亚马逊云科技

2021 Security Day

身份及权限 - 实现企业统一安全标准框架

身份与权限管理

在AWS服务、操作和资源中定义、实施和审核用户权限

AWS Identity and Access Management (IAM)
安全地控制对AWS服务和资源的访问

AWS Single Sign-On (SSO)
集中管理多个AWS账号和业务程序的SSO访问

AWS Directory Service
AWS云中的托管Microsoft Active Directory

Amazon Cognito
将用户注册、登录和访问控制添加到您的Web / 移动应用

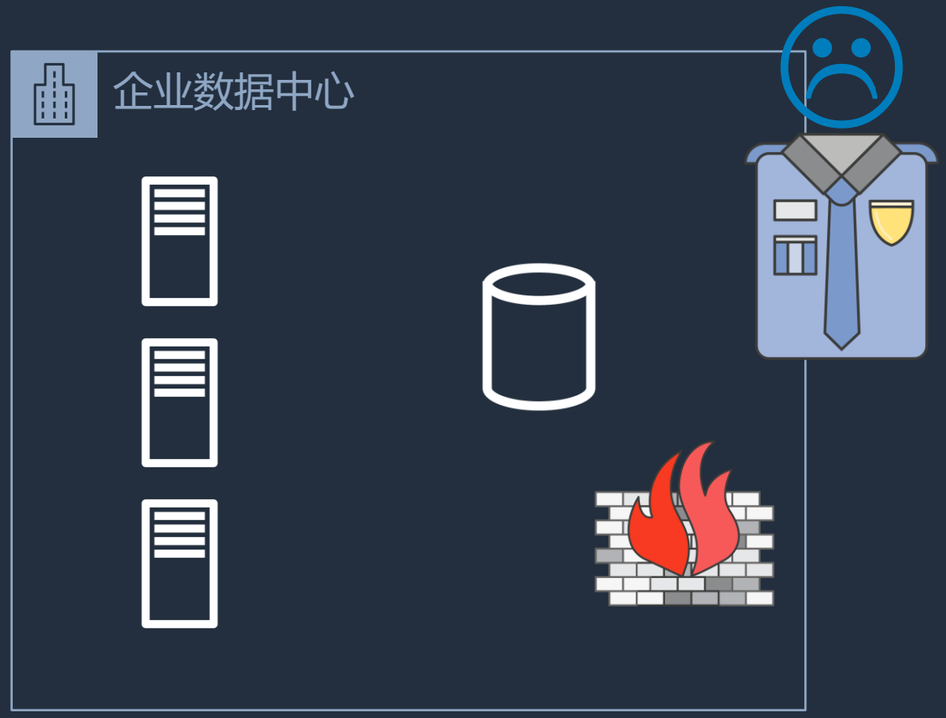
AWS Organizations
多个AWS账户的基于策略的管理

AWS Secrets Manager
在其生命周期内轻松轮换、管理和检索数据库凭证、API密钥和其他密码

AWS Resource Access Manager
简单安全地共享AWS资源

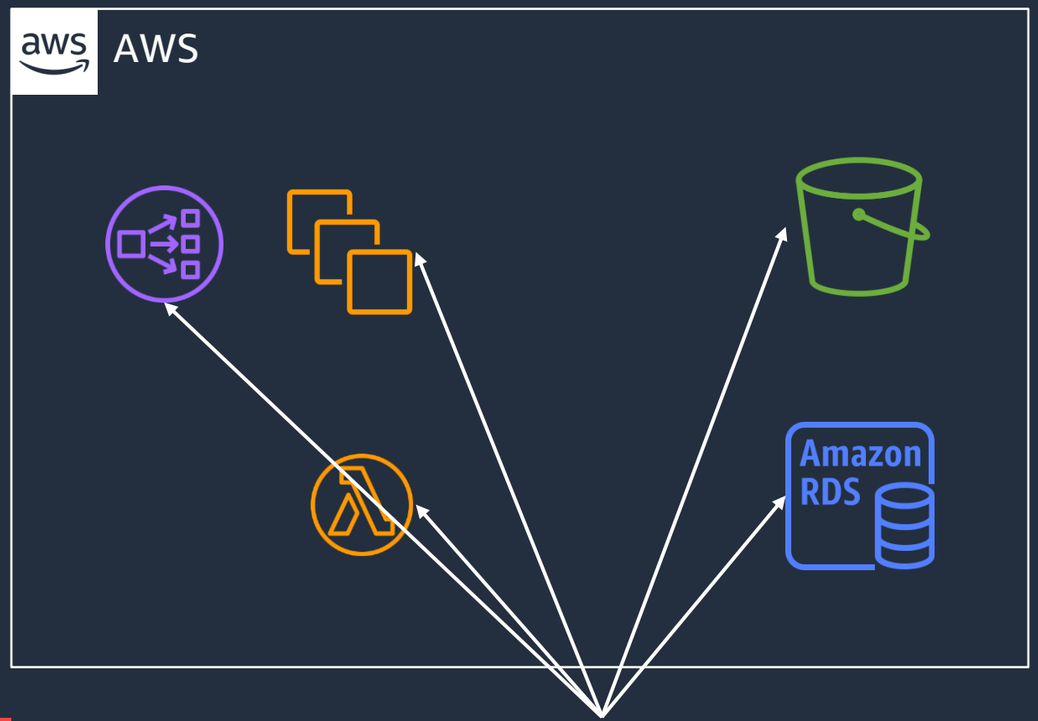
为什么学习AWS IAM

上云前的安全



在外围设备实现安全防护

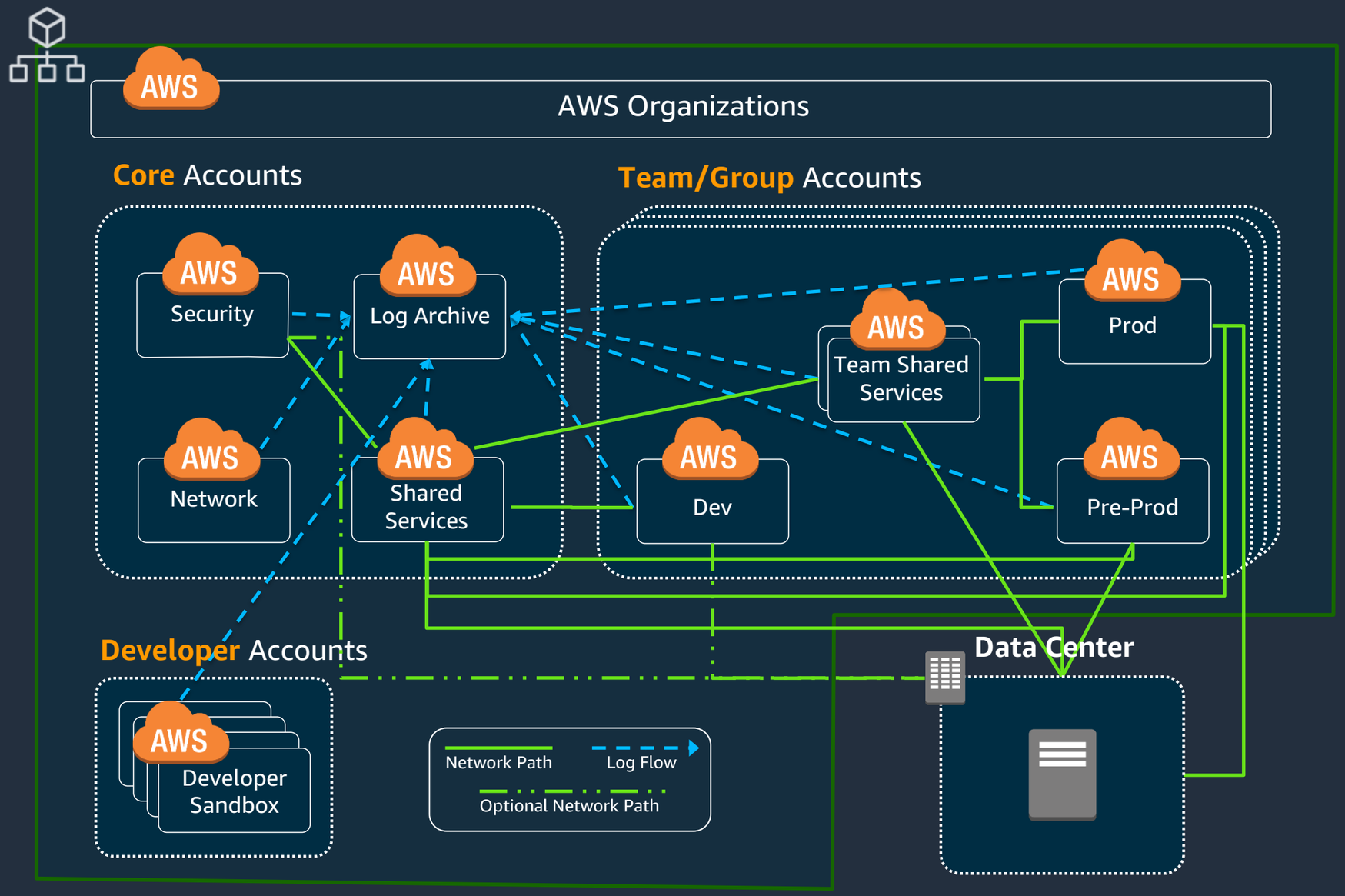
云上的安全



所有资源上的IAM鉴权：

应用程序的全面安全性

多账户管理策略



Orgs: 账号管理

