Segurança na nuvem com AWS

Willyan Guimarães - @willyancaetanodev

Objetivo Geral

Apresentar e discutir os conceitos relativos a segurança na nuvem com AWS bem como também falar sobre os principais serviços e recursos relacionados.

Percurso

Etapa 1 O modelo de responsabilidade compartilhada

Etapa 2 Criptografia

Etapa 3 Gerenciamento de acessos

Percurso

Etapa 4 AWS Organizations

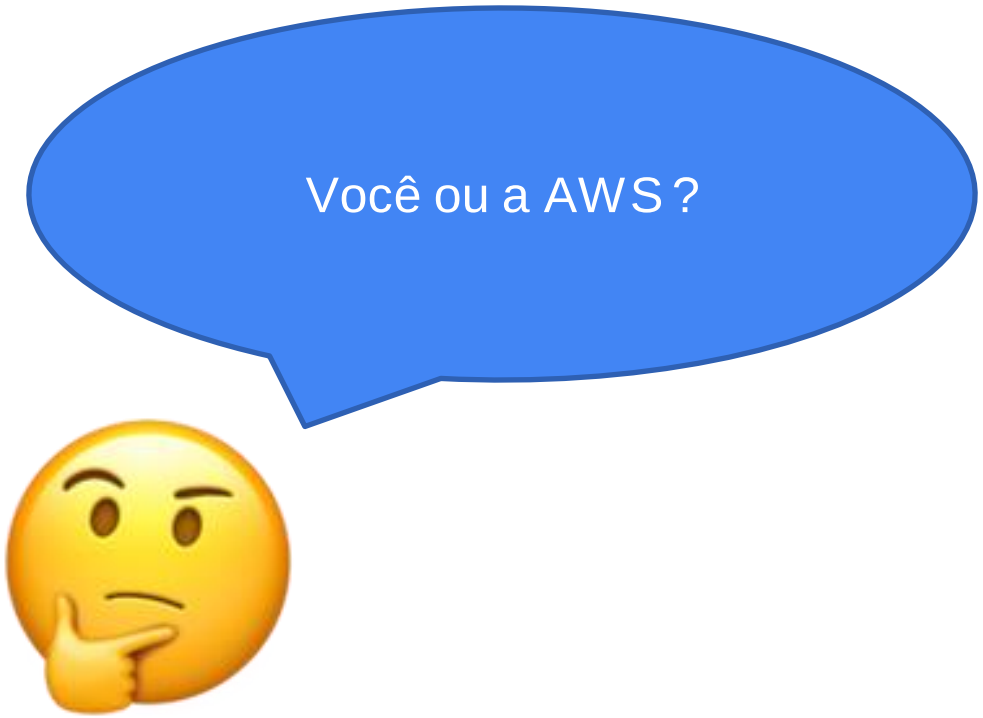
Etapa 5 Conformidade e suporte

Etapa 6 Serviços adicionais

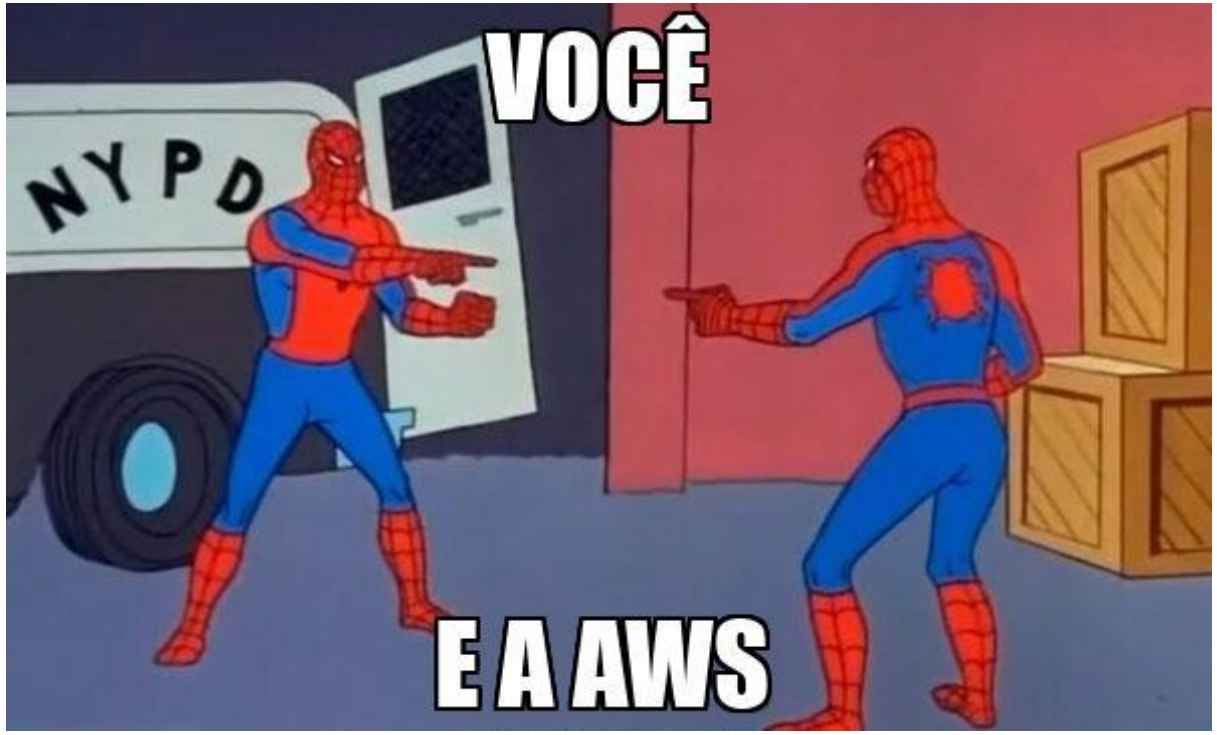
Etapa 1

O modelo de responsabilidade compartilhada

Quem é responsável pela segurança ?



