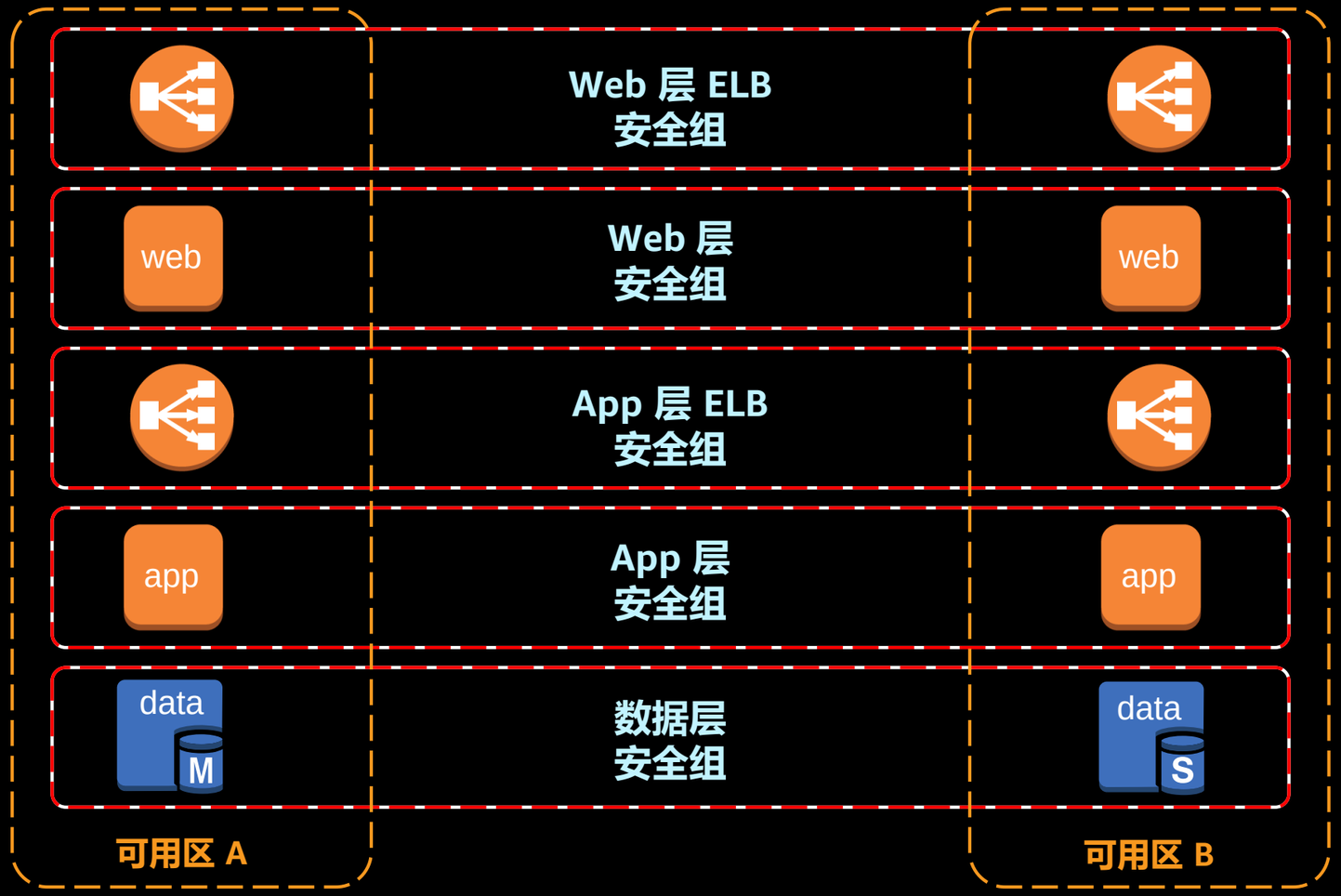
Edit

Type	Protocol	Port Range	Source
All traffic	All	All	10.81.0.0/16
HTTP	TCP	80	sg-a3c4d9c6 (org-portal_webtier_elb_dev)

如何配置安全组

- 安全组默认允许所有出流量的规则
- 在安全组上修改这条缺省的出流量的规则会增加复杂性，因此不推荐，除非有合规的要求
- 大多数企业为每类应用在安全组中配置入站规则
- 优先考虑使用安全组作为源
- 如果要安全组内实例通讯，请将源设为自己

安全组链图



入站规则
Allow TCP Port 443
Source: 0.0.0.0/0 (Any)