Log Archive: 安全日志

Security: 安全工具, AWS Config rules

Shared services: 活动目录, 限制监控

Network: Direct Connect专线

Dev Sandbox: 实验环境

Dev: 开发环境

Pre-Prod: 预发布环境

Prod: 生产环境

Team SS: 团队共享服务, 数据湖

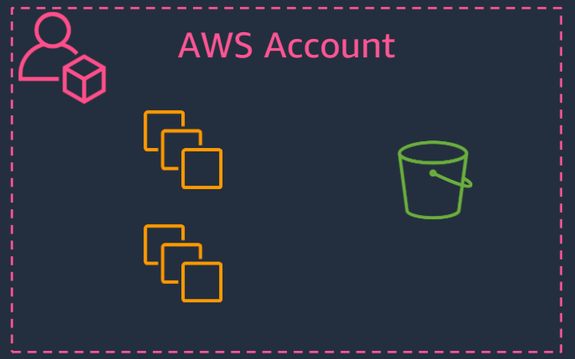
议程

- 如何给 “人” 和 “应用” 授权
- 如何阅读和编写IAM
- IAM实体的权限边界
- 多账户管理 - AWS Control Tower

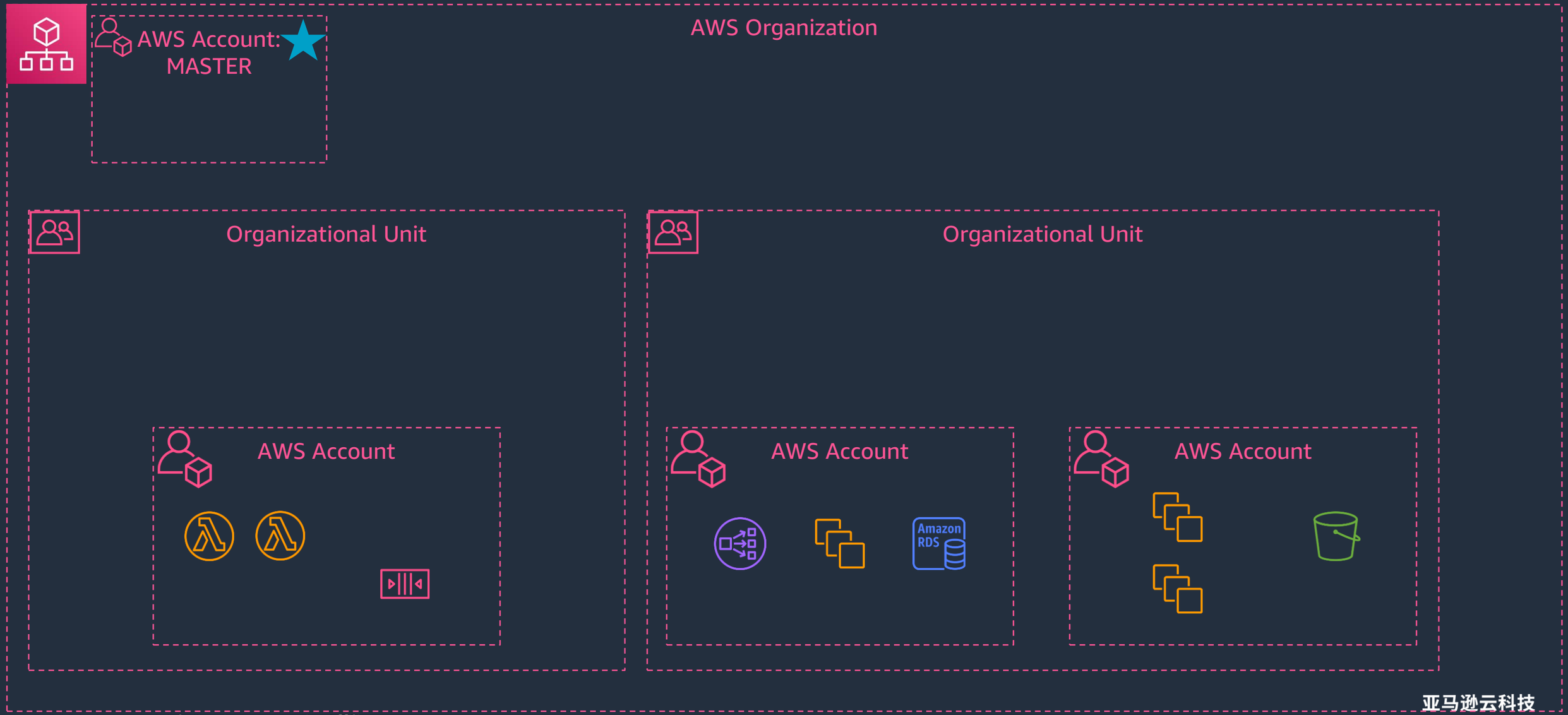
如何给“人”和“应用”授权

亚马逊云科技

AWS上的账户

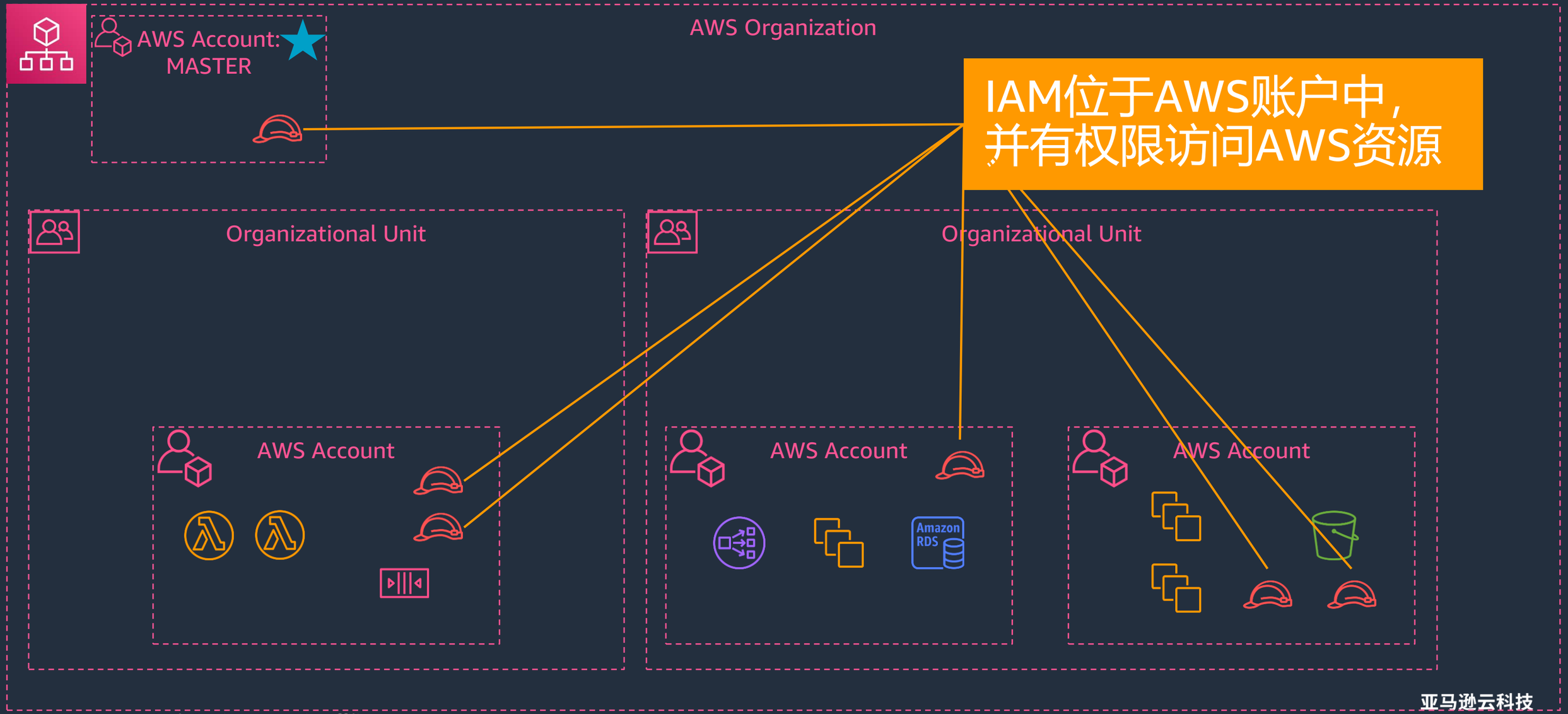


AWS上的账户

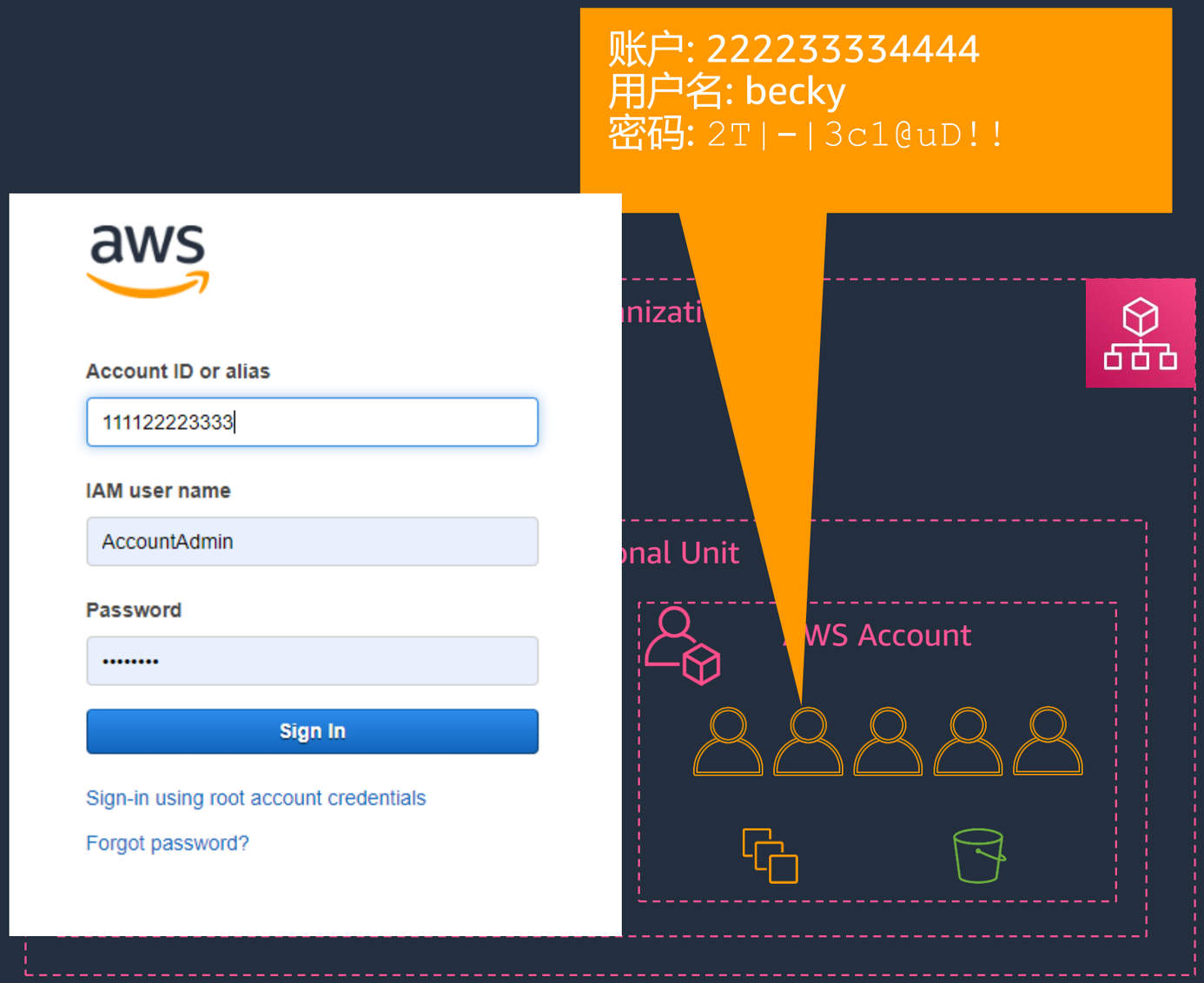


亚马逊云科技

AWS上的账户



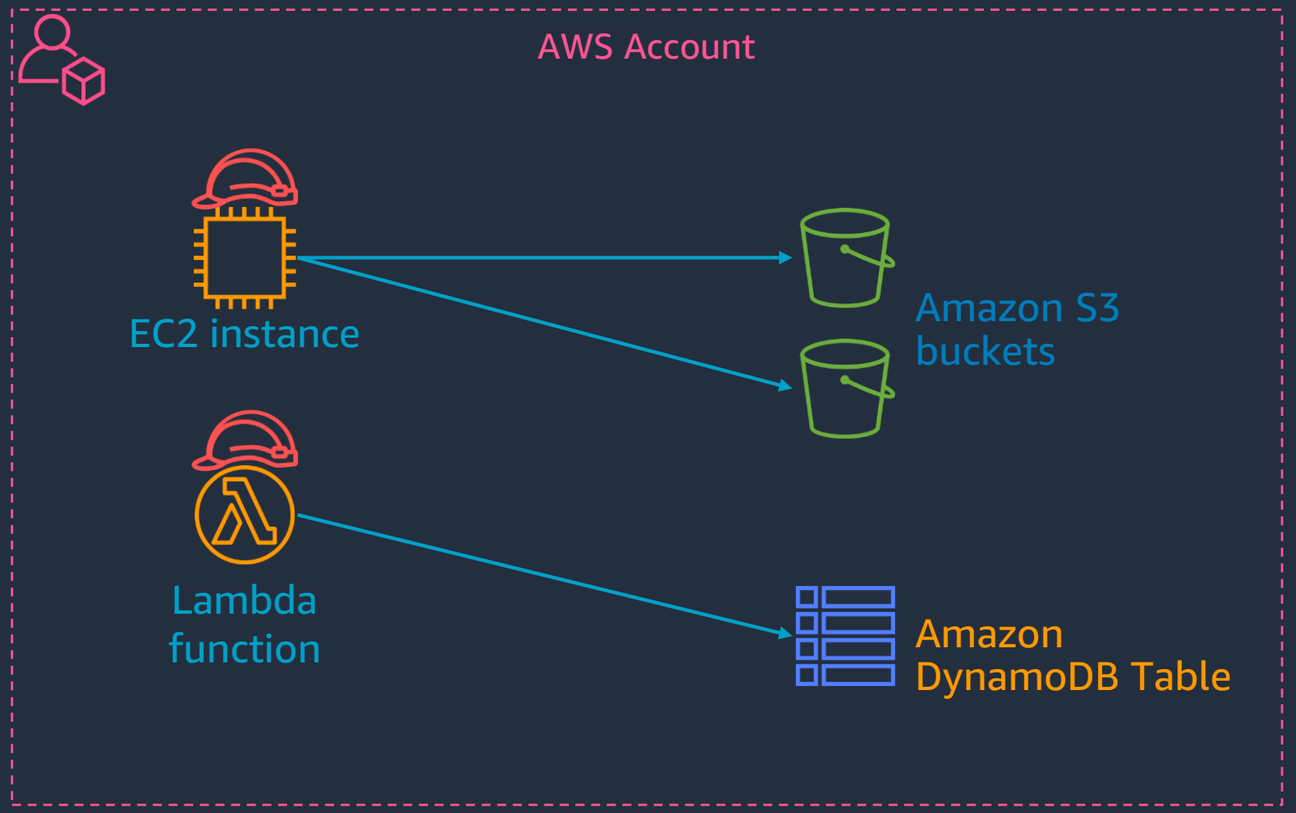
IAM 用户



在以下情况效果最佳:

- 用户数量相对较少 (上限为5,000)
- 一个或者相对较少数量的AWS账户
- 需要长期的凭证
- 没有目录服务，或者无法将目录服务连接到AWS
- 您的第一个AWS账户

