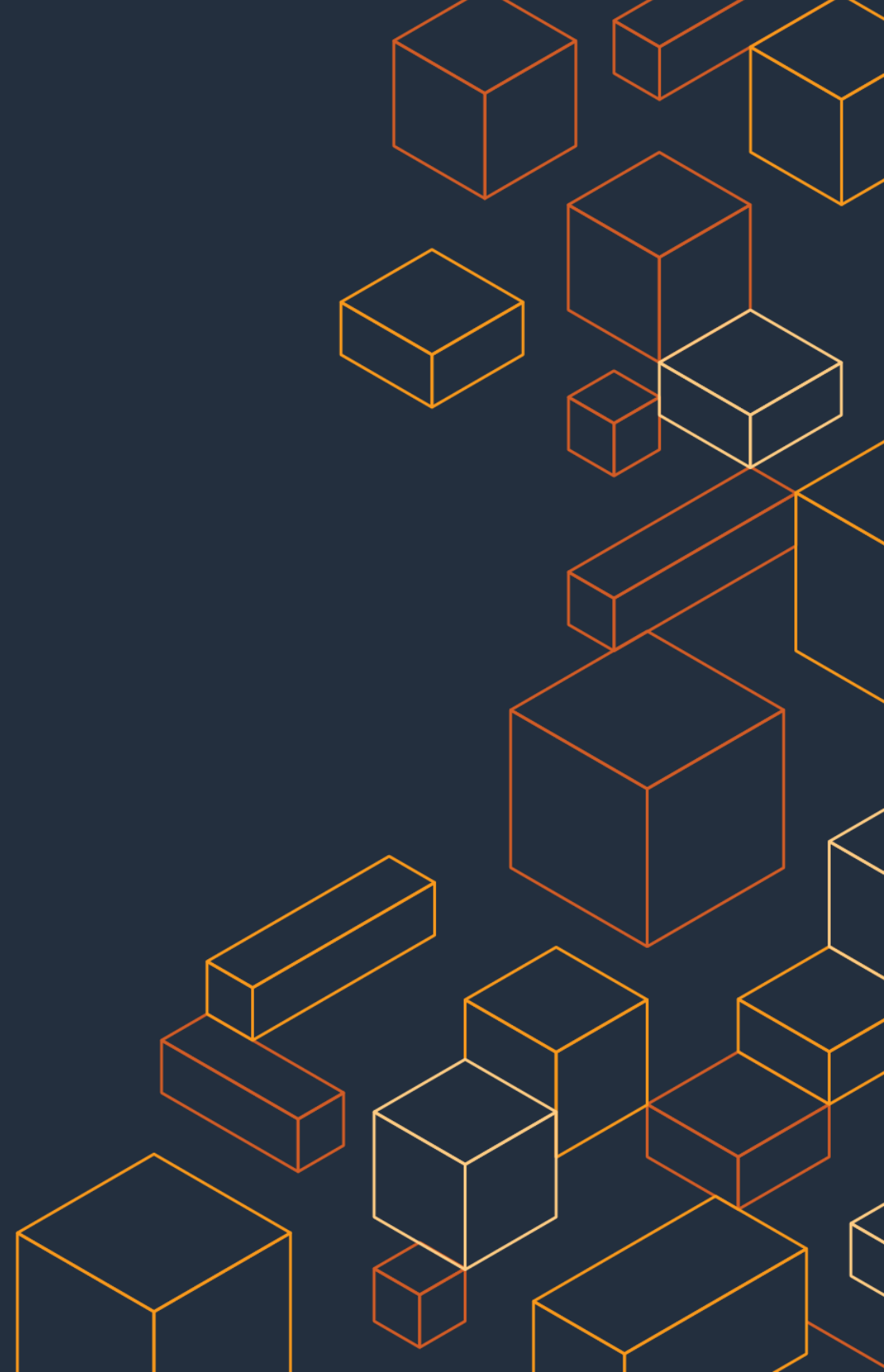




2021 Security Day

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

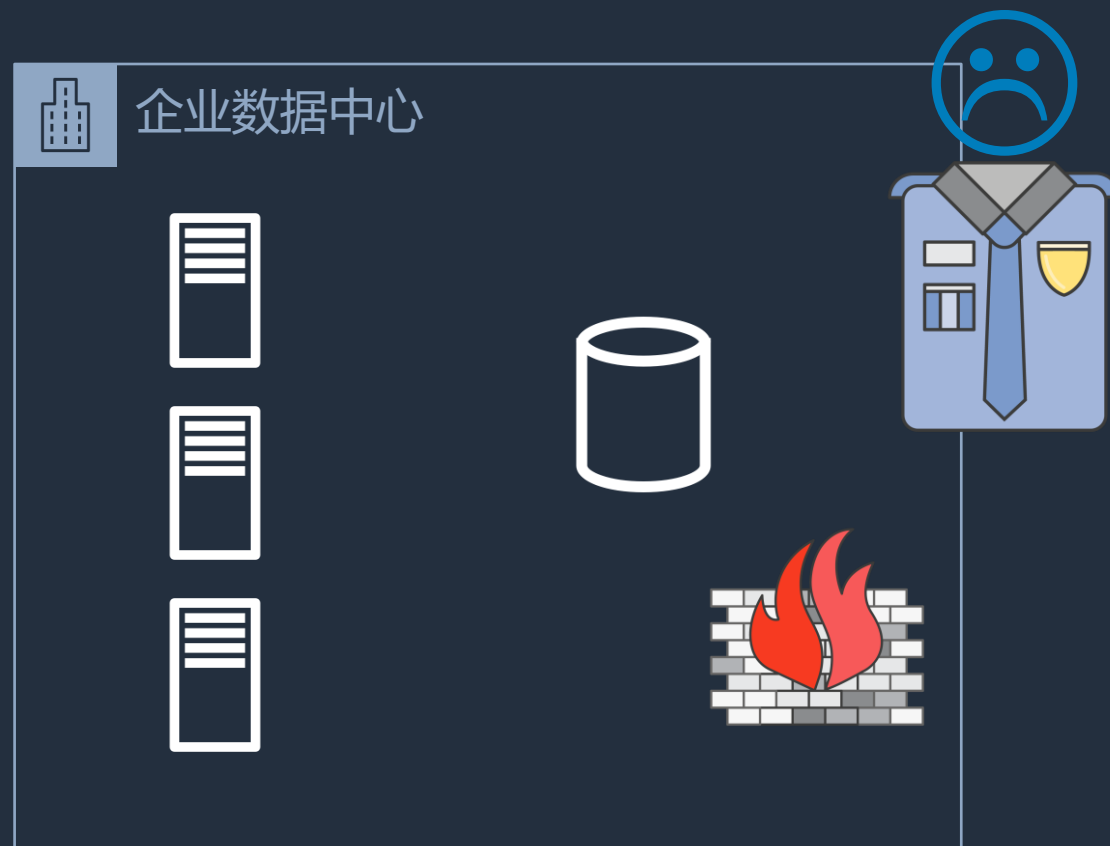


AWS Resource Access Manager

简单安全地共享AWS资源

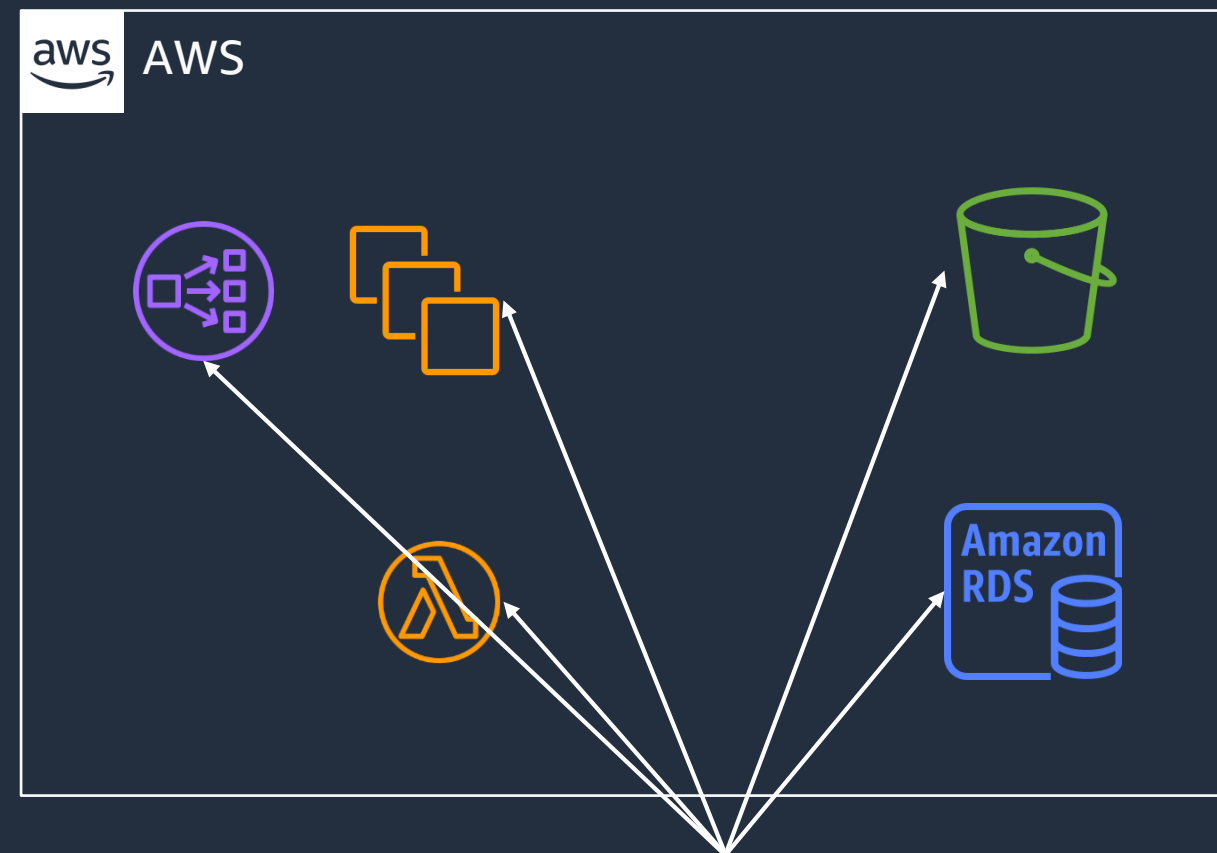
为什么学习AWS IAM

上云前的安全



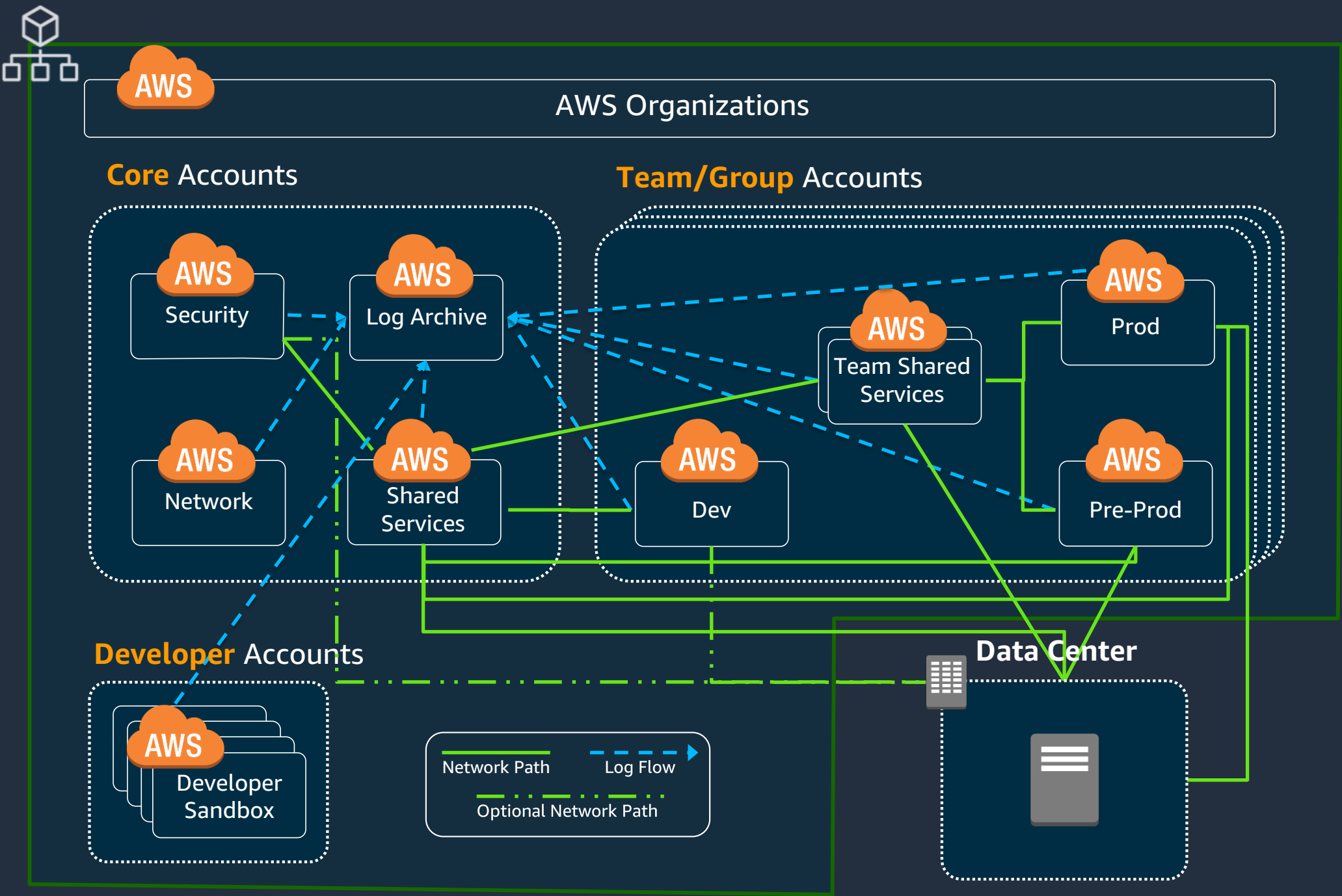
在外围设备实现安全防护

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