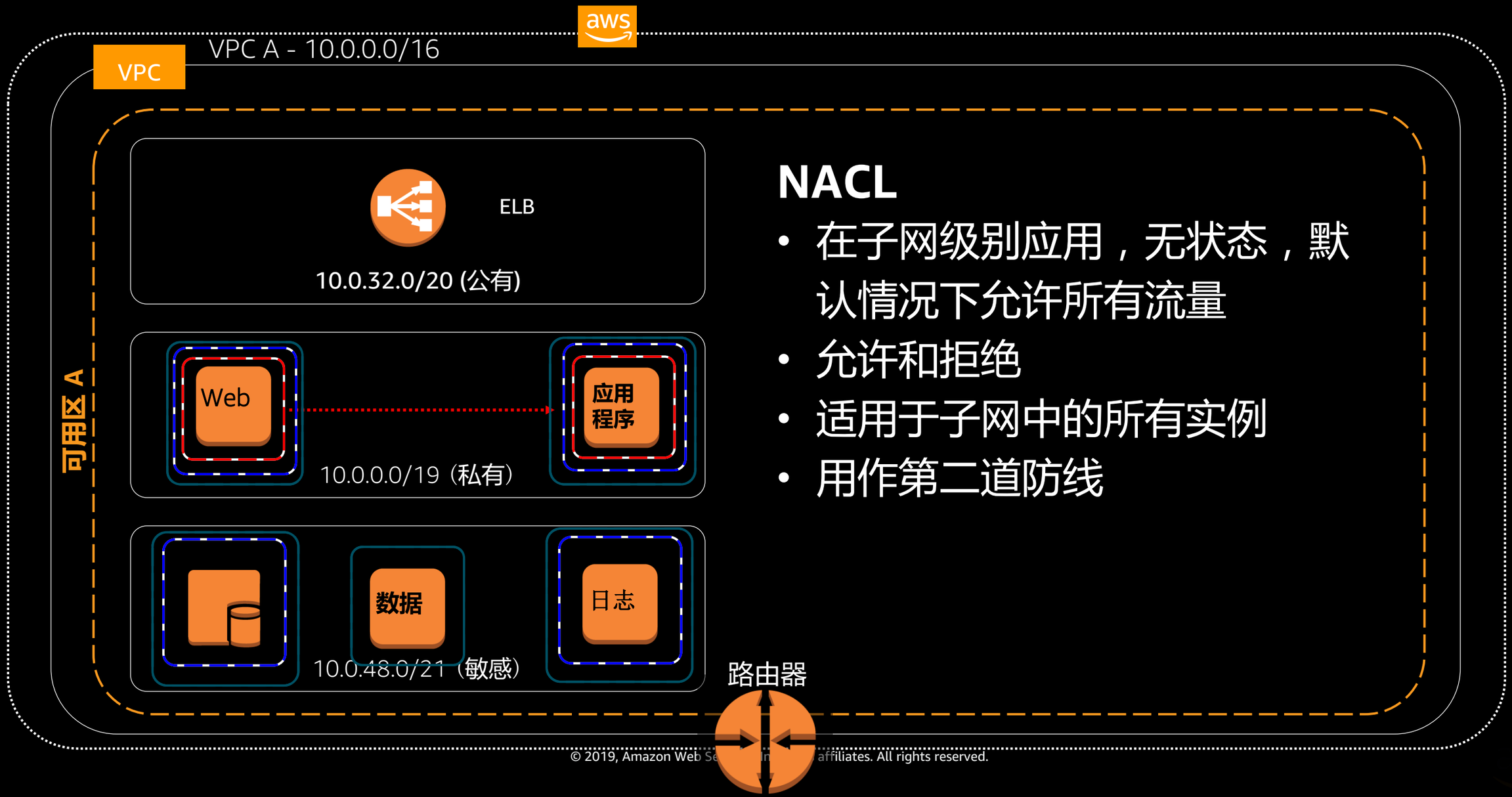
入站规则
Allow TCP Port 80
Source: Web 层 ELB