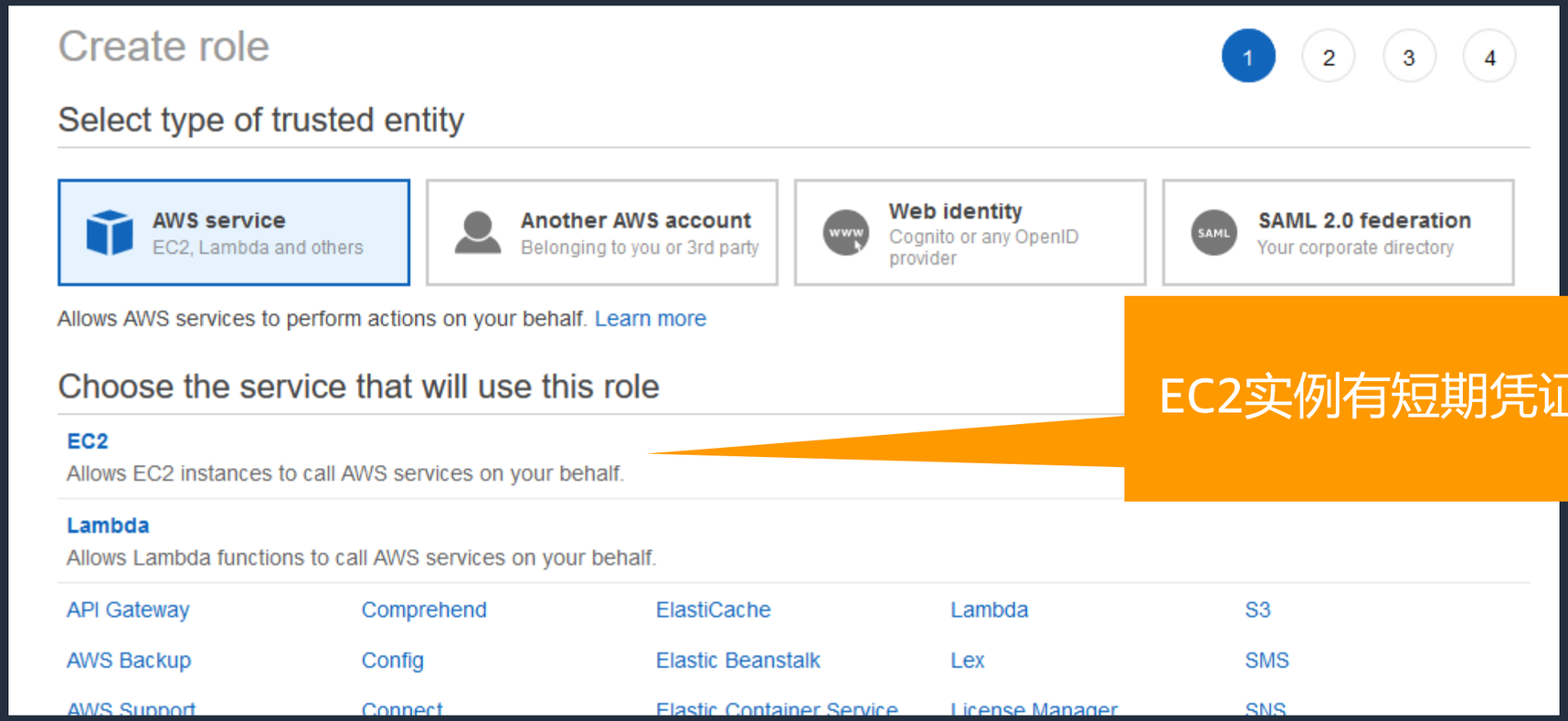
IAM 角色 （非 “人” 访问）



使用IAM角色从以下位置访问AWS资源：

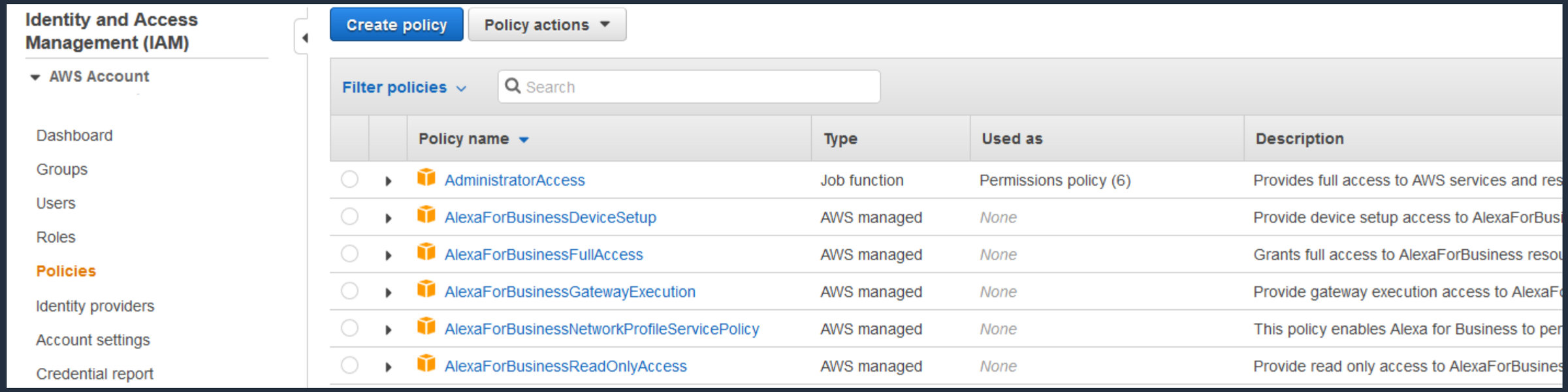
- 您的应用程序在AWS计算环境上运行，例如EC2实例、Lambda函数等。
- 允许AWS服务访问您的资源的权限