Resposta



Modelo de responsabilidade compartilhada

Analogia

Analogia

Modelo de responsabilidade compartilhada

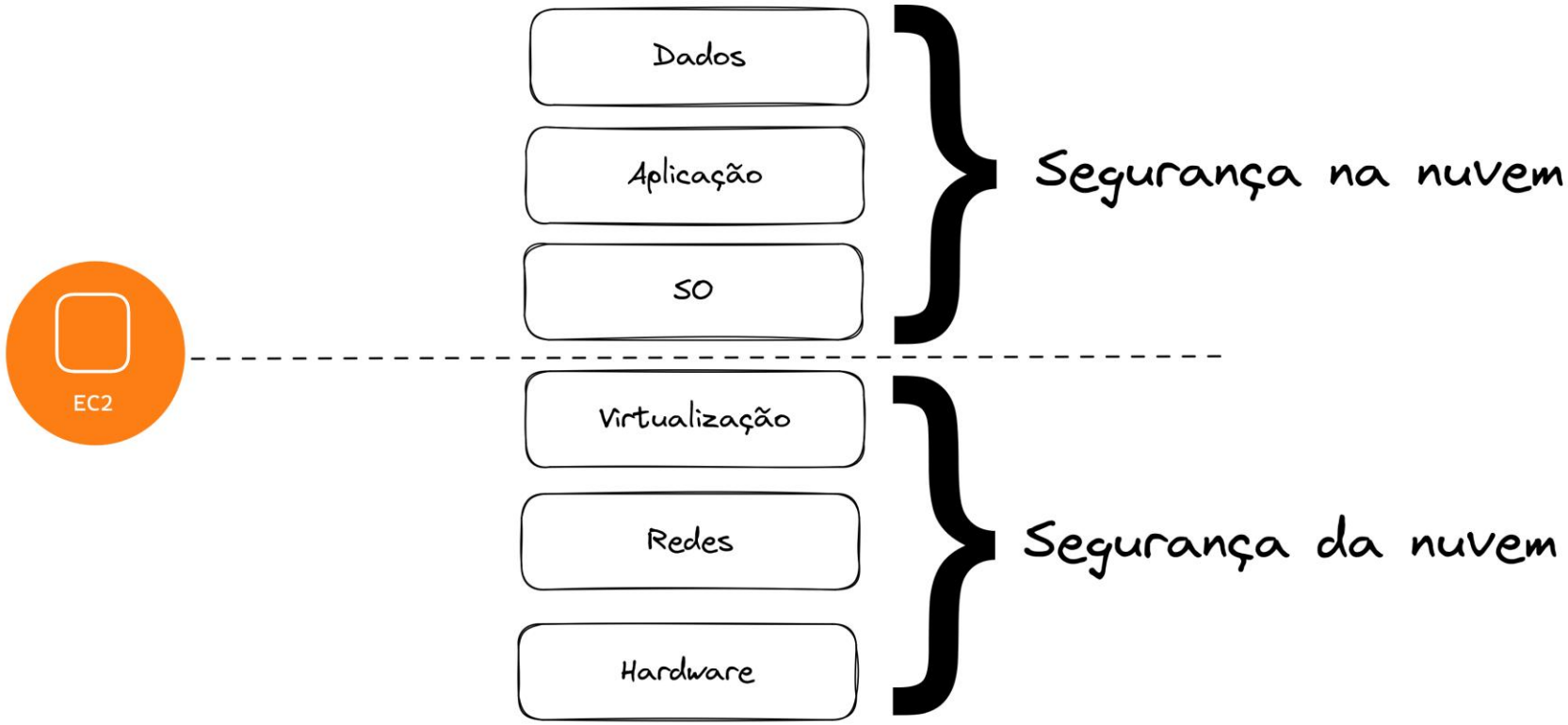
"Segurança na nuvem"

CLIENTES	DADOS DO CLIENTE		
	PLATAFORMA, APLICATIVOS, IDENTITY AND ACCESS MANAGEMENT		
	CONFIGURAÇÃO DO SISTEMA OPERACIONAL, DA REDE E DO FIREWALL		
	CRIPTOGRAFIA DE DADOS DO LADO DO CLIENTE	CRIPTOGRAFIA DO LADO DO SERVIDOR	PROTEÇÃO DE TRÁFEGO DE REDE

"Segurança da nuvem"

AWS	SOFTWARE			
	COMPUTAÇÃO	ARMAZENAMENTO	BANCO DE DADOS	REDES
	HARDWARE/INFRAESTRUTURA GLOBAL DA AWS			
	REGIÕES	ZONAS DE DISPONIBILIDADE	LOCAIS DE BORDA	

Exemplo


Dados
Aplicação
SO
Segurança na nuvem
EC2
Virtualização
Redes
Hardware
Segurança da nuvem

Segurança da nuvem

- Responsável: AWS
- Segurança física dos data centers
- Infraestrutura de hardware e software
- Infraestrutura de rede
- Infraestrutura de virtualização

Segurança na nuvem

- Responsável: Cliente
- Controle total sobre o conteúdo
- Controle de acesso e permissões
- Patches de segurança
- Muda conforme o serviço utilizado

Para saber mais

- https://aws.amazon.com/pt/compliance/shared-responsibility-model/
- https://www.youtube.com/watch?v=Hg_N2SpJYqM