入站规则
Allow TCP Port 8080
Source: Web 层

入站规则
Allow TCP Port 8080
Source: App 层 ELB

入站规则
Allow TCP Port 3306
Source: App 层

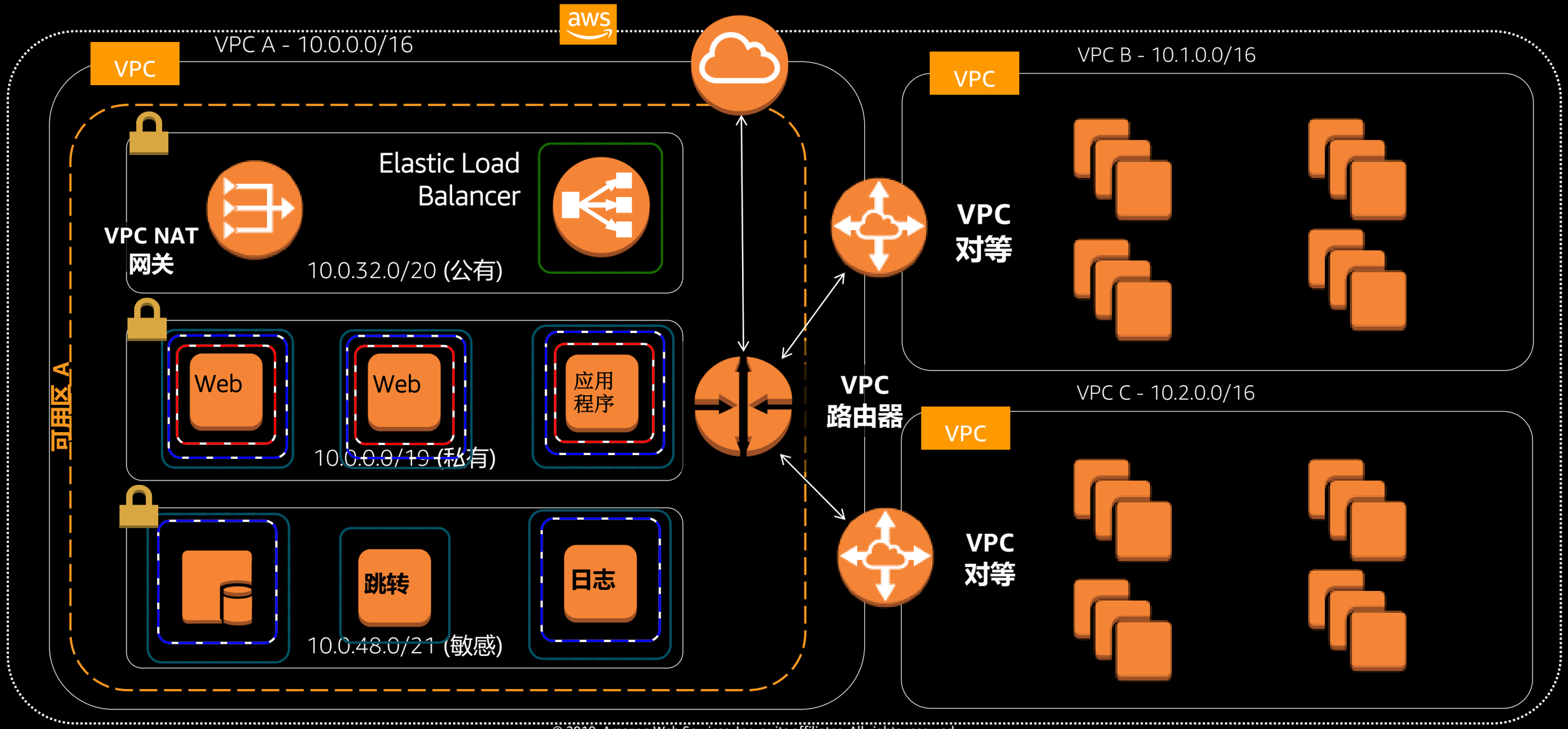
什么是 Network ACLs