创建 IAM 角色



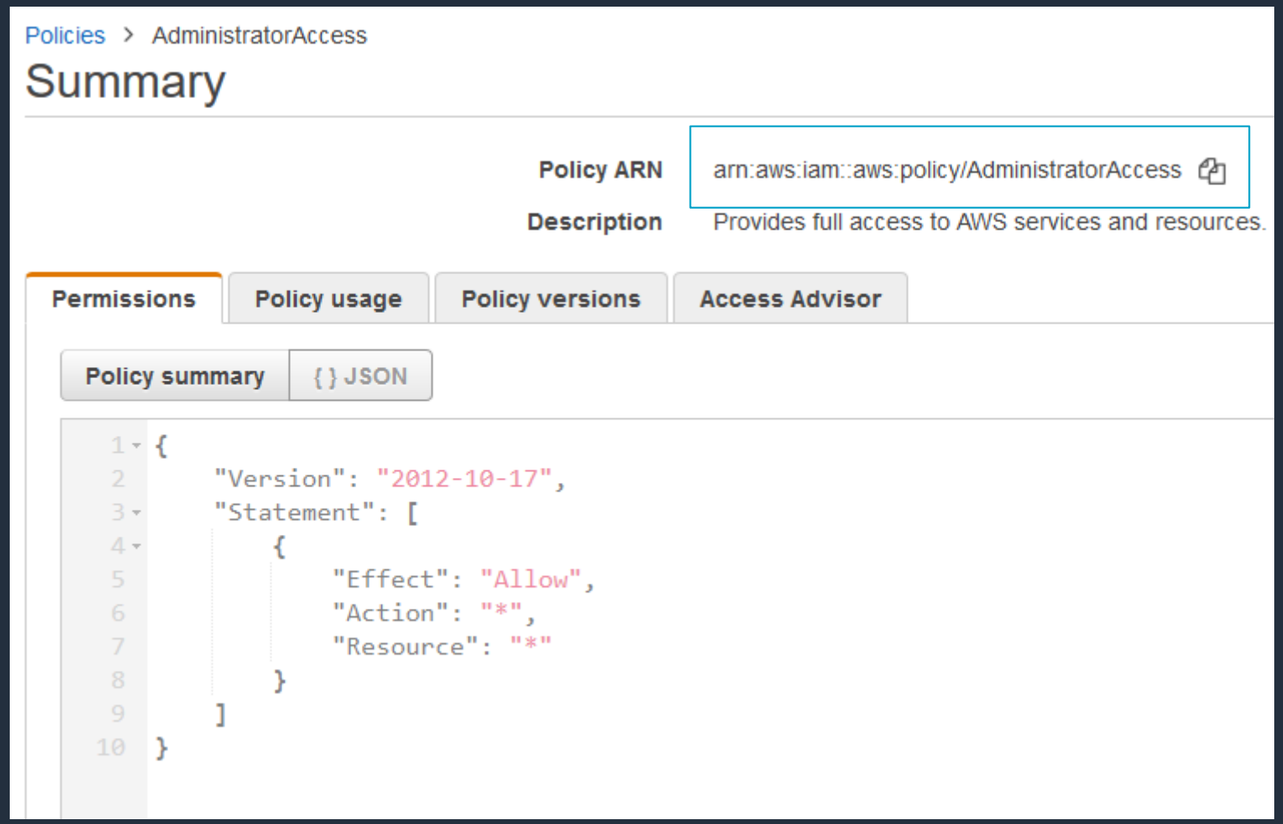
EC2实例有短期凭证访问AWS资源

分配 AWS 托管策略

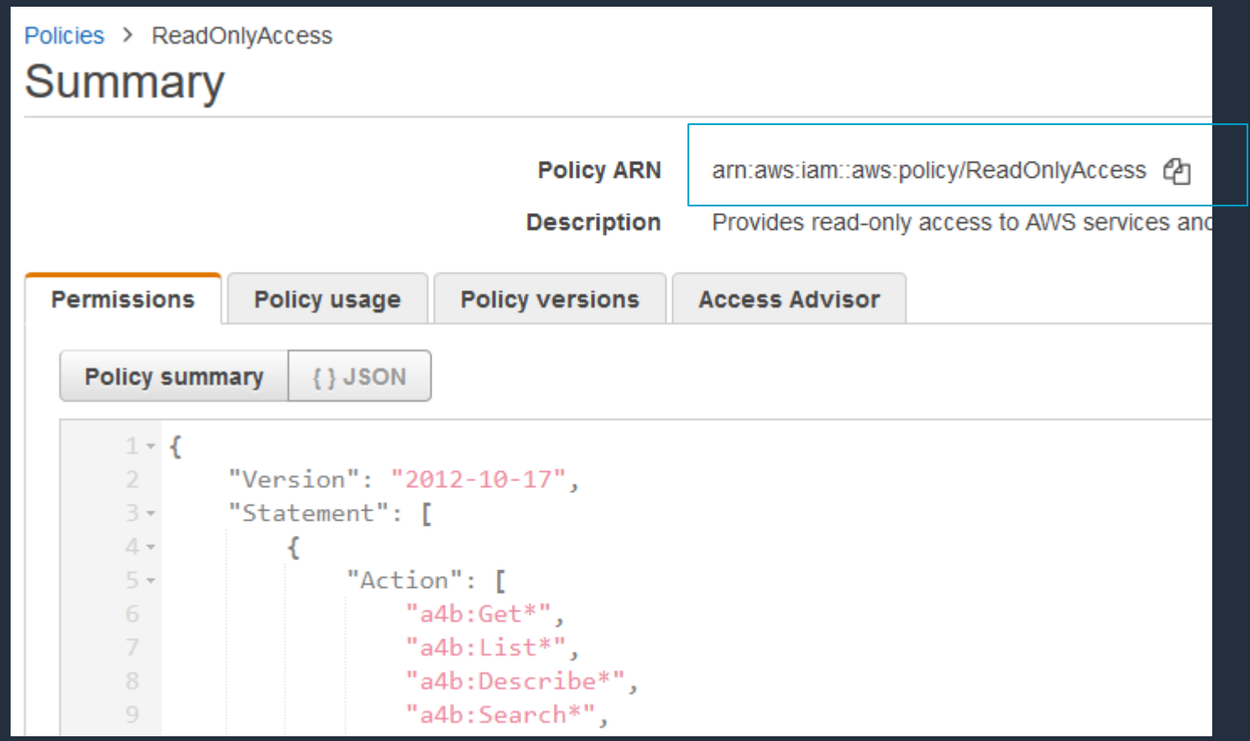


. . . 和其他更多AWS托管策略

举例: 管理员权限策略

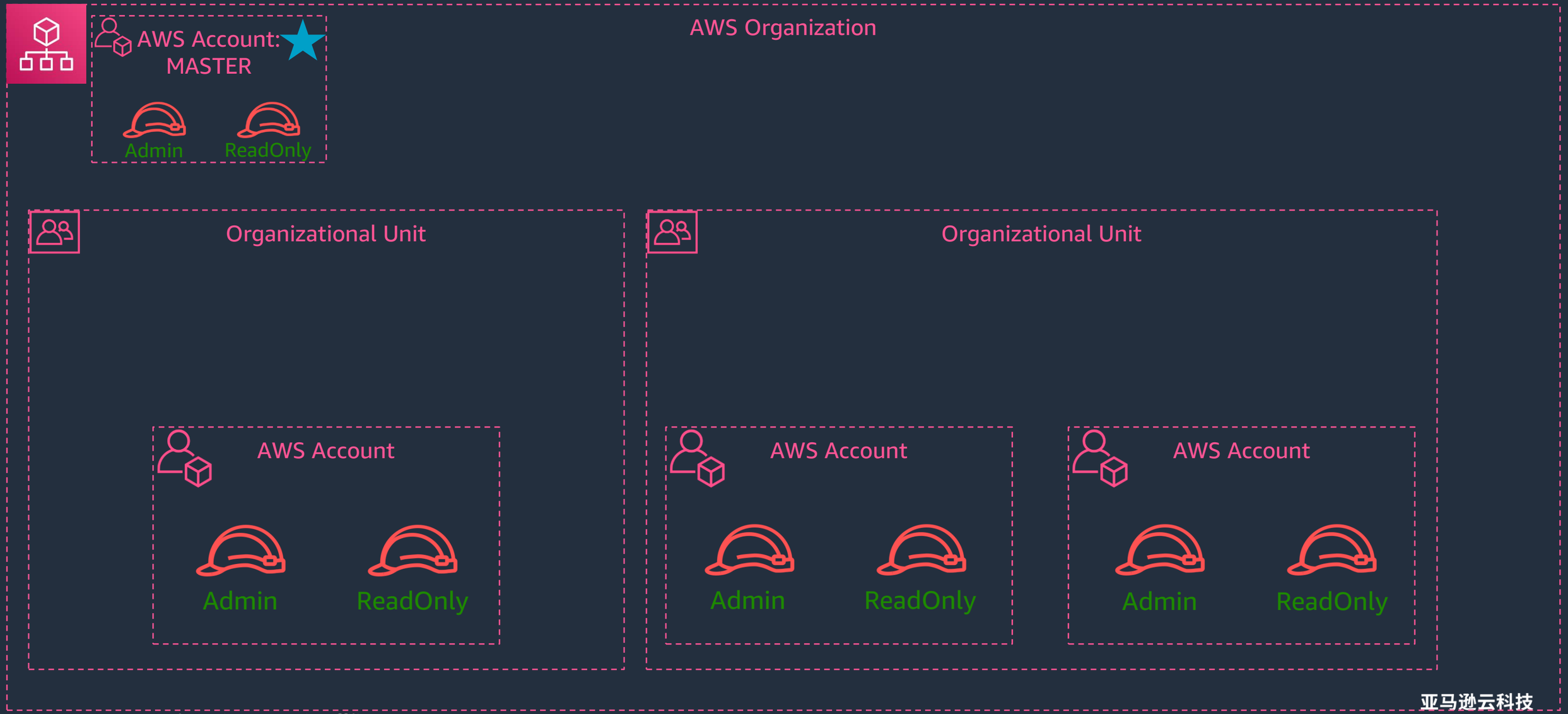


举例: 只读权限策略

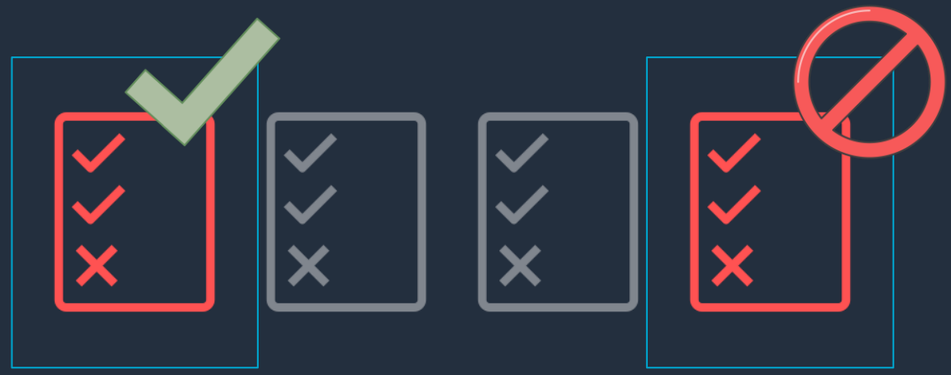


. . . 和其他 ReadOnly APIs

建议: 至少拥有如下两个IAM用户



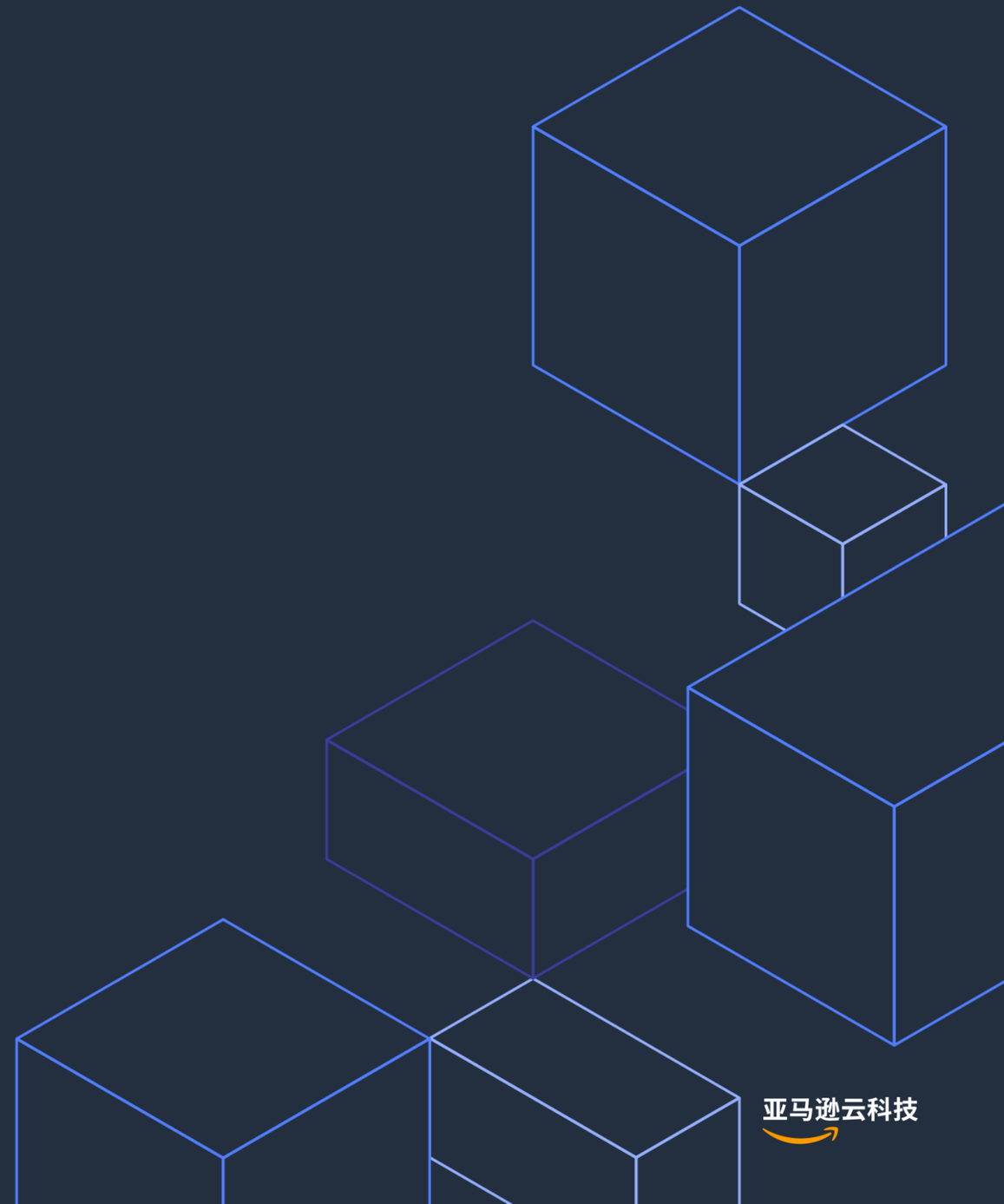
AWS 鉴权的工作方式



规则:

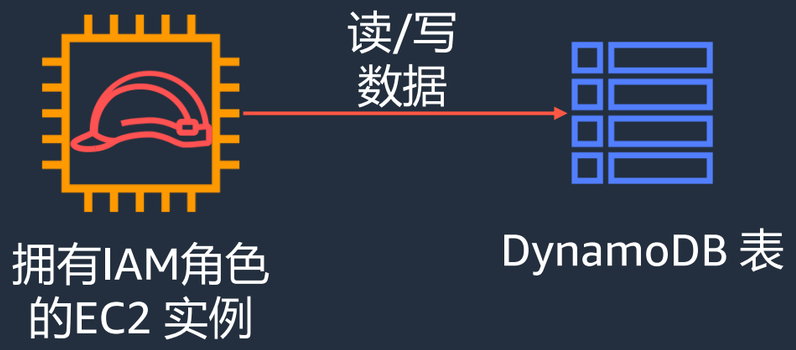
- 如果有任意拒绝策略 → AccessDenied
- 如果有允许 → Allow
- 否则 AccessDenied