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

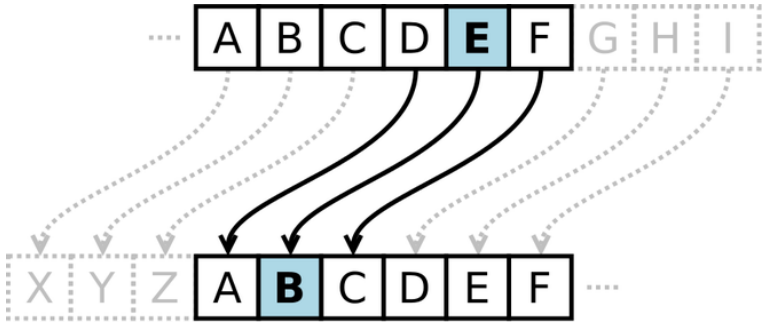
SCAN ME

Etapa 2

Criptografia

O que é Criptografia

Criptografia é a prática de proteger informações por meio do uso de algoritmos codificados, *hashes* e assinaturas.



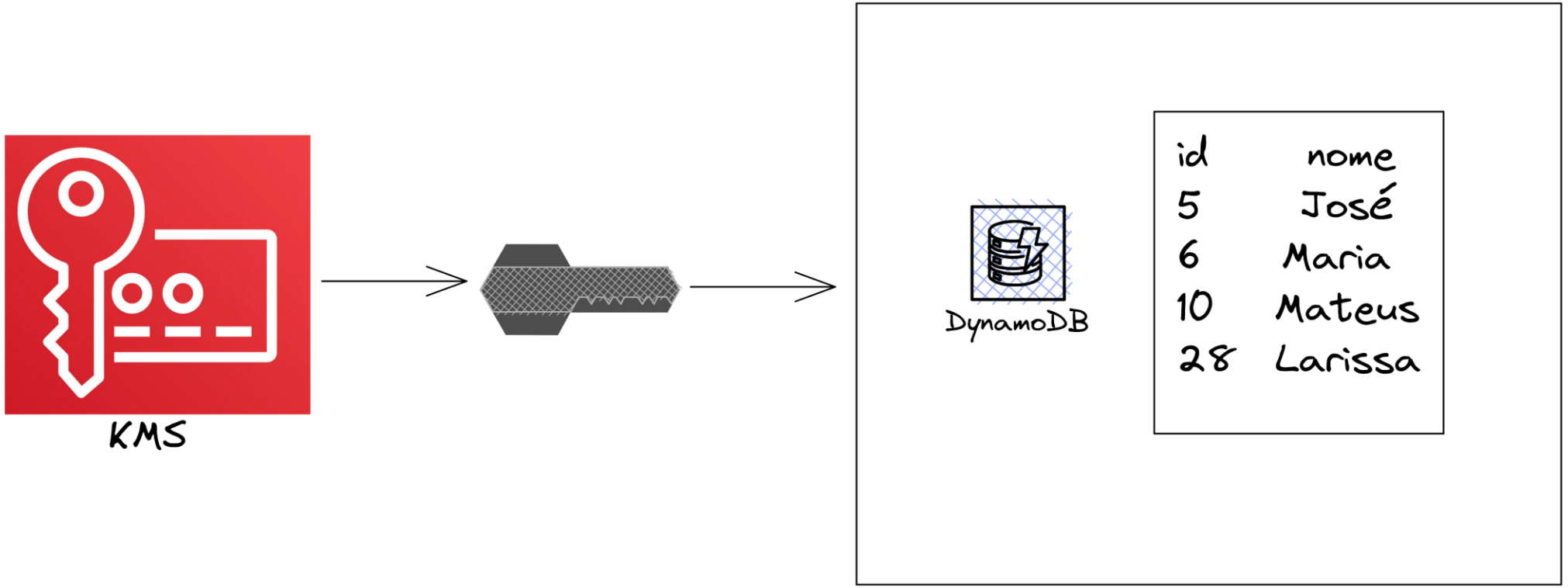
Informações que queremos proteger

- Repouso: Dados em um volume EBS, em *buckets* S3
- Trânsito: Dados que estão sendo enviados de uma origem para um destino