NACL

- 在子网级别应用，无状态，默认情况下允许所有流量
- 允许和拒绝
- 适用于子网中的所有实例
- 用作第二道防线

VPC 对等



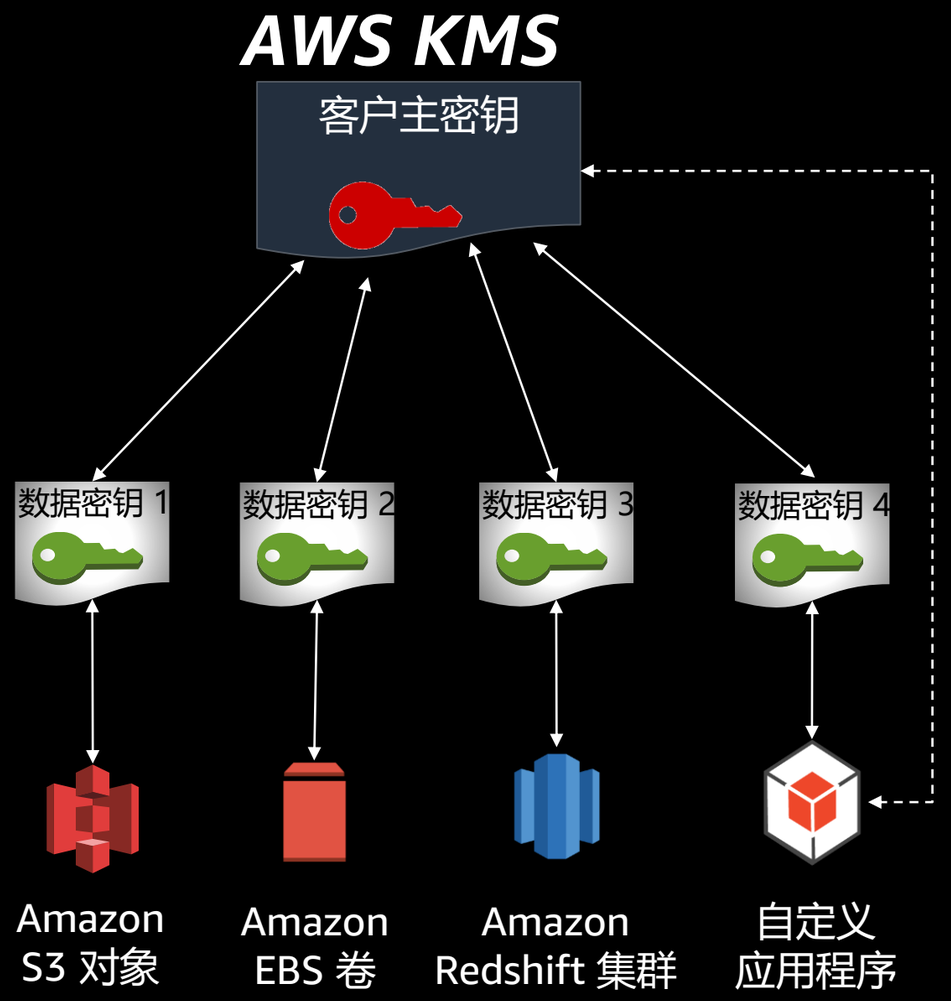
数据保护

aws INNOVATE
ONLINE CONFERENCE

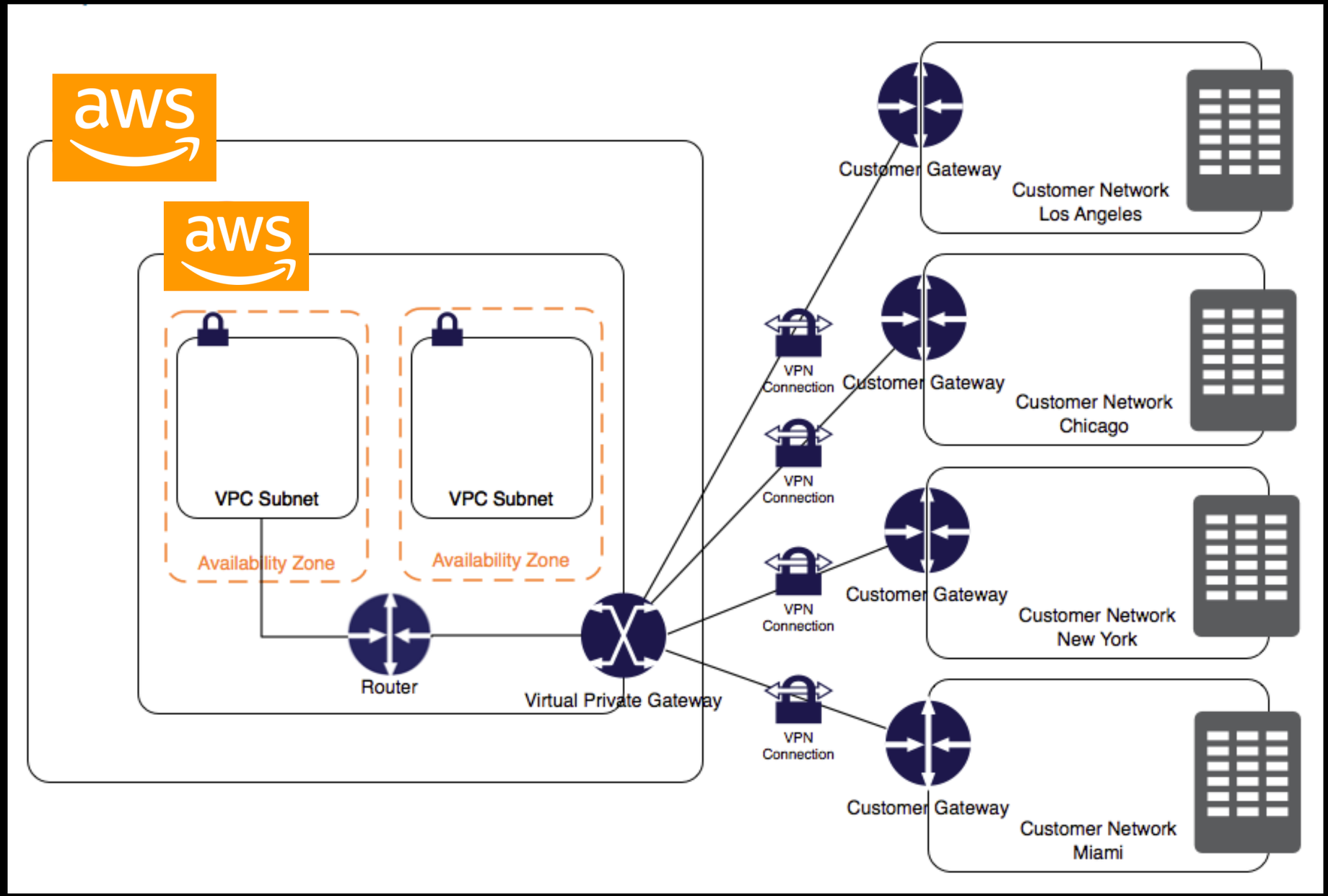