如何阅读和编写IAM

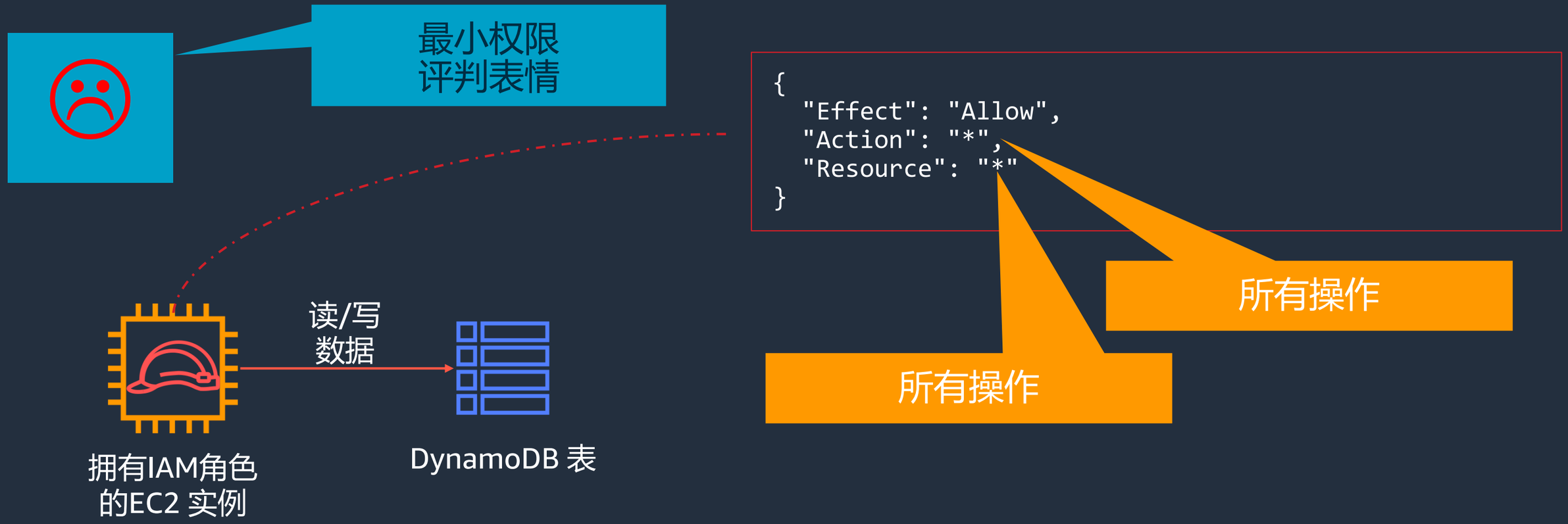


亚马逊云科技

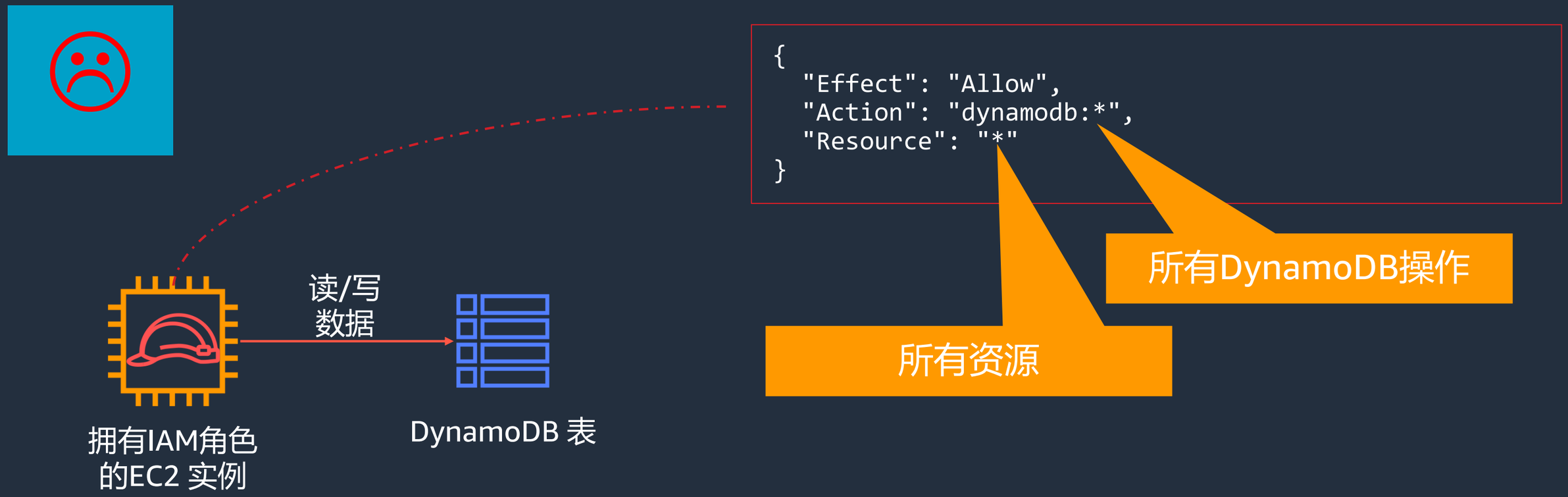
举例: 从DynamoDB读写数据



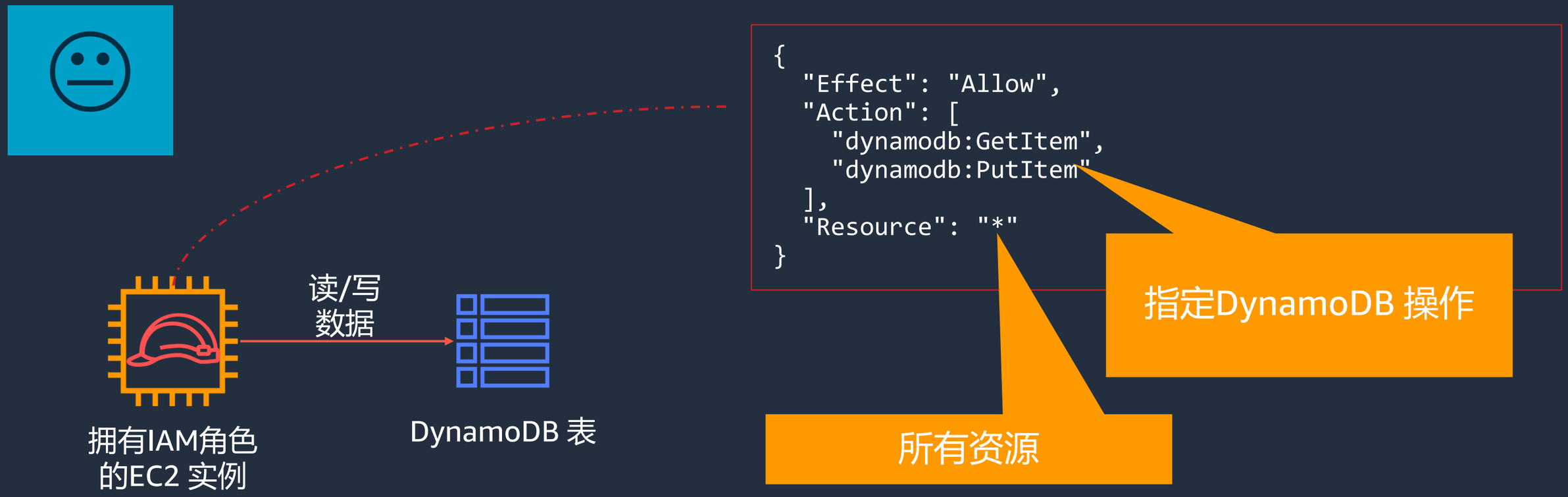
举例: 从DynamoDB读写数据



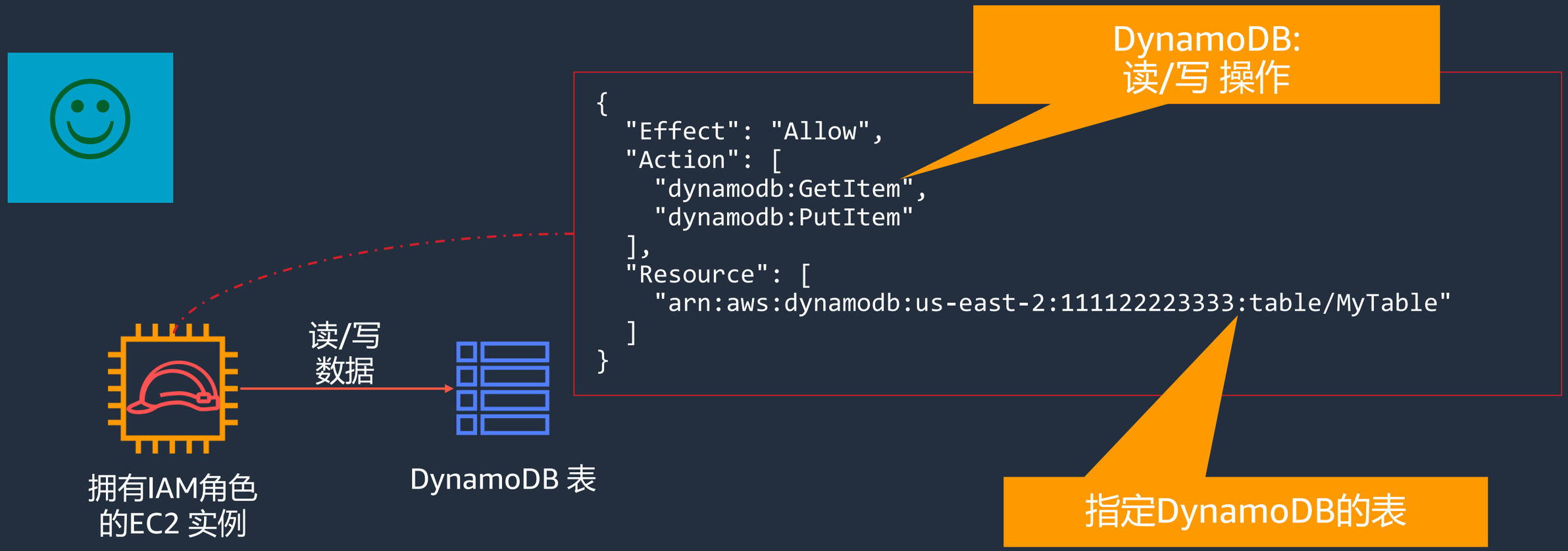
举例: 从DynamoDB读写数据



举例: 从DynamoDB读写数据

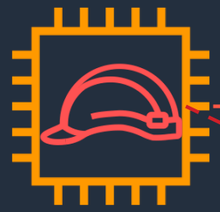


举例: 从DynamoDB读写数据



AWS鉴权的工作方式

```
dynamodb.putItem({
  TableName:"MyTable",
  Item: {
    "Id": {
      S: "a1b2c3d4"
  …
});
```



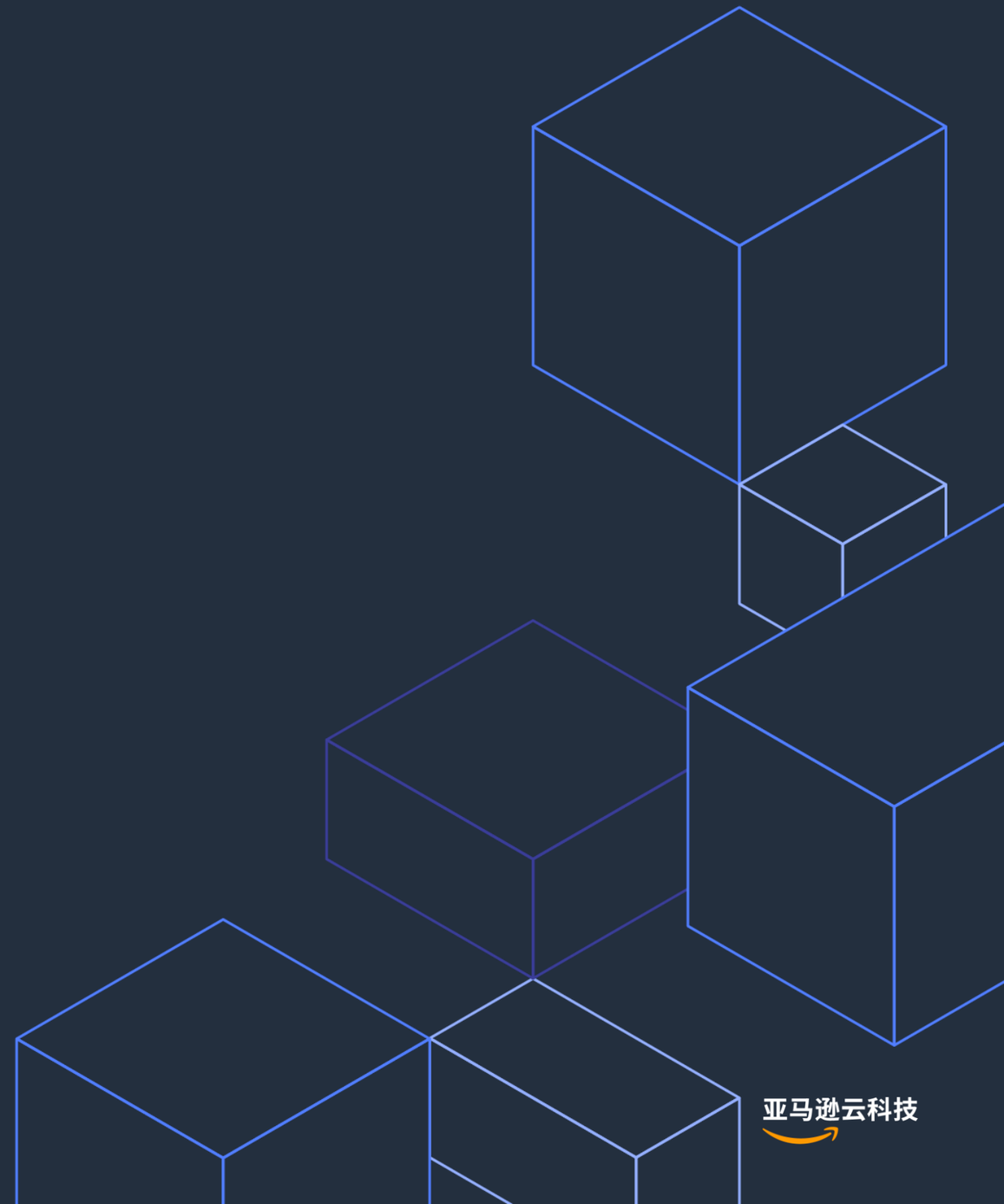
拥有IAM角色
的EC2 实例

DynamoDB表

“PutItem” 动作和“table” 资源与Allow语句匹配，因此请求被允许

```
{
  "Effect": "Allow",
  "Action": [
    "dynamodb:GetItem",
    "dynamodb:PutItem"
  ],
  "Resource": [
    "arn:aws:dynamodb:us-east-2:111122223333:table/MyTable"
  ]
}
```

IAM实体的权限边界



亚马逊云科技

问题：安全授权管理

- 授予创建用户和角色的权限时应谨慎
- 但是许多情况下，需要创建用户和角色
- 因此，我们需要一种安全地委派权限管理的方法

解决方案：权限边界

- 安全地委派权限管理
- 还允许同一账户中的多个团队进行权限管理

什么是权限边界

允许您委派权限来创建用户和角色，同时防止特权升级或不必要的广泛权限。

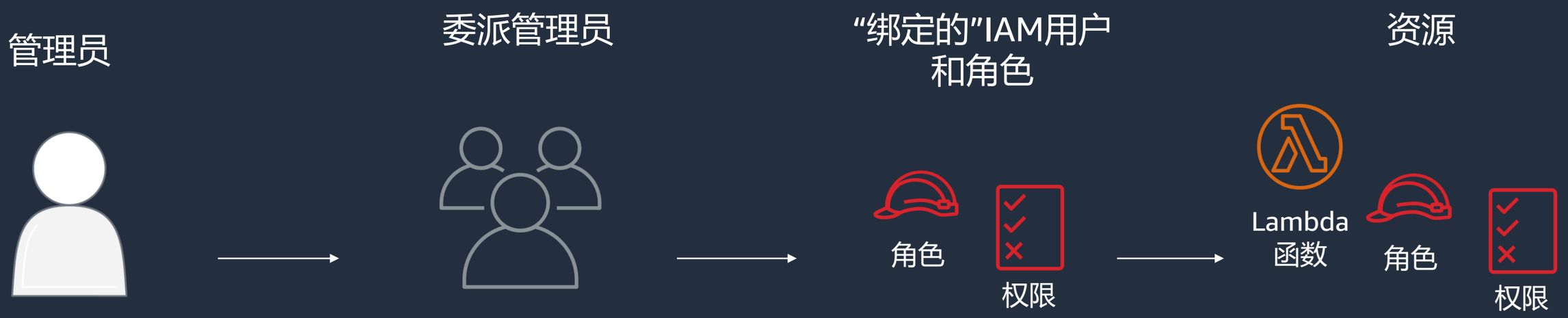
权限边界控制由委派管理员创建的用户或角色的最大权限。

使用权限边界之前


```
"Effect": "Allow",
"Action": ["iam:CreateRole"],
"Resource": ["*"]
```

```
"Effect": "Allow",
"Action": [“s3:*"],
"Resource": ["*"]
```