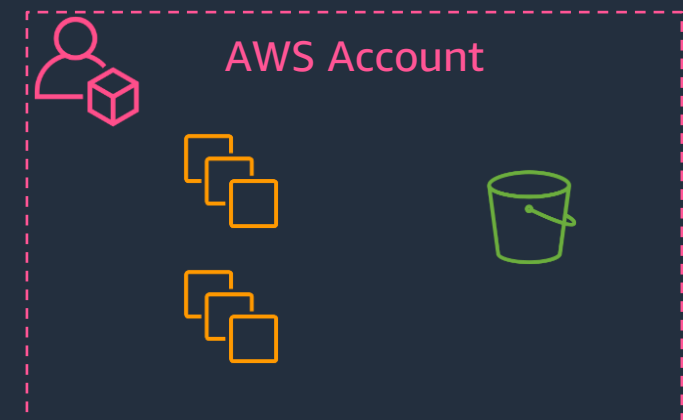
- Orgs:** 账号管理
- Log Archive:** 安全日志
- Security:** 安全工具, AWS Config rules
- Shared services:** 活动目录, 限制监控
- Network:** Direct Connect专线
- Dev Sandbox:** 实验环境
- Dev:** 开发环境
- Pre-Prod:** 预发布环境
- Prod:** 生产环境
- Team SS:** 团队共享服务, 数据湖

议程

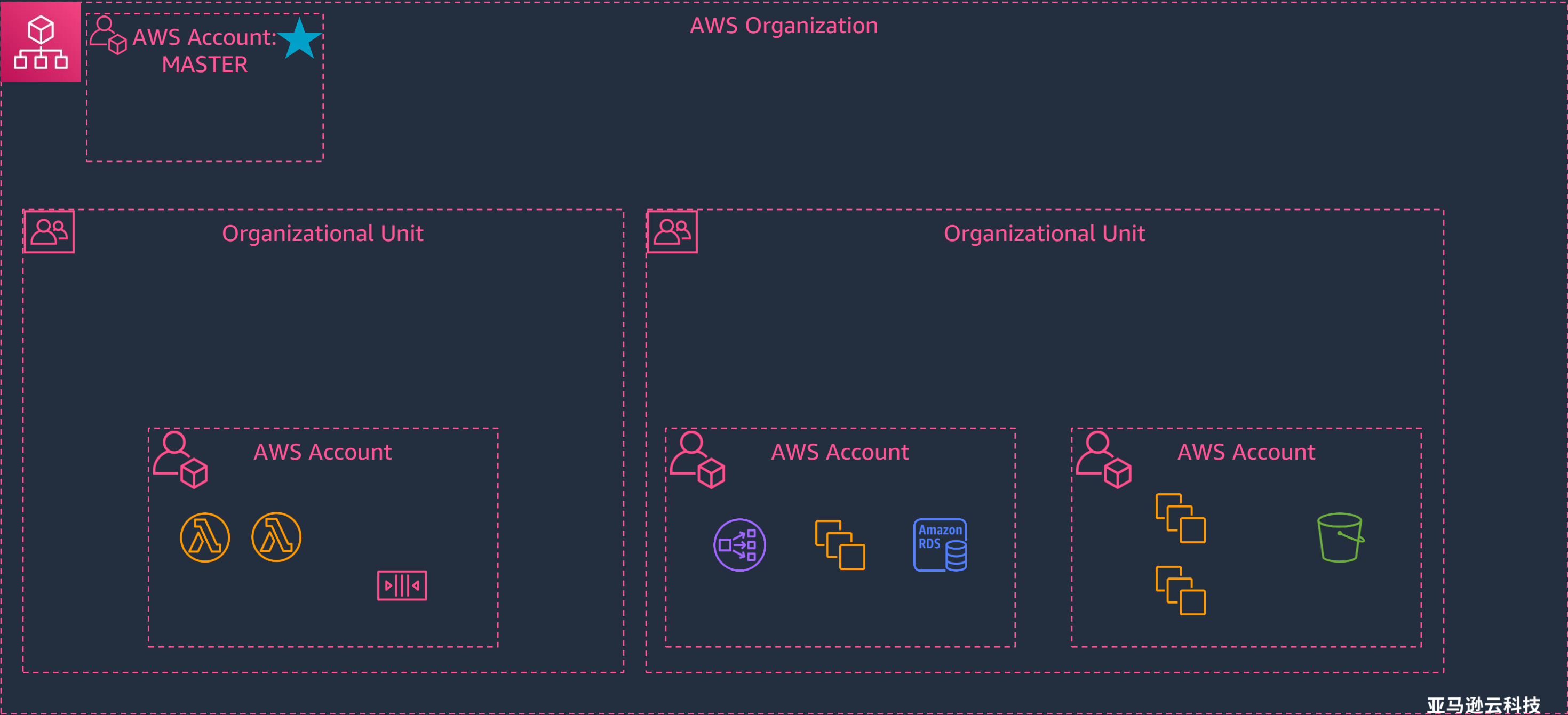
- 如何给“人”和“应用”授权
- 如何阅读和编写IAM
- IAM实体的权限边界
- 多账户管理 - AWS Control Tower