存储中的数据加密：AWS KMS 密钥层次结构

使用信封加密的多层密钥层次结构

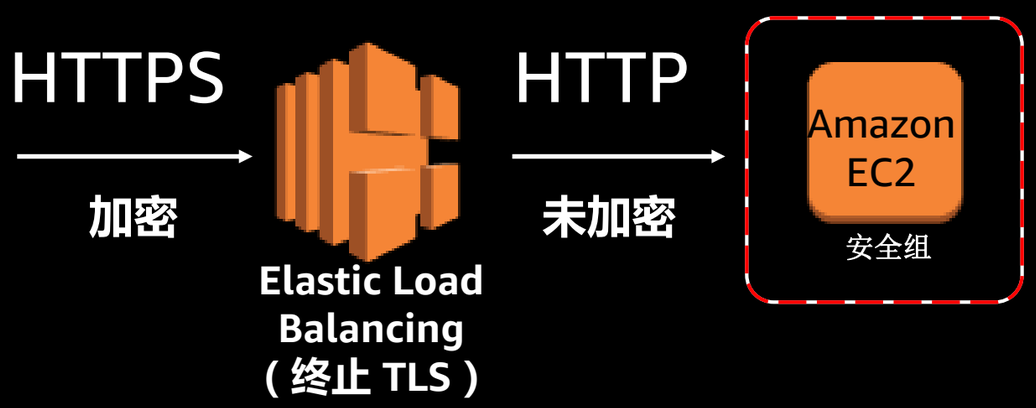
- 通过独一无二的数据密钥对单个客户数据进行加密
- 通过 AWS KMS 主密钥对数据密钥进行加密
- 通过区域主密钥对客户 AWS KMS 密钥进行加密