使用权限边界




```
"Effect": "Allow",
"Action": ["iam:CreateRole"],
"Resource": ["arn:aws:iam::ACCOUNT_ID:role/path/*"],
"Condition": {"StringEquals":
      {"iam:PermissionsBoundary":
      "arn:aws:iam::ACCOUNT_ID:policy/boundary"
      }
}
```

```
"Effect": "Allow",
"Action": [“s3:*"],
"Resource": ["*"]
```

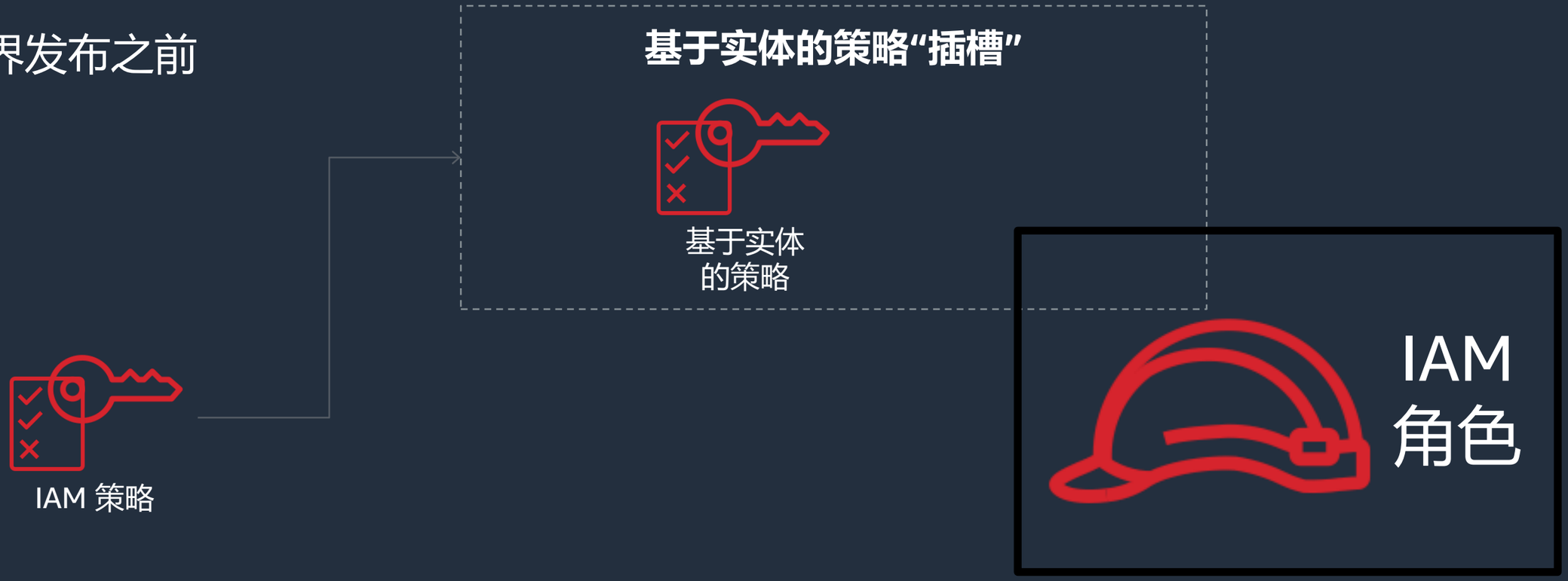
基于实体的权限“插槽”

```
"Effect": "Allow",
"Action": [“s3:GetObject"],
"Resource": ["arn:aws:s3:::app1/*"]
```

权限边界“插槽”

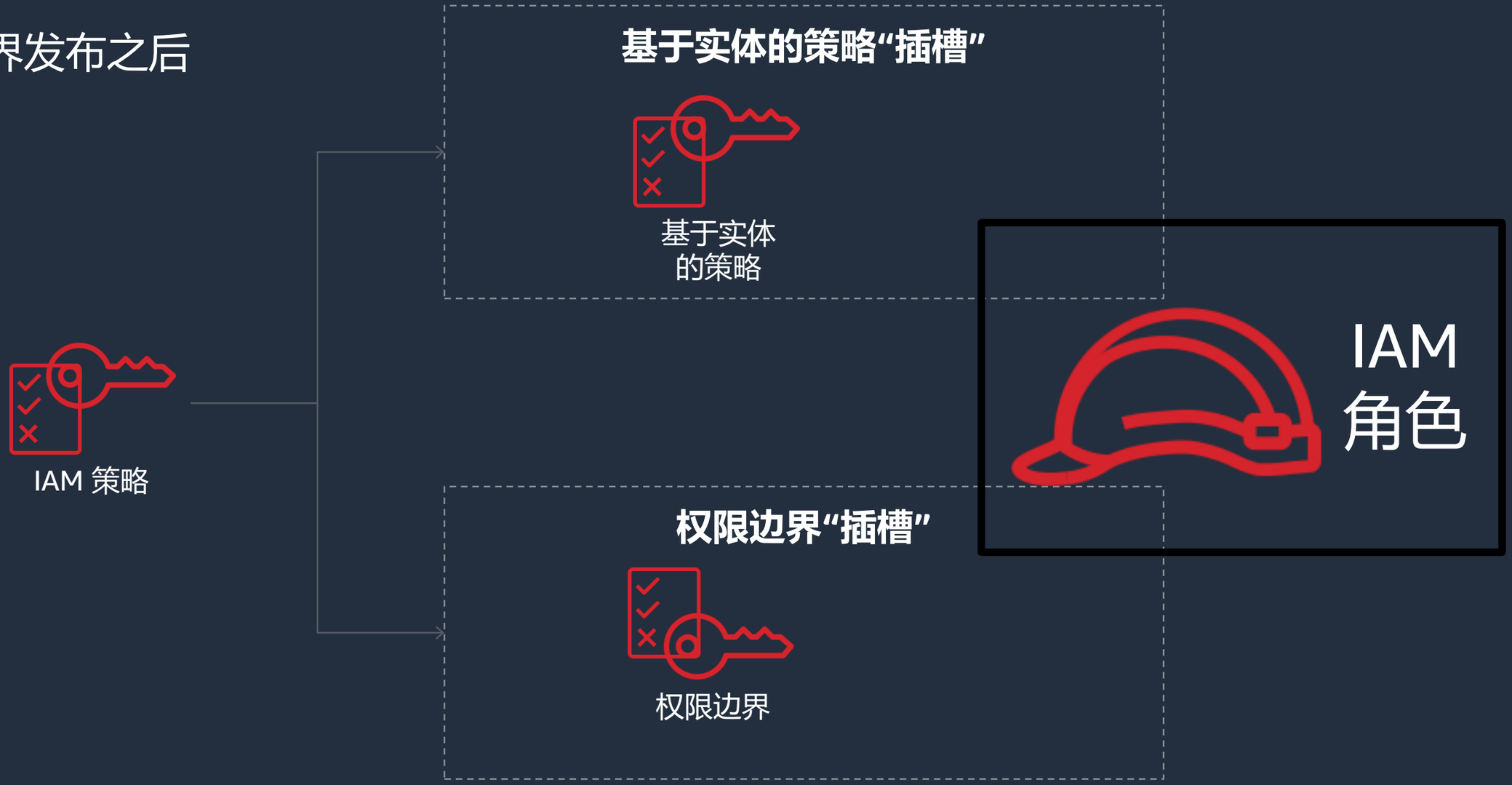
权限策略 “插槽”

权限边界发布之前

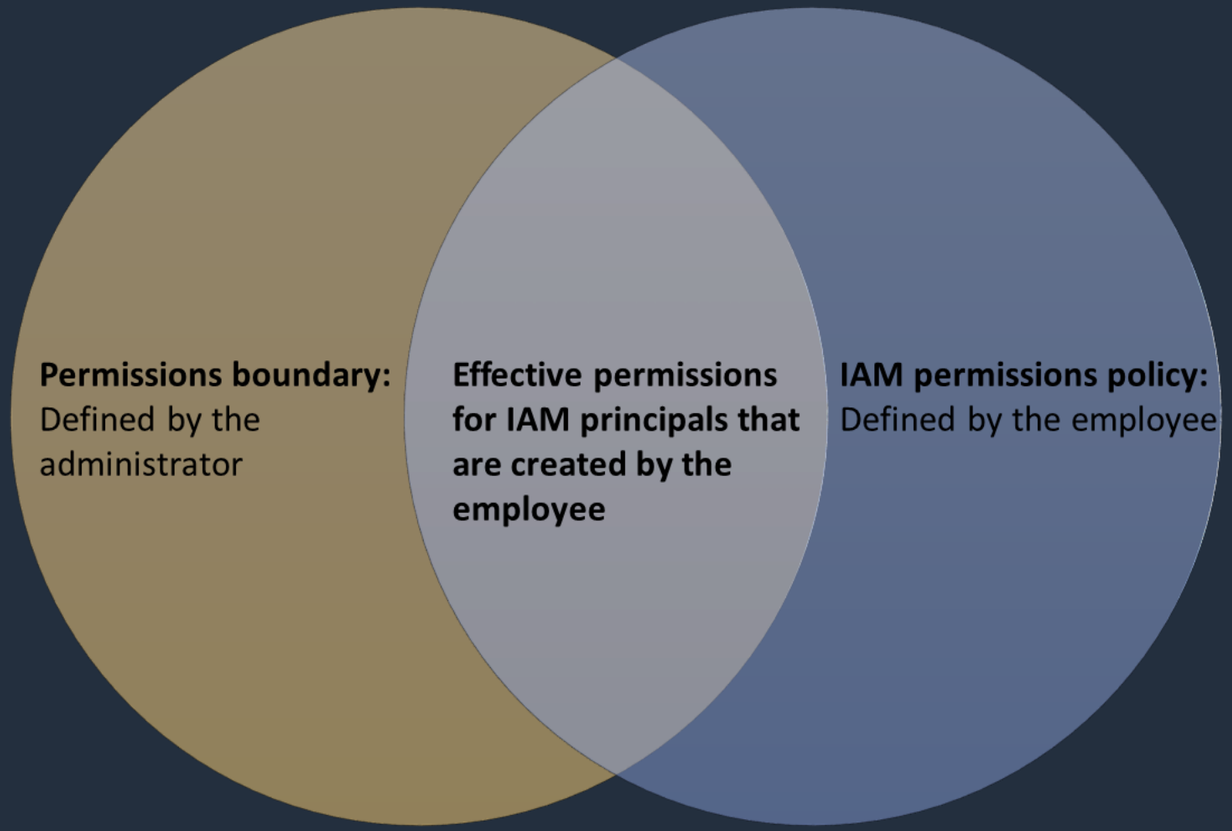


权限策略 “插槽”