如何给“人”和“应用”授权

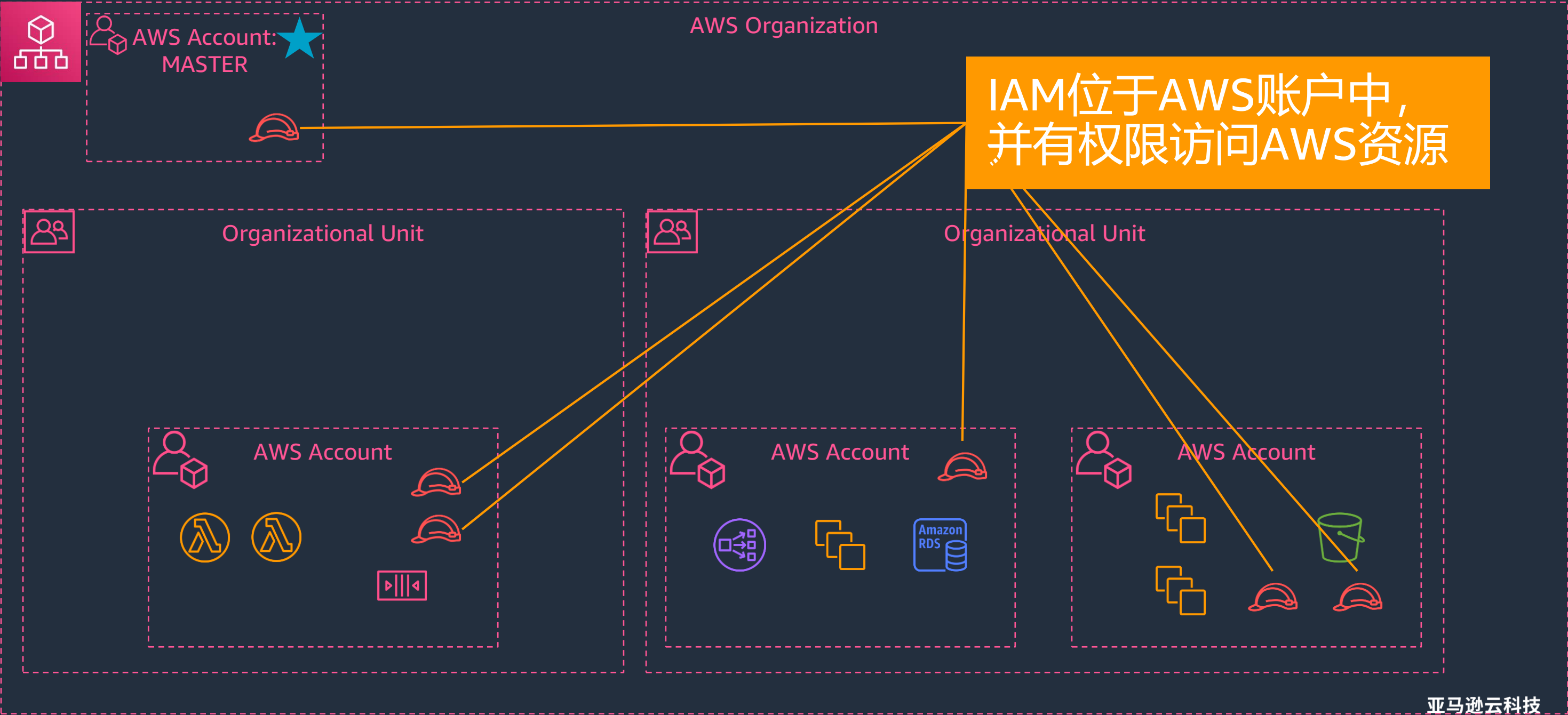
AWS上的账户



AWS上的账户



AWS上的账户



IAM 用户

账户: 222233334444
用户名: becky
密码: 2T|-|3c1@uD!!



Account ID or alias

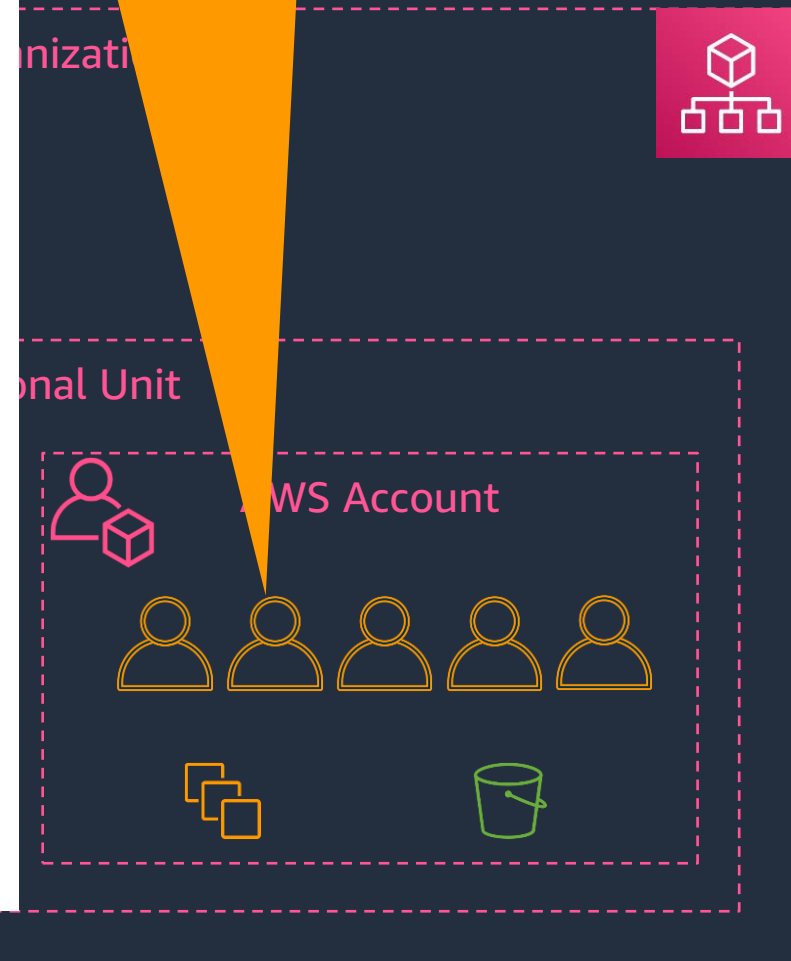
IAM user name

Password

Sign In

[Sign-in using root account credentials](#)

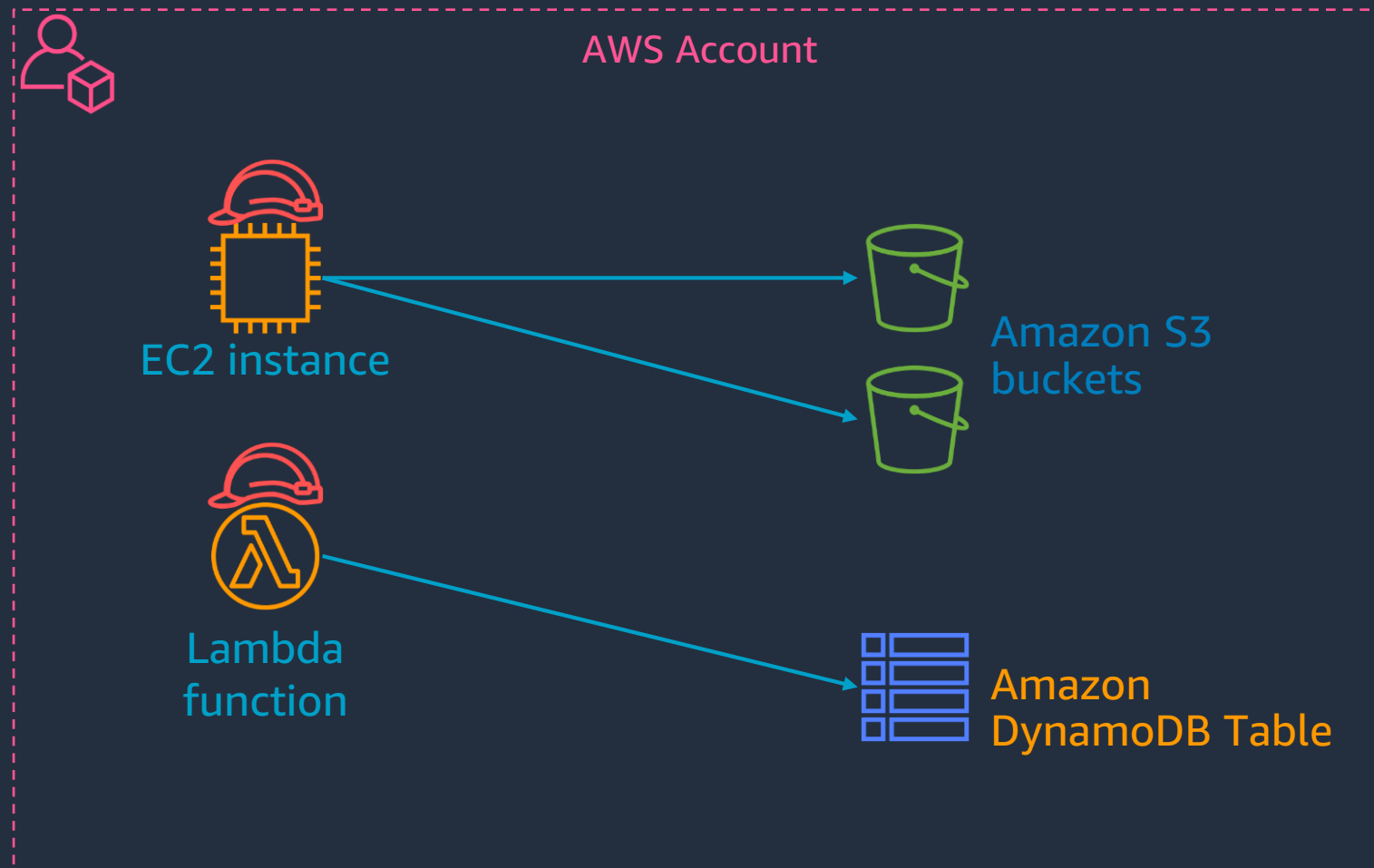
[Forgot password?](#)