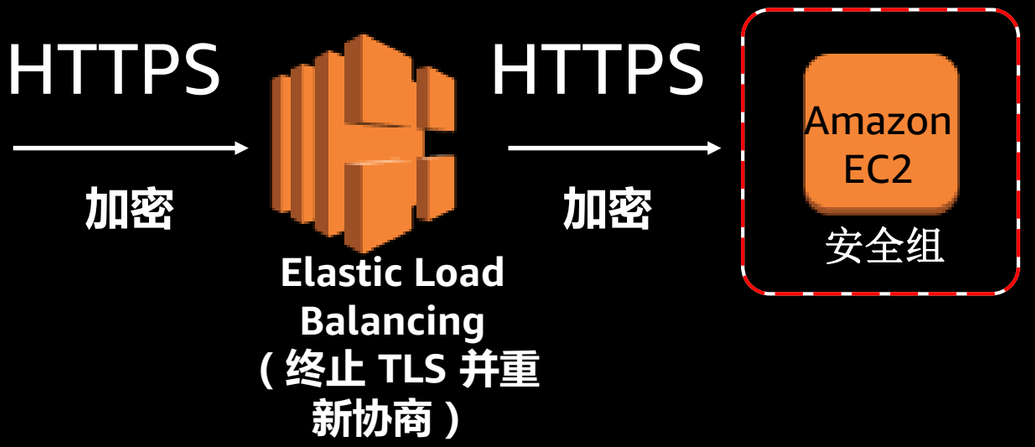


传输中的数据加密：VPN



传输中的数据加密：TLS 证书卸载方式





持续合规

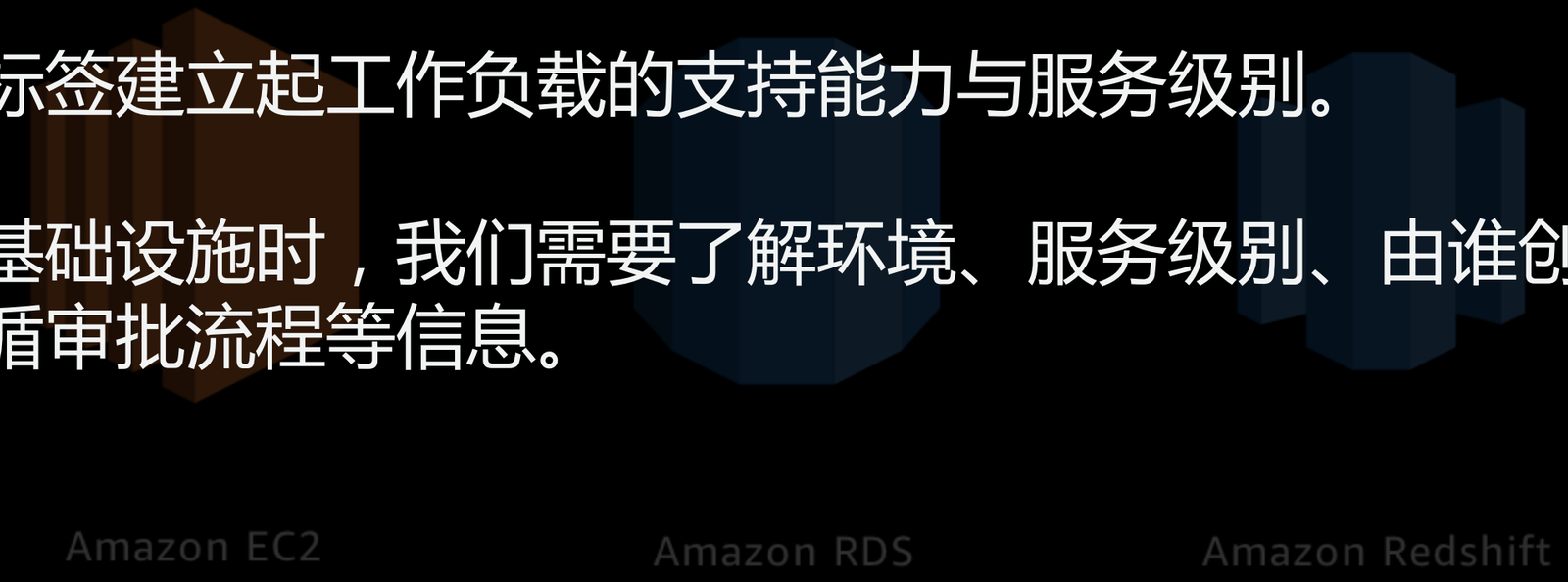
aws INNOVATE
ONLINE CONFERENCE

业务，是否需要交付团队更敏捷、更自主？

有可能出现哪些问题？

我们基于标签建立起工作负载的支持能力与服务级别。

当创建新基础设施时，我们需要了解环境、服务级别、由谁创建以及创建者是否遵循审批流程等信息。



具体涉及以下资源.....