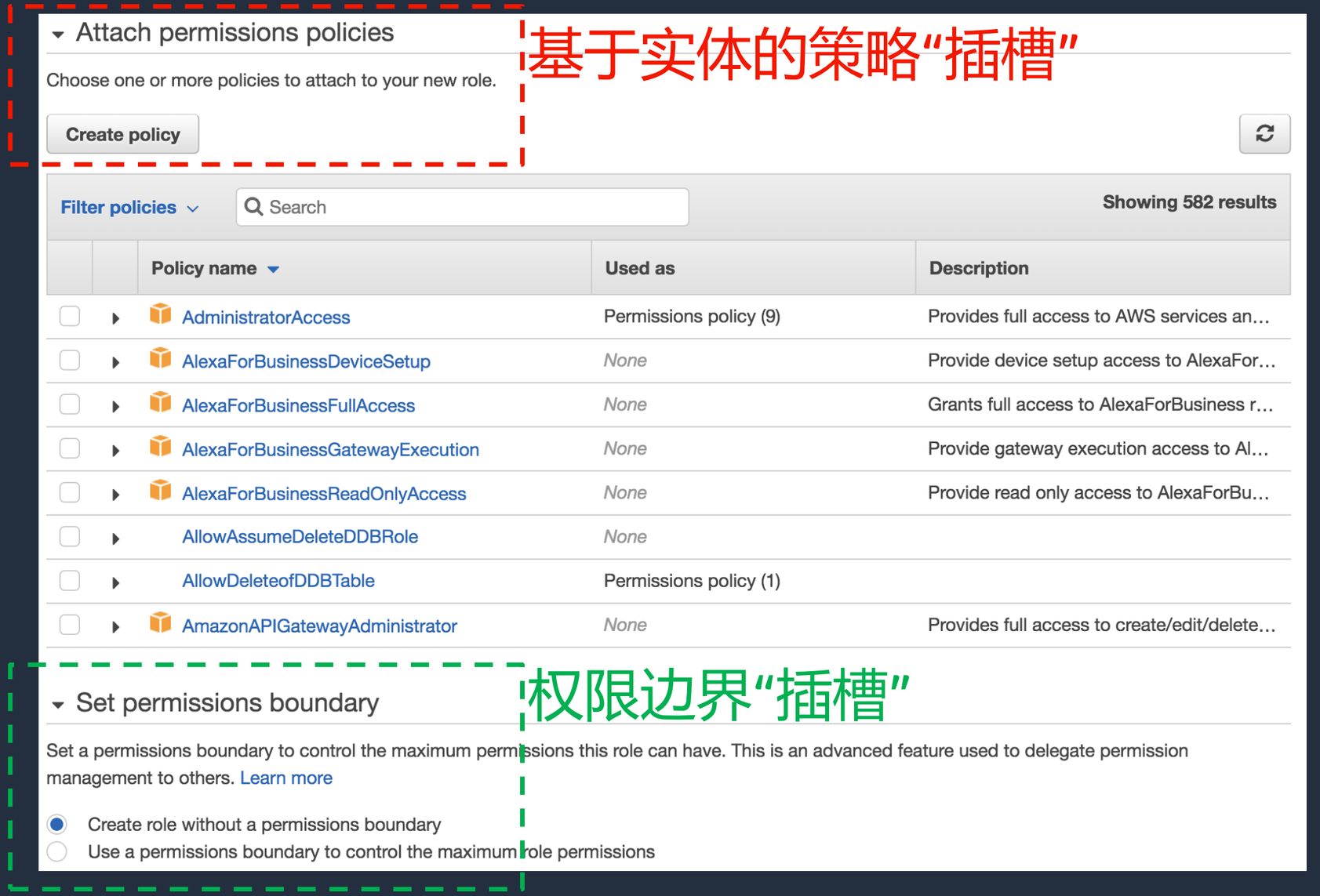
权限边界发布之后



权限策略 “插槽”



权限策略 “插槽”



支持的条件

- AttachRolePolicy
- AttachUserPolicy
- CreateRole
- CreateUser
- DeleteRolePermissionsBoundary
- DeleteUserPermissionsBoundary
- DeleteRolePolicy
- DeleteUserPolicy
- DetachRolePolicy
- DetachUserPolicy
- PutRolePermissionsBoundary
- PutUserPermissionsBoundary
- PutRolePolicy
- PutUserPolicy

权限边界工作流

管理员

创建委派管理员

要求：由委派管理员创建的用户和角色必须具有权限边界

委派管理员

创建“绑定的”用户和角色

能力：可以创建具有权限边界的用户和角色

“绑定的”IAM用户和角色

通过权限边界限制的用户和角色

结果：权限边界限制了用户和角色的权限

限制的资源

限制资源的权限

附加到资源（例如Lambda函数）的角色的权限受权限边界限制

多账户管理 – AWS Control Tower

亚马逊云科技

一个账户是不足够的...

多团队

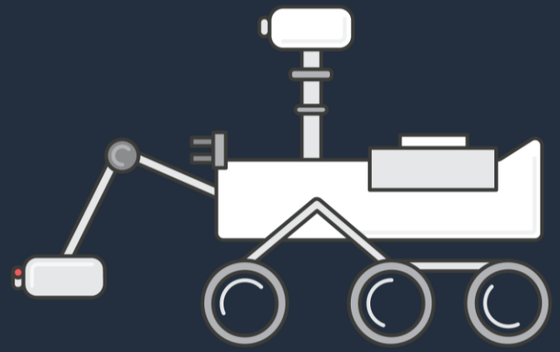
计费

隔离

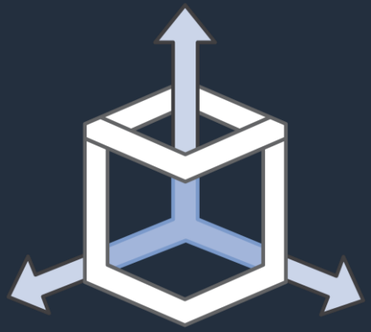
安全与合规控制

业务流程

目标

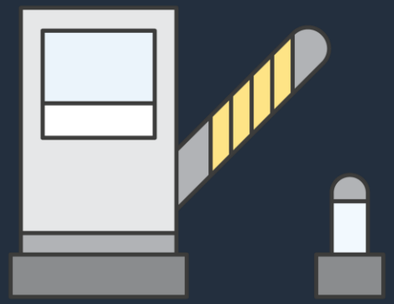


自动化



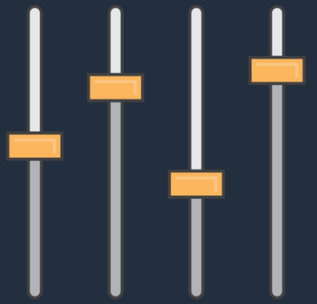
可扩展

自服务



护栏 **非** 障碍

可审计



灵活性

需要创建哪些账户?

组织账户

日志归档

安全审计

共享服务

网络

账单

沙箱环境

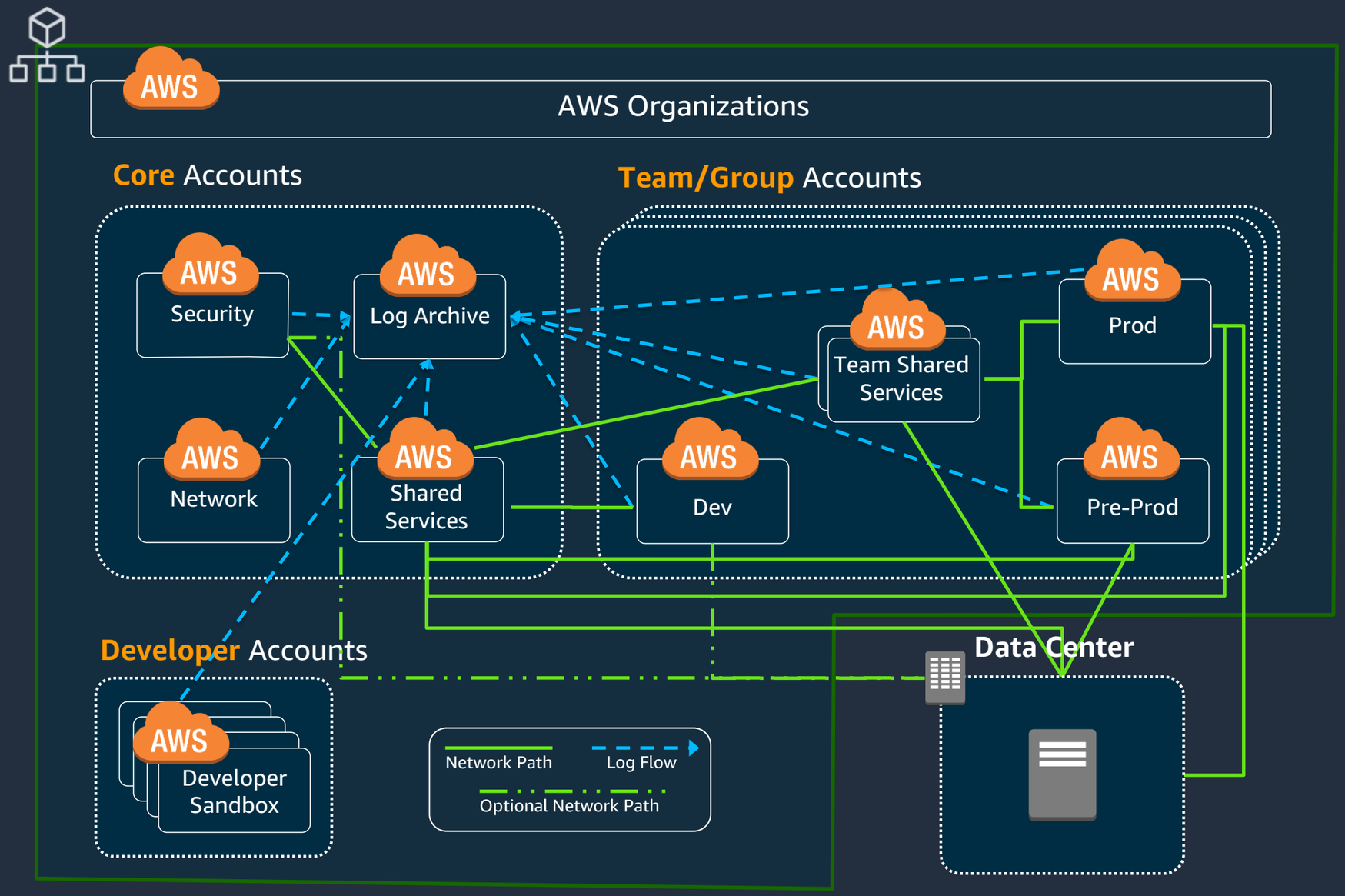
开发环境

预发布环境

生产环境

其他

多账户管理策略



Orgs: 账号管理

Log Archive: 安全日志

Security: 安全工具, AWS Config rules

Shared services: 活动目录, 限制监控

Network: Direct Connect专线

Dev Sandbox: 实验环境

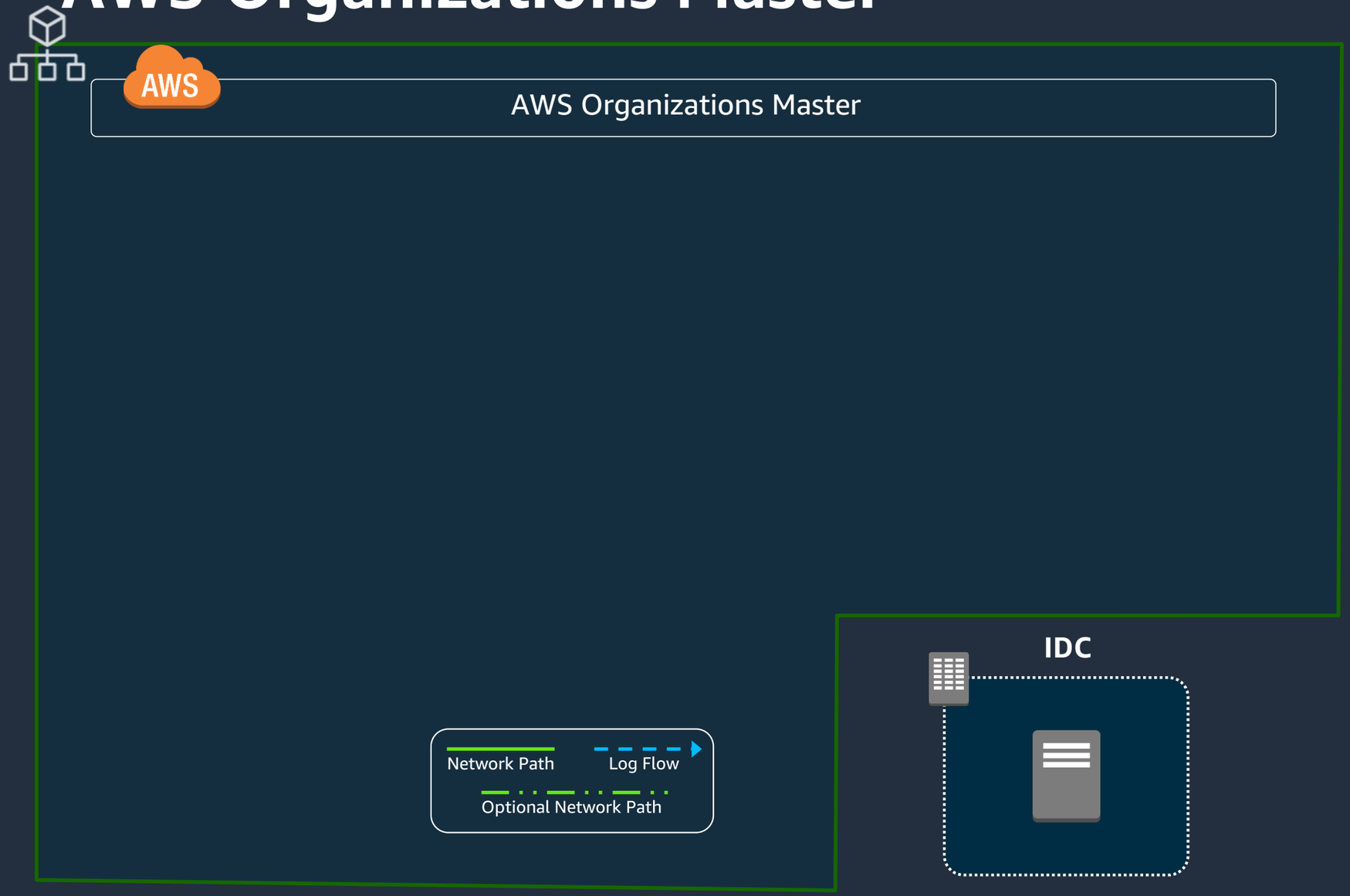
Dev: 开发环境

Pre-Prod: 预发布环境

Prod: 生产环境

Team SS: 团队共享服务, 数据湖

AWS Organizations Master



无法连接至IDC

服务控制策略 (SCP)

账单整合

总额折扣

最小资源管理

限制访问

限制组织角色!