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计算环境中运行，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

Create role

1

2

3

4

Select type of trusted entity



AWS service

EC2, Lambda and others



Another AWS account

Belonging to you or 3rd party



Web identity

Cognito or any OpenID provider



SAML 2.0 federation

Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

API Gateway	Comprehend	ElastiCache	Lambda	S3
AWS Backup	Config	Elastic Beanstalk	Lex	SMS
AWS Support	Connect	Elastic Container Service	License Manager	SNS

EC2实例有短期凭证访问AWS资源

© 2021, Amazon Web Services, Inc. or its Affiliates.

亚马逊科技

分配 AWS 托管策略

Identity and Access Management (IAM)

▼ AWS Account

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Create policy

Policy actions ▼

Filter policies ▼

Search

		Policy name ▼	Type	Used as	Description
☐	▶	 AdministratorAccess	Job function	Permissions policy (6)	Provides full access to AWS services and res
☐	▶	 AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusi
☐	▶	 AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resou
☐	▶	 AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaFo
☐	▶	 AlexaForBusinessNetworkProfileServicePolicy	AWS managed	None	This policy enables Alexa for Business to per
☐	▶	 AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusines

... 和其他更多AWS托管策略

举例：管理员权限策略

Policies > AdministratorAccess

Summary

Policy ARN

arn:aws:iam::aws:policy/AdministratorAccess

Description

Provides full access to AWS services and resources.

Permissions

Policy usage

Policy versions

Access Advisor

Policy summary

{ } JSON

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Effect": "Allow",

6 "Action": "*",

7 "Resource": "*"

8 }

9]