Amazon EC2

Amazon RDS

Amazon Redshift

传统合规

- 传统合规方法
- 合规人员的技术水平
- 临时应对审计

AWS 上的云合规优势

- 实时且持续监控
- 合规态势展示
- 配置强制实施
- 提高可复用性
- 规范化与程序化管理

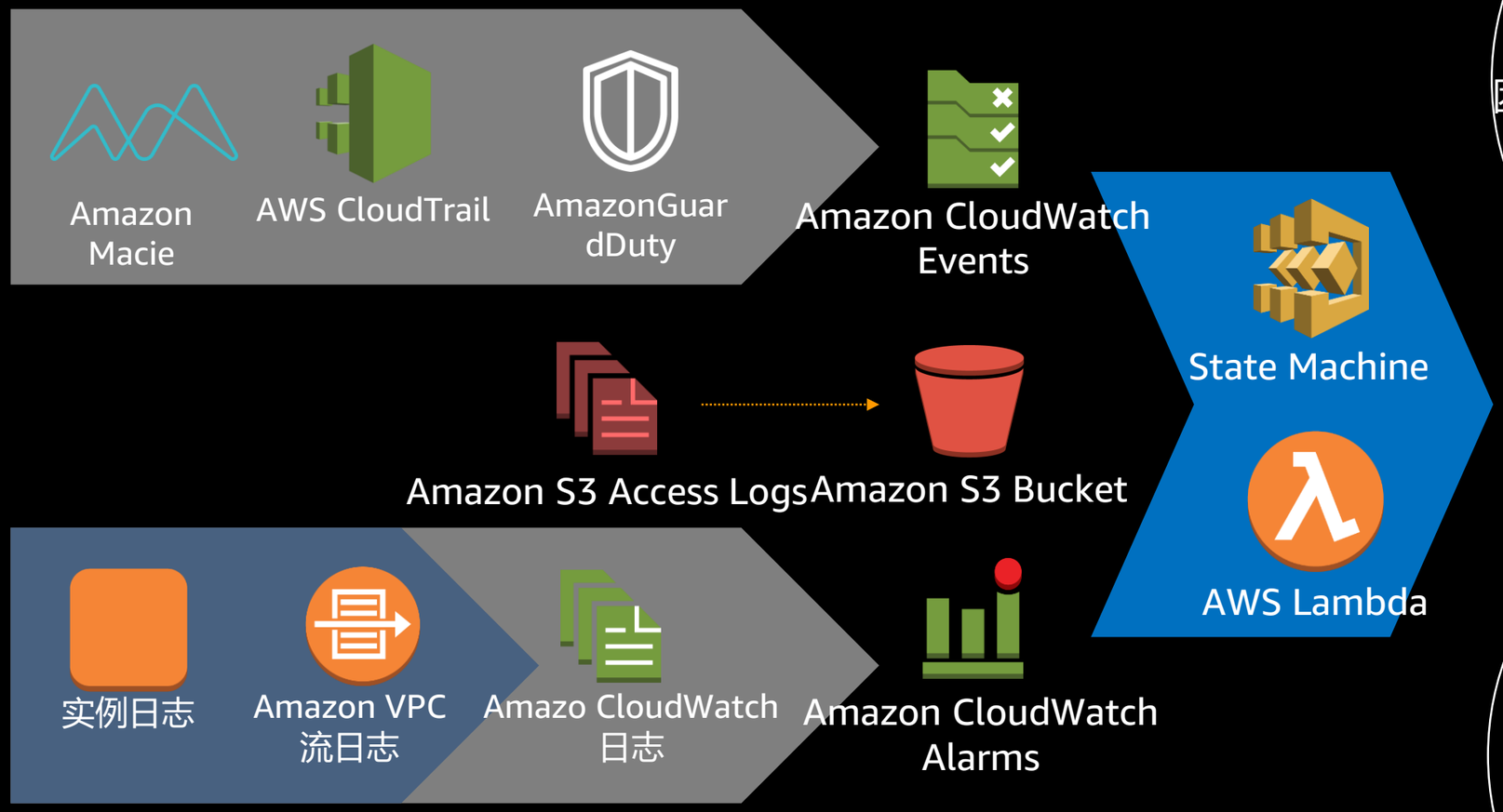
我们的任务

用 AWS Config 服务，创建规则以查看我们的特定配置，在配置不符合我们的安全策略时自动报警，同时也可以自动化进行强制修复。

事件响应

aws INNOVATE
ONLINE CONFERENCE

面向 AWS 的高层级事件响应



警报
修复
取证

检测
验证

持续自动化，直到达成一切目标

- 从单一工作流入手，最好选择简单场景，确保具有明确的是/否结果。
- 以事件检测为起点，自动化所有工作：

- 回滚至已知良好状态
- 获取关于该事件的全部日志
- 从中选择必要的数值、相关人员、事件内容、发生于何时、发生于何处
- 将数值与人员及资产关联起来
- 分析数据、评估风险并分配优先级
- 引入所有者并进行事件升级
- 随时报告给任何合适的相关人

AWS CloudTrail 关闭事件响应手册

1. 重新启动 AWS CloudTrail
2. 收集与 AWS CloudTrail 相关的事件数据
3. 从事件数据中提取主体 principal、日期、时间以及源IP等
4. 将主体 principal 与人员映射起来
5. 查找人员联系信息
6. 与其联系，提供指导以及相关支持
7. 在报告中生成事件摘要

注意：整个过程以自动化方式实现，因此不会影响我们的正常作息。

AWS CloudTrail 关闭事件响应手册

1. 重新启动 AWS CloudTrail

```
cloudtrail.start_logging(Name=trail_name)
```

AWS CloudTrail 关闭事件响应手册

2. 收集与 AWS CloudTrail 关闭相关的事件数据

```
{
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "cloudtrail.amazonaws.com"
    ],
    "eventName": [
      "StopLogging"
    ]
  }
}
```

```
{
  "account": "483366358098",
  "region": "us-west-2",
  "detail": {
    "eventVersion": "1.06",
    "eventID": "85ce2937-6984-4484-8629-13d15ed03071",
    "eventTime": "2018-11-20T23:47:08Z",
    "requestParameters": {
      "name": "sec327-demo-1-rCloudTrailTrail-12XXNQSQJAHC"
    },
    "eventType": "AwsApiCall",
    "responseElements": "",
    "awsRegion": "us-west-2",
    "eventName": "StopLogging",
    "readOnly": "false",
    "userIdentity": {
      "principalId": "AROAIRT6OZJ4JDSDZ3NTA:botocore-session-1542757567",
      "accessKeyId": "XXXXXXXXXXXXXXXXXX",
      "sessionContext": {
        "sessionIssuer": {
          ...
```

AWS CloudTrail 关闭事件响应手册

3. 从事件数据中提取主体、日期、时间以及源 IP 等

{ $.eventName = "StopLogging"