亚马逊云科技

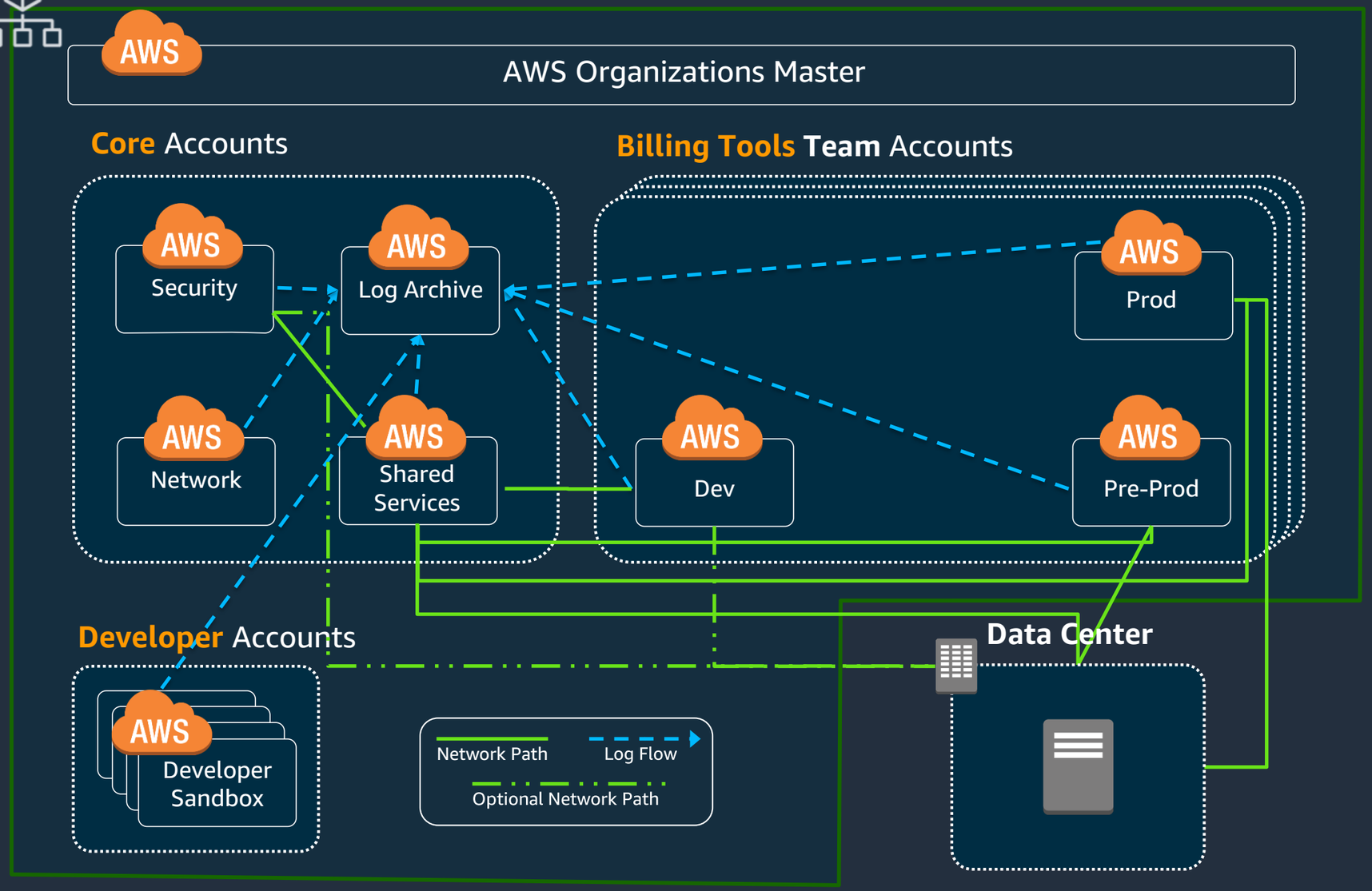
SCP: 防止 AWS CloudTrail 被禁用

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": ”cloudtrail:StopLogging",
      "Resource": "*"
    }
  ]
}
```

SCP: 不允许VPC创建互联网网管(IGW)

```
"Statement": [
     {
      "Effect": "Deny",
      "Action": [
          "ec2:AttachInternetGateway”,
          “ec2:CreateInternetGateway”,
          “ec2:AttachEgressOnlyInternetGateway”,
          “ec2:CreateVpcPeeringConnection”,
          “ec2:AcceptVpcPeeringConnection"
               ],
      "Resource": "*"
    }
  ]
```

团队: 账单账户



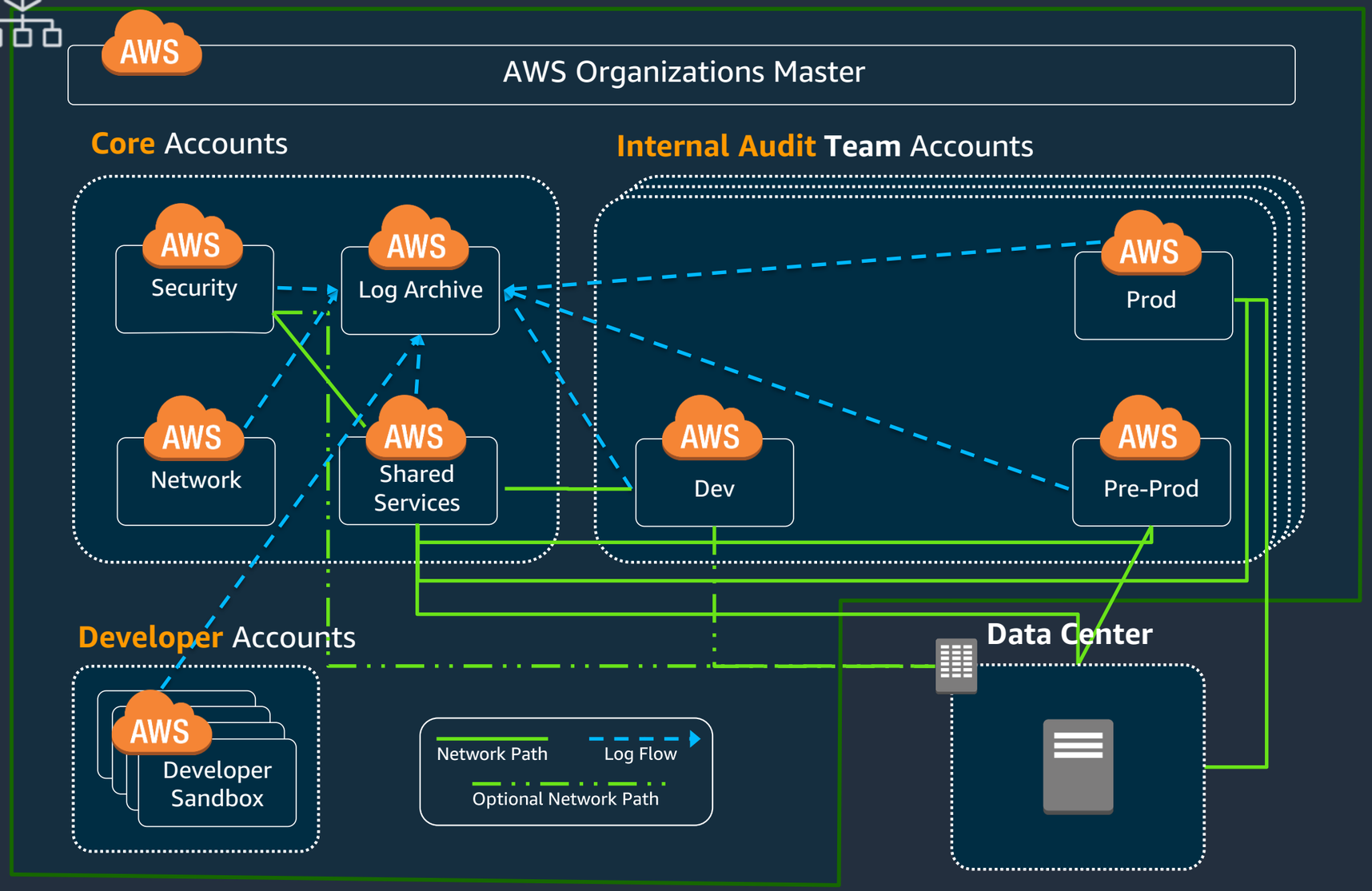
减少访问组织账户

账单报告

使用账单监控和报告

成本优化和预留实例

团队: 内部审计

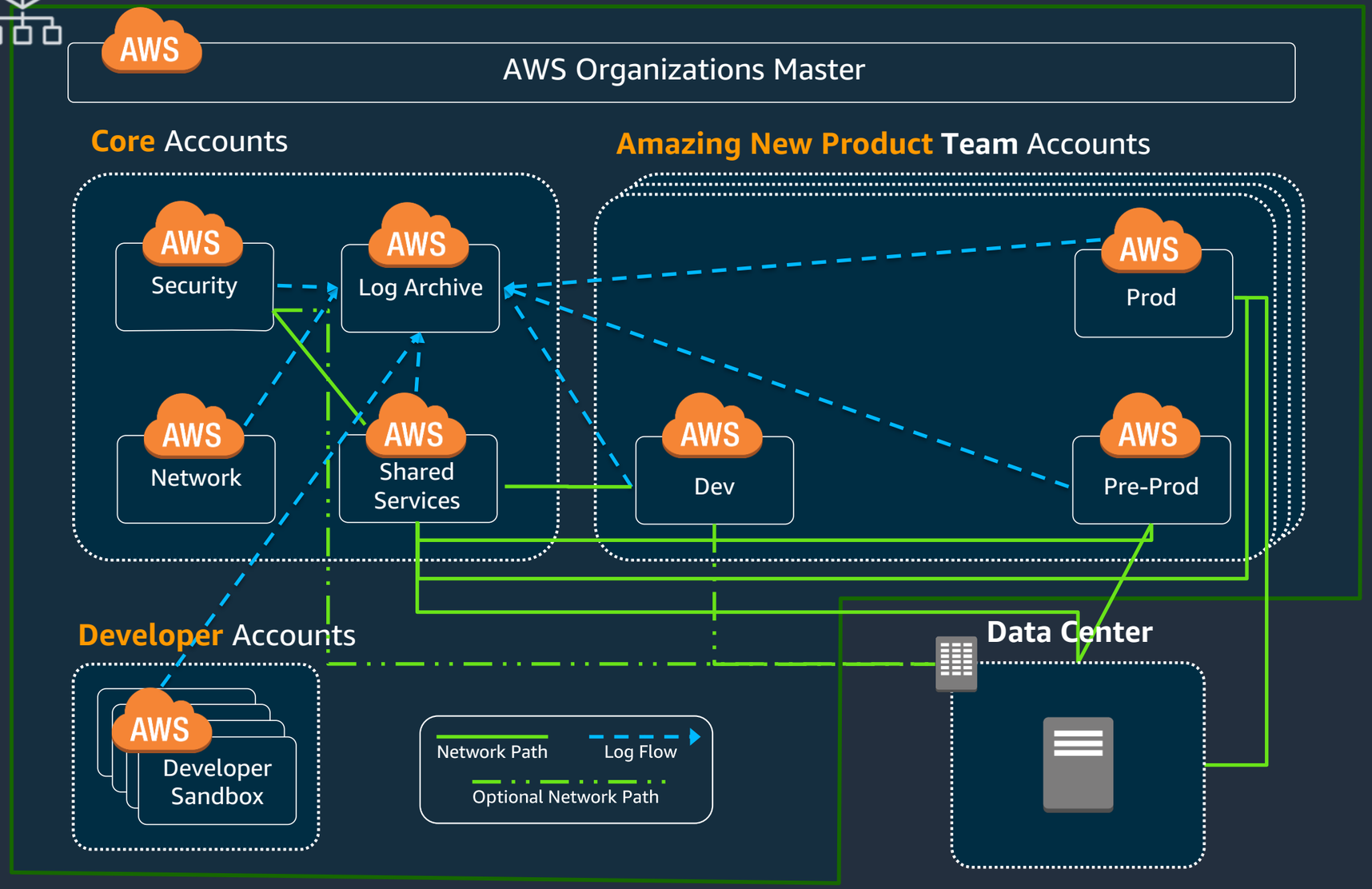


合规遵从

只读权限访问日志

受限的权限

团队: 新产品



匹配开发生命周期

Think small

回顾

- 如何给 “人” 和 “应用” 授权
- 如何阅读和编写IAM
- IAM实体的权限边界
- 多账户管理 - AWS Control Tower

亚马逊云科技

Thank you!