10 }

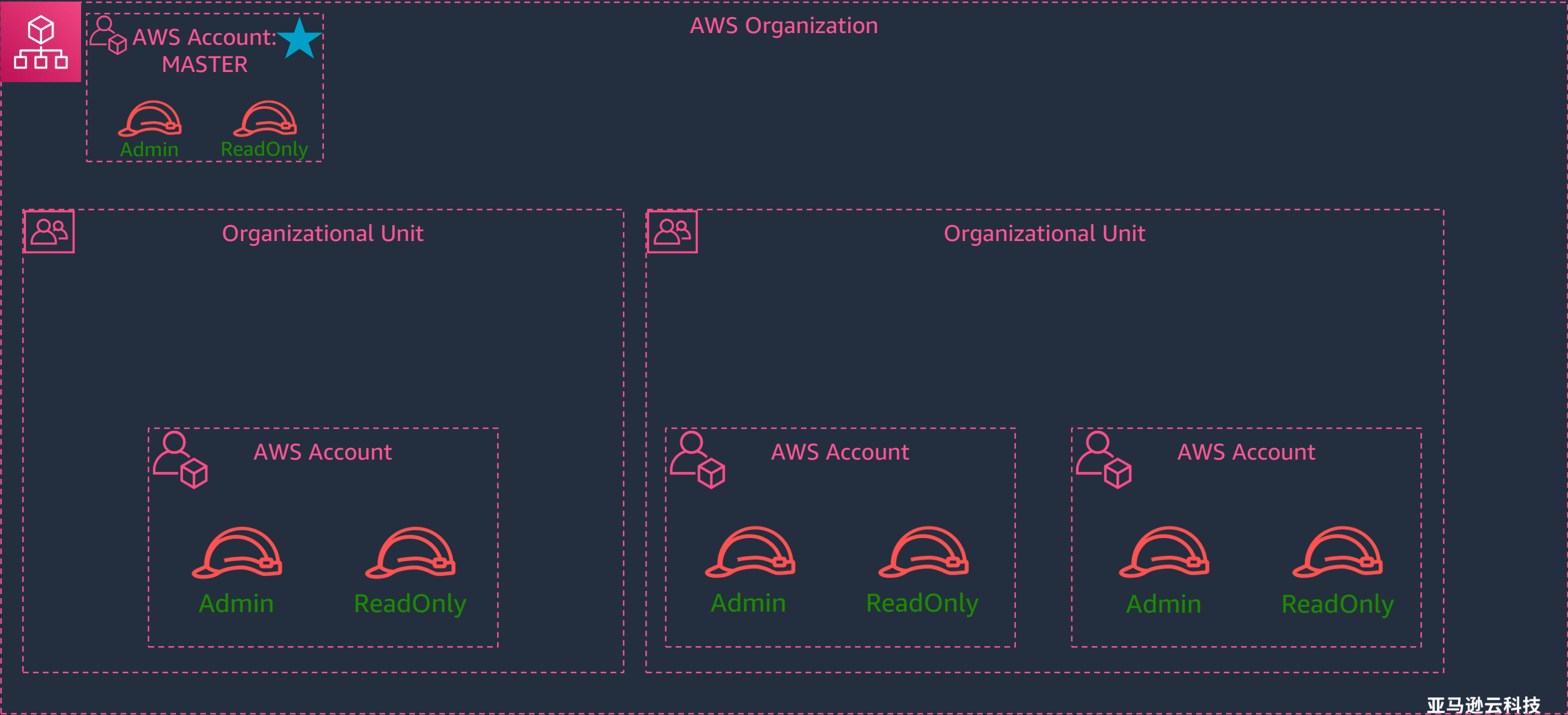
举例: 只读权限策略

The screenshot shows the AWS IAM console interface for the **ReadOnlyAccess** policy. The breadcrumb navigation at the top indicates the path: **Policies > ReadOnlyAccess**. The main heading is **Summary**. Below this, there are two rows of information: **Policy ARN** with the value `arn:aws:iam::aws:policy/ReadOnlyAccess` (highlighted with a blue box), and **Description** with the text "Provides read-only access to AWS services and". Below the summary section, there are four tabs: **Permissions** (selected), **Policy usage**, **Policy versions**, and **Access Advisor**. Under the **Permissions** tab, there are two sub-tabs: **Policy summary** and **{ } JSON**. The **{ } JSON** sub-tab is active, displaying the policy's JSON definition. The JSON is formatted with line numbers on the left and syntax highlighting. The policy version is `"2012-10-17"`, and the `"Statement"` array contains a single statement with `"Action"` permissions: `"a4b:Get*", "a4b:List*", "a4b:Describe*", "a4b:Search"`.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "a4b:Get*",
7         "a4b:List*",
8         "a4b:Describe*",
9         "a4b:Search"
```

... 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:

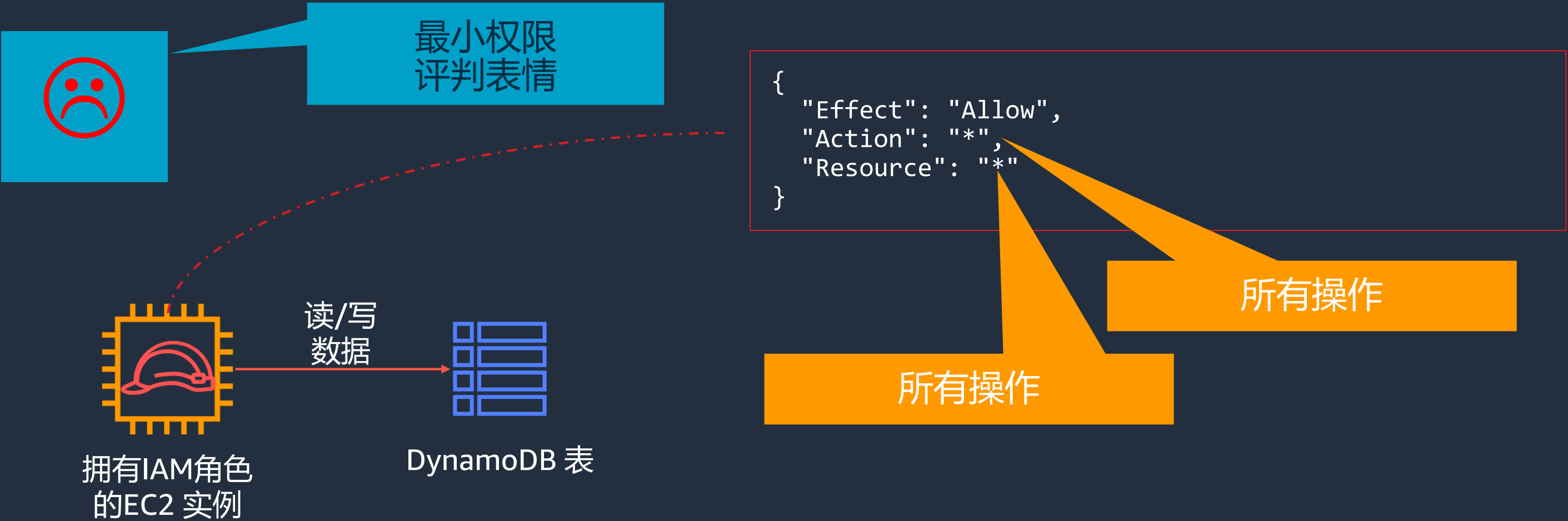
- 如果有任意拒绝策略 → AccessDenied
- 如果有允许 → Allow
- 否则 AccessDenied

如何阅读和编写IAM

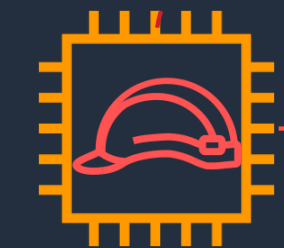
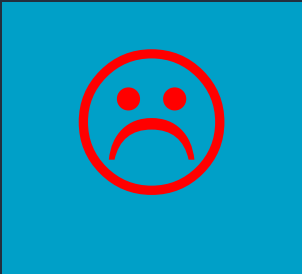
举例: 从DynamoDB读写数据



举例: 从DynamoDB读写数据



举例: 从DynamoDB读写数据



拥有IAM角色
的EC2 实例

读/写
数据



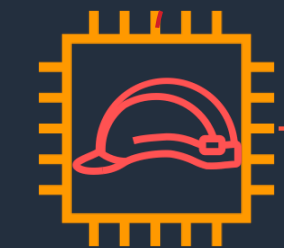
DynamoDB 表

```
{  
  "Effect": "Allow",  
  "Action": "dynamodb:*",  
  "Resource": "*" }  
}
```

所有DynamoDB操作

所有资源

举例: 从DynamoDB读写数据



拥有IAM角色的EC2 实例

读/写
数据



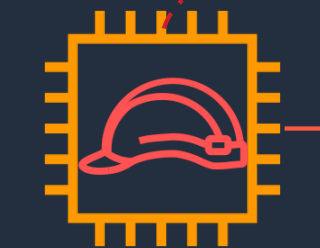
DynamoDB 表

```
{
  "Effect": "Allow",
  "Action": [
    "dynamodb:GetItem",
    "dynamodb:PutItem"
  ],
  "Resource": "*"
}
```

指定DynamoDB 操作

所有资源

举例: 从DynamoDB读写数据



拥有IAM角色
的EC2 实例

读/写
数据



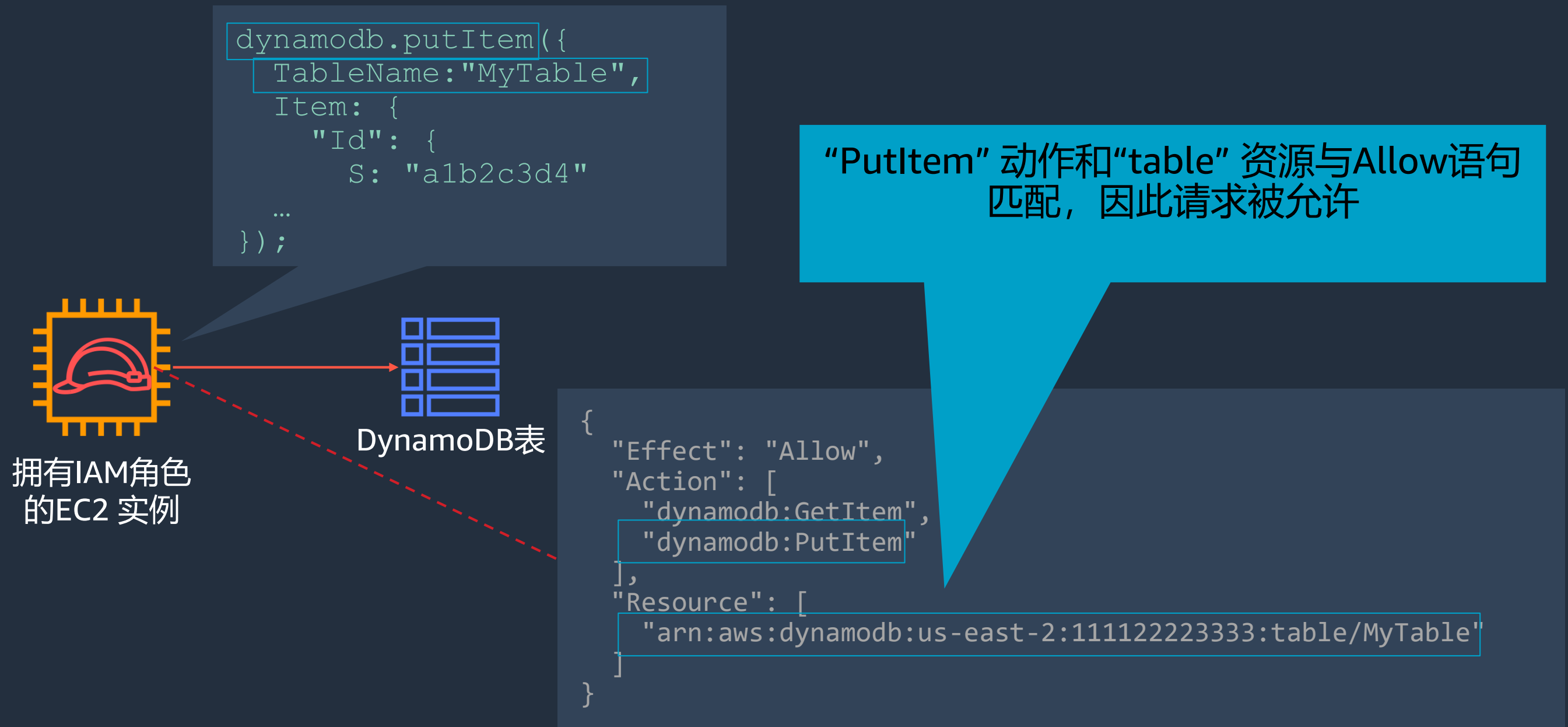
DynamoDB 表

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

DynamoDB:
读/写 操作

指定DynamoDB的表

AWS鉴权的工作方式



IAM实体的权限边界

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

管理员



委派管理员



IAM用户和角色



角色



权限



资源



Lambda
函数



角色



权限

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

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

使用权限边界

管理员



委派管理员



“绑定的”IAM用户
和角色



角色



权限

资源



Lambda
函数



角色



权限