AWS CloudTrail 关闭事件响应手册

4. 将主体与人员映射起来

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
"arn:aws:iam::483366358098:role/NonProdAdmin" }
```

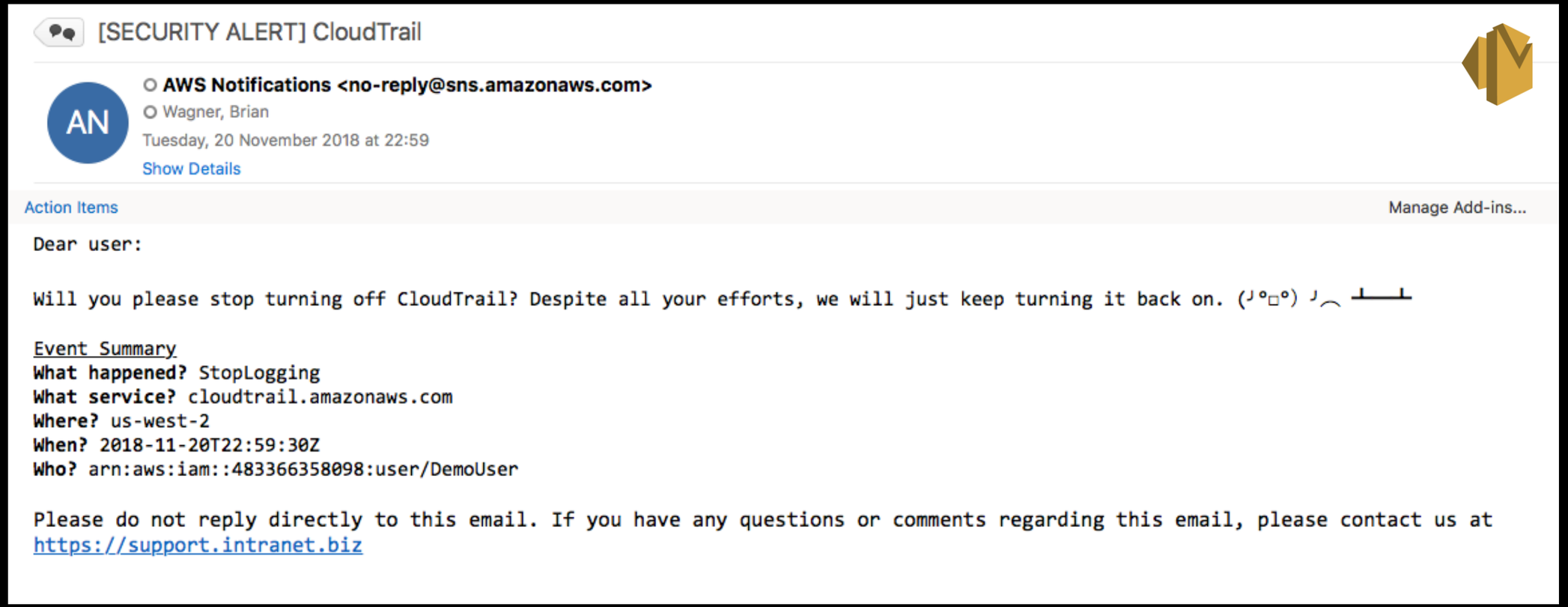
AWS CloudTrail 关闭事件响应手册

5. 查找人员联系信息

```
(&(objectCategory=person)(objectC
lass=user)
(cn=Brian*))
```

AWS CloudTrail 关闭事件响应手册

6. 与其联系，提供指导以及相关支持


[SECURITY ALERT] CloudTrail

AN

AWS Notifications <no-reply@sns.amazonaws.com>

Wagner, Brian

Tuesday, 20 November 2018 at 22:59

Show Details

Action Items Manage Add-ins...

Dear user:

Will you please stop turning off CloudTrail? Despite all your efforts, we will just keep turning it back on. (ノ°□°）ノ ┻━┻

Event Summary
What happened? StopLogging
What service? cloudtrail.amazonaws.com
Where? us-west-2
When? 2018-11-20T22:59:30Z
Who? arn:aws:iam::483366358098:user/DemoUser

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://support.intranet.biz

AWS CloudTrail 关闭事件响应手册

7. 在报告中生成事件摘要

EVENT: StopLogging

AN

AWS Notifications <no-reply@sns.amazonaws.com>
Wagner, Brian
Tuesday, 20 November 2018 at 22:59
Show Details

Action Items

```
What happened? StopLogging
What service? cloudtrail.amazonaws.com
Where? us-west-2
When? 2018-11-20T22:59:30Z
Who? {
  "principalId": "AROAIRT6OZJ4JDSDZ3NTA:botocore-session-1542754709",
  "accessKeyId": "ASIAXBCXBJRJKAQZ7YOC",
  "sessionContext": {
    "sessionIssuer": {
      "userName": "NonProdAdmin",
      "type": "Role",
      "arn": "arn:aws:iam::483366358098:role/NonProdAdmin",
      "principalId": "AROAIRT6OZJ4JDSDZ3NTA",
      "accountId": "483366358098"
    },
    "attributes": {
      "creationDate": "2018-11-20T22:59:30Z",
      "mfaAuthenticated": "false"
    }
  },
  "type": "AssumedRole",
  "arn": "arn:aws:sts::483366358098:assumed-role/NonProdAdmin/botocore-session-1542754709",
  "accountId": "483366358098"
}
```

AWS CloudTrail 关闭事件响应工作流自动化

1. Amazon CloudWatch Event
2. AWS Lambda
3. AWS CloudTrail
4. AWS CloudTrail
5. AWS Lambda
6. Amazon Simple Email Service (Amazon SES)
7. Amazon SES

感谢参加 AWS INNOVATE 2019 在线技术大会

我们希望您在这里找到感兴趣的内容！

也请帮助我们完成**投票打分**和**反馈问卷**。

欲获取关于 AWS 的更多信息和技术内容，可以通过以下方式找到我们：


微信公众号：AWSChina


新浪微博：https://www.weibo.com/amazonaws/


领英：https://www.linkedin.com/company/aws-china/


知乎：https://www.zhihu.com/org/aws-54/activities/


视频中心：http://aws.amazon.bokecc.com/


更多线上活动：https://aws.amazon.com/cn/about-aws/events/webinar/

aws INNOVATE
ONLINE CONFERENCE