```
"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

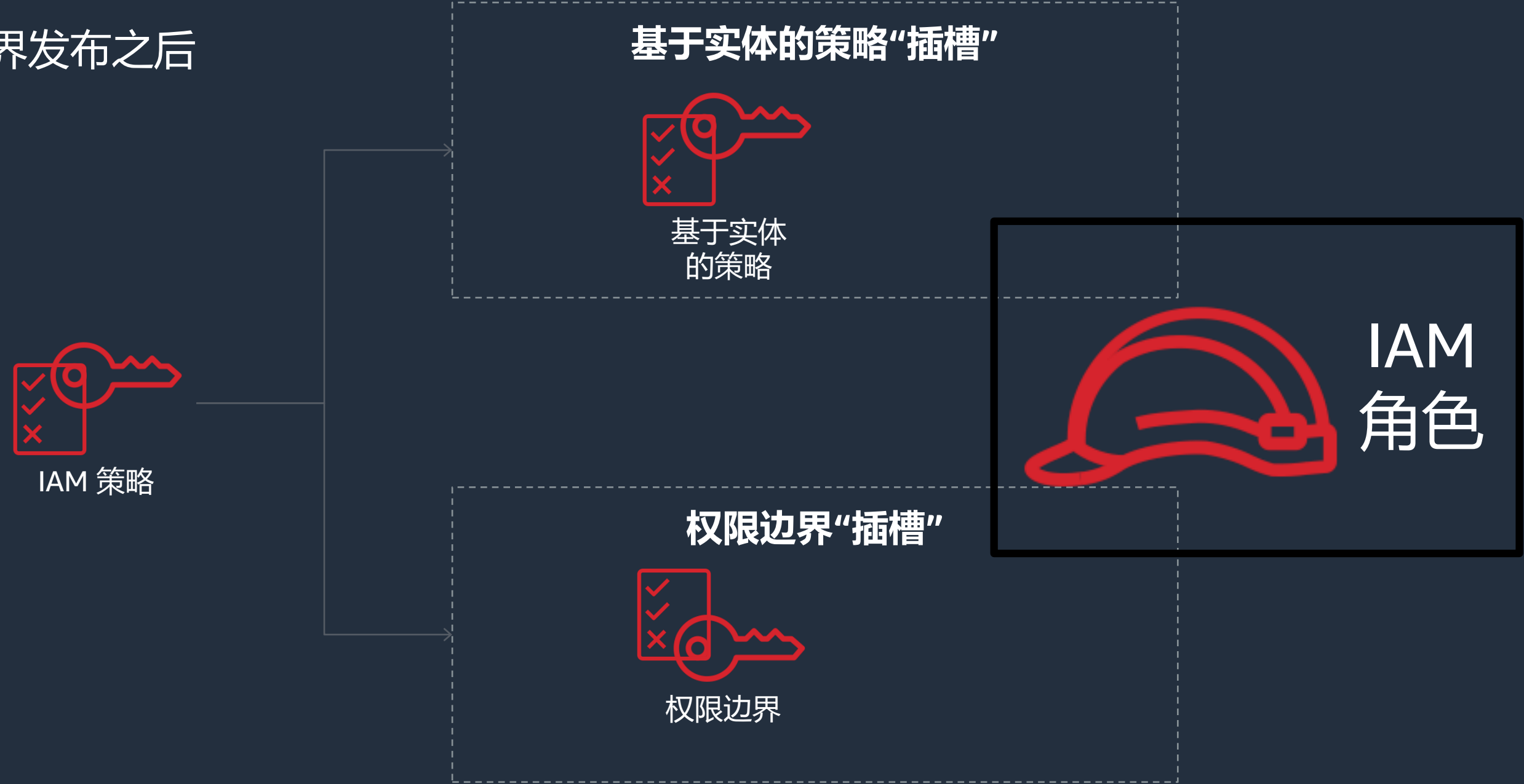


基于实体的策略“插槽”

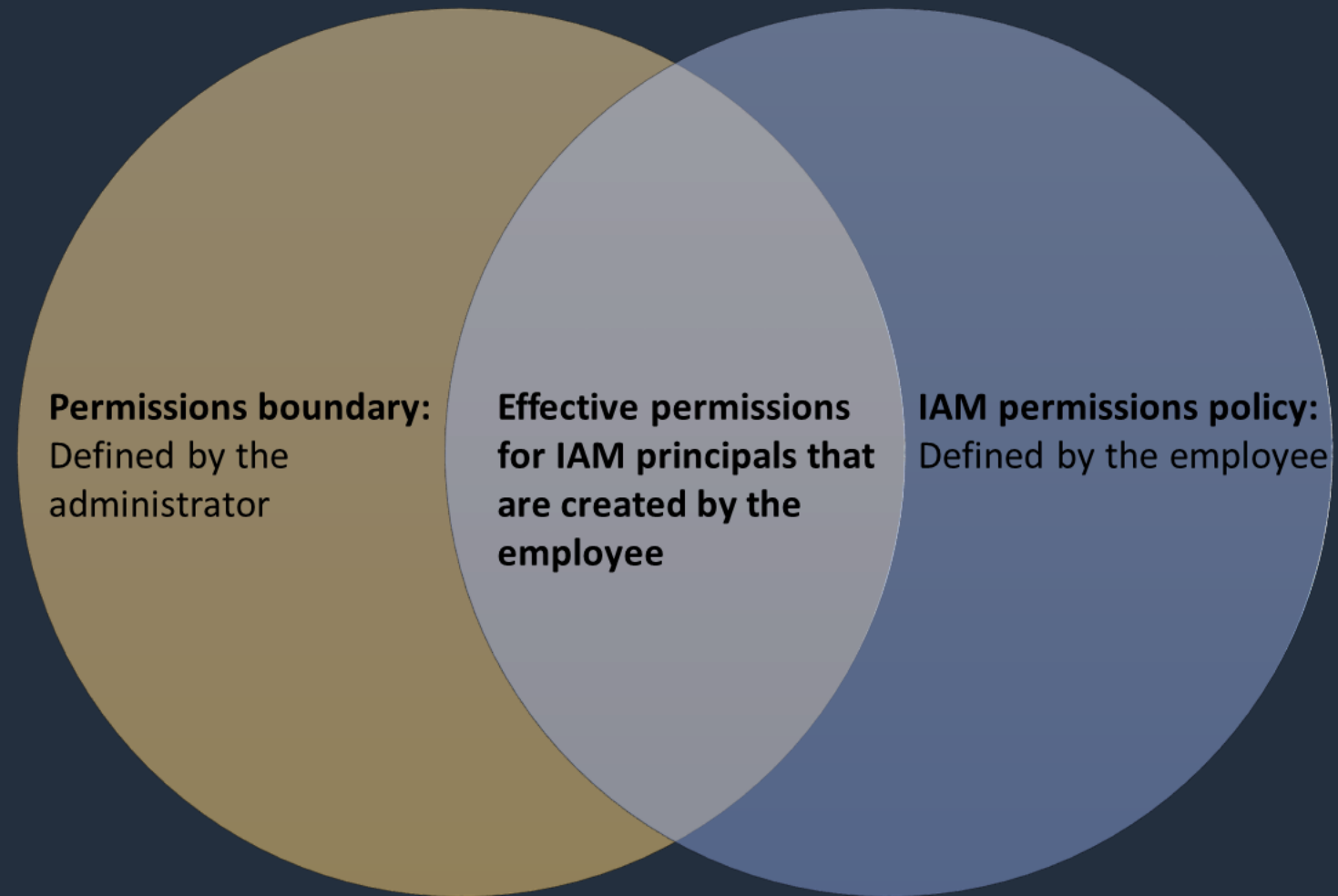


权限策略“插槽”

权限边界发布之后



权限策略“插槽”



权限策略“插槽”

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ▼

Search

Showing 582 results

	Policy name ▼	Used as	Description
☐	▶  AdministratorAccess	Permissions policy (9)	Provides full access to AWS services an...
☐	▶  AlexaForBusinessDeviceSetup	None	Provide device setup access to AlexaFor...
☐	▶  AlexaForBusinessFullAccess	None	Grants full access to AlexaForBusiness r...
☐	▶  AlexaForBusinessGatewayExecution	None	Provide gateway execution access to Al...
☐	▶  AlexaForBusinessReadOnlyAccess	None	Provide read only access to AlexaForBu...
☐	▶ AllowAssumeDeleteDDBRole	None	
☐	▶ AllowDeleteofDDbTable	Permissions policy (1)	
☐	▶  AmazonAPIGatewayAdministrator	None	Provides full access to create/edit/delete...

▼ Set permissions boundary

Set a permissions boundary to control the maximum permissions this role can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

☒ Create role without a permissions boundary

☐ Use a permissions boundary to control the maximum role permissions

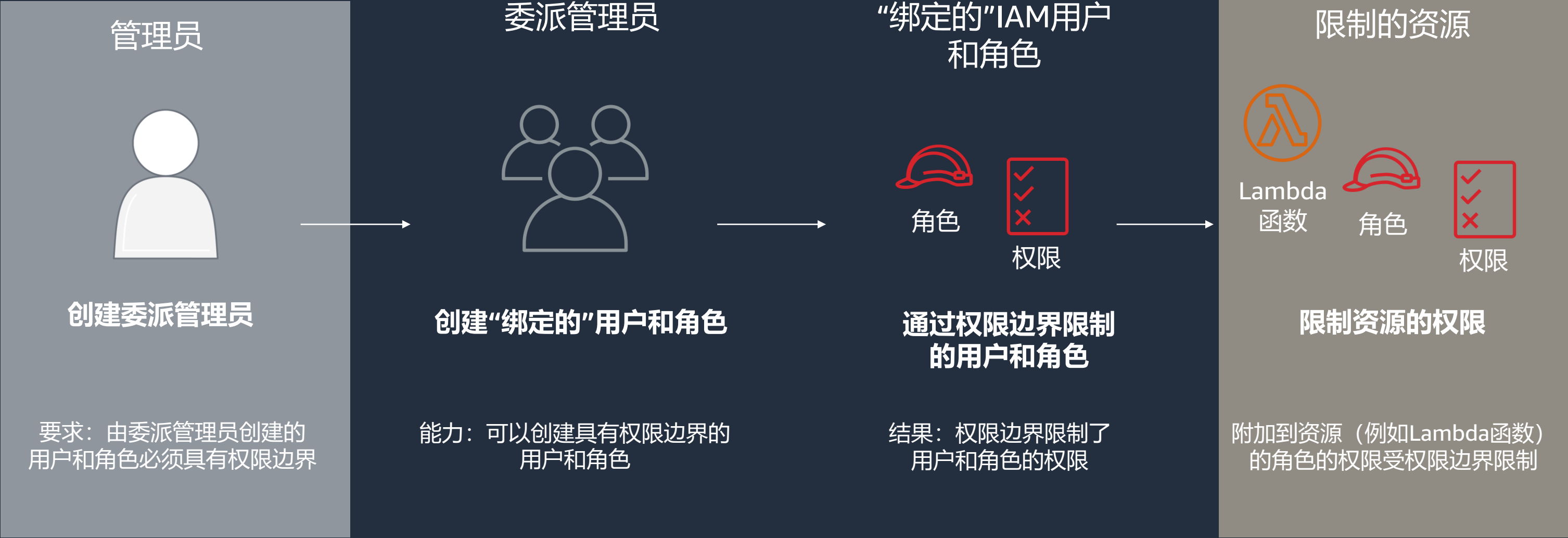
基于实体的策略“插槽”

权限边界“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 workflow



多账户管理 – AWS Control Tower

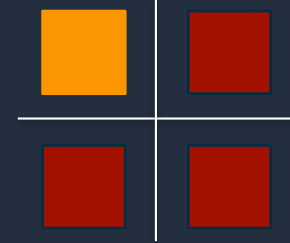
一个账户是不够的...



多团队



计费



隔离

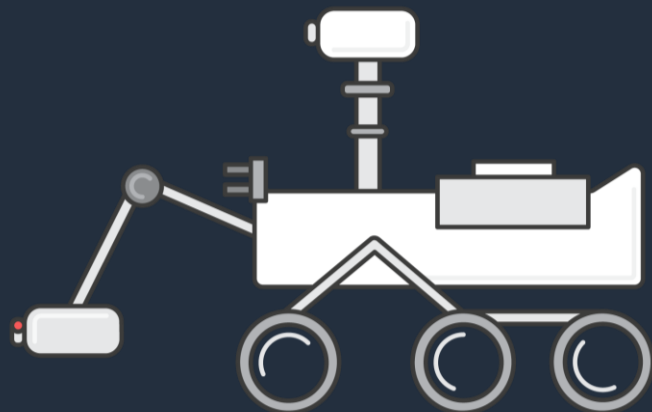


安全与合规控制

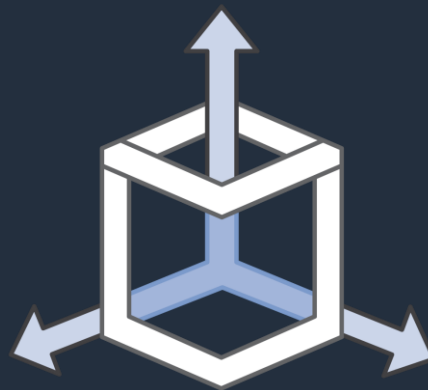


业务流程

目标



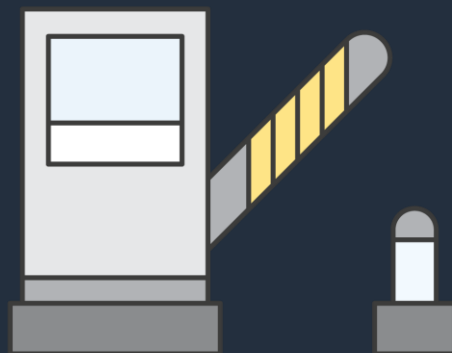
自动化



可扩展



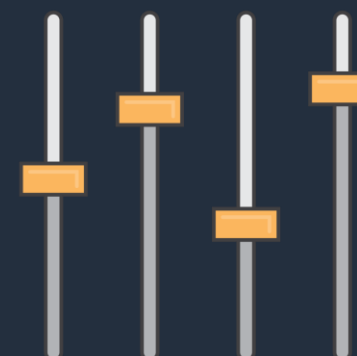
自服务



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

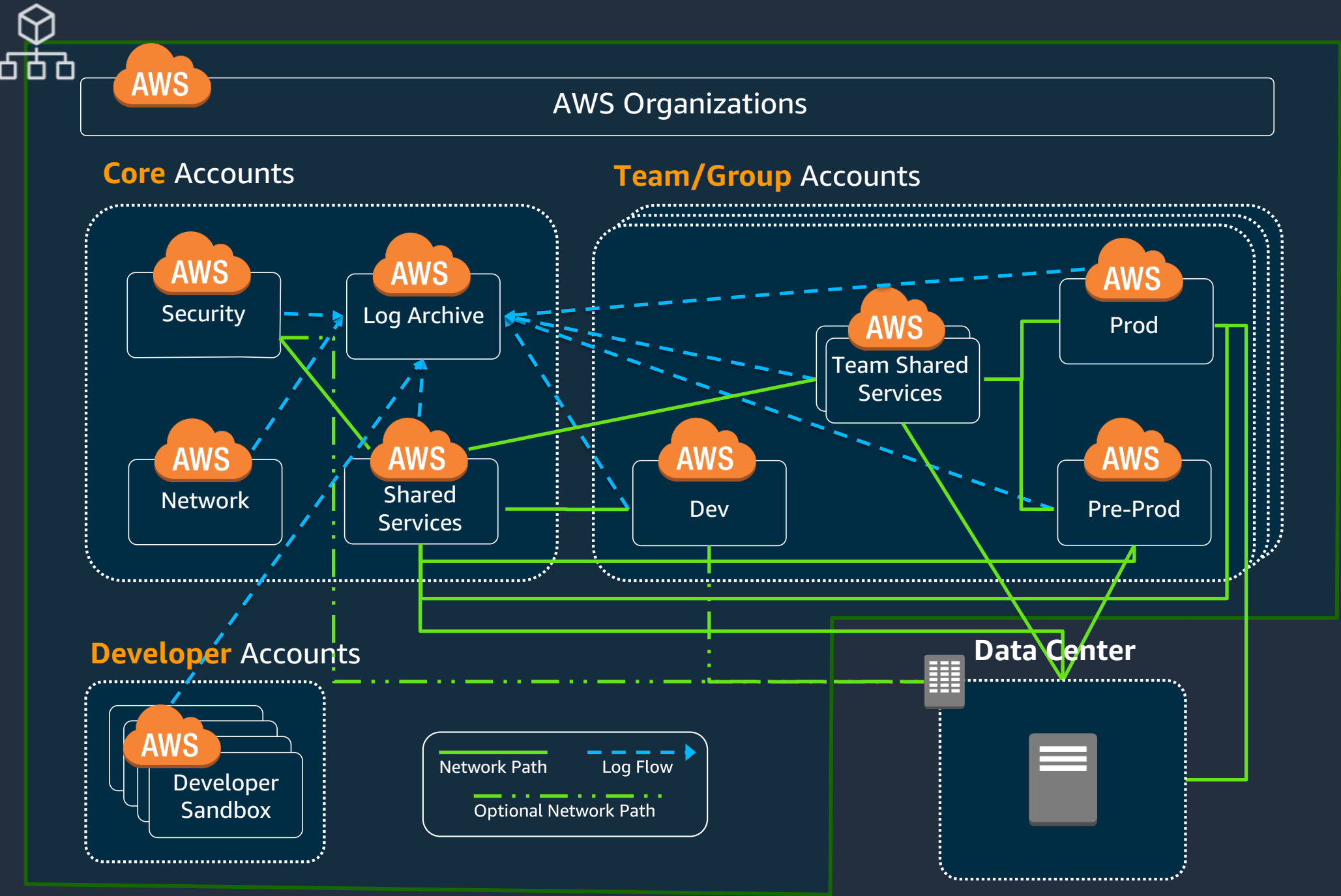


生产环境



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!

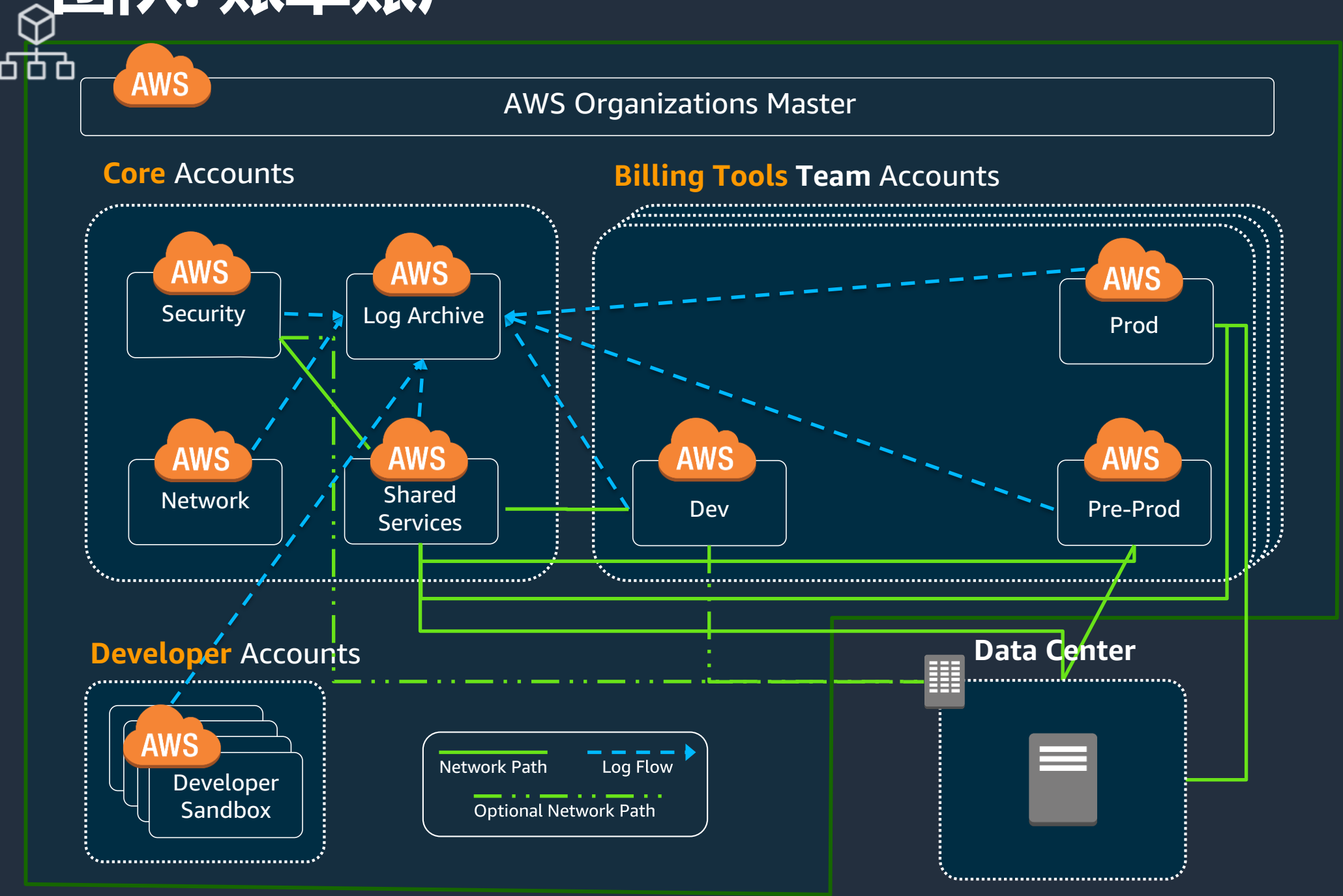
SCP: 防止 AWS CloudTrail 被禁用

```
{  
  "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



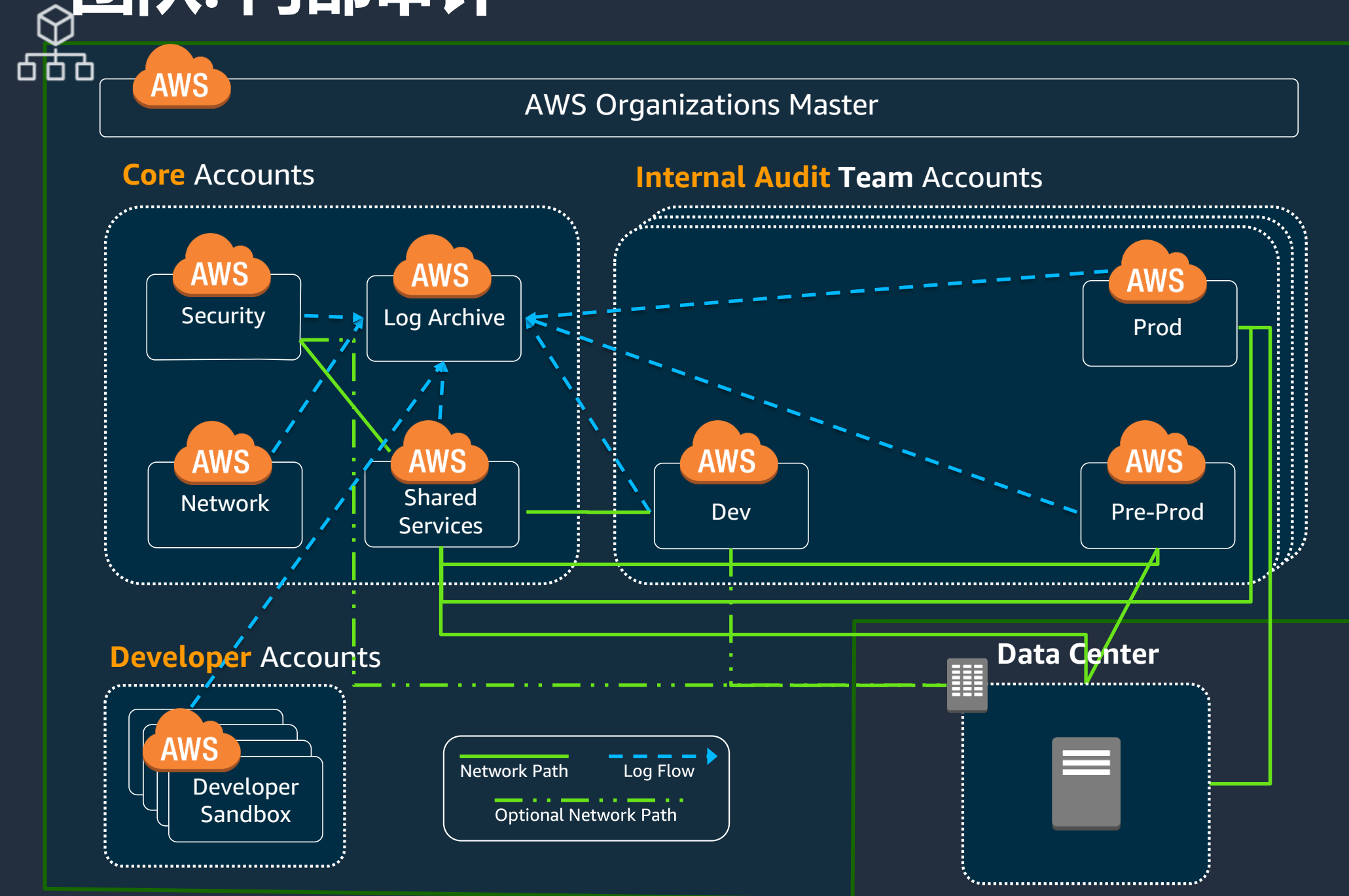
减少访问组织账户

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

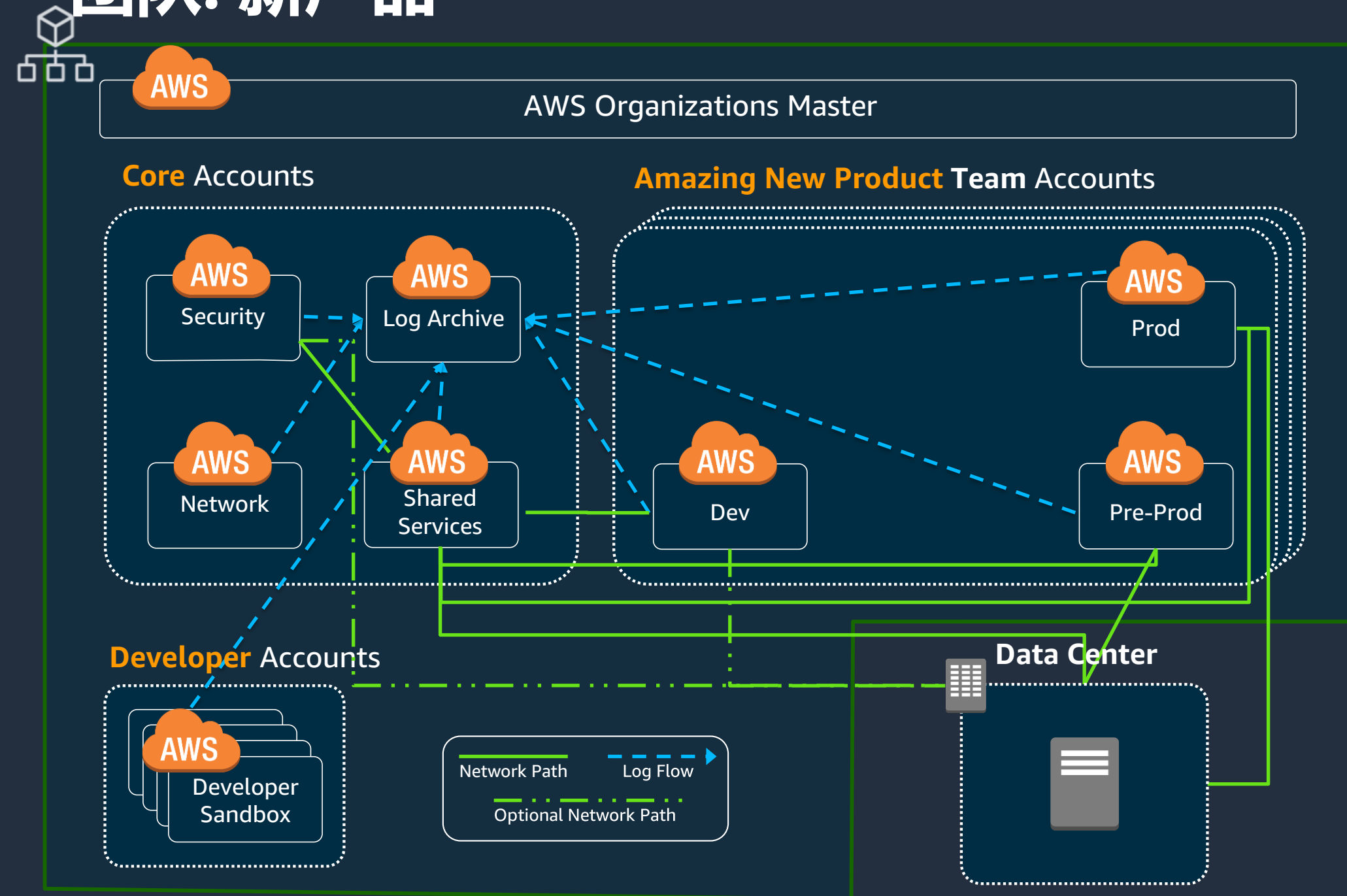


合规遵从

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



Thank you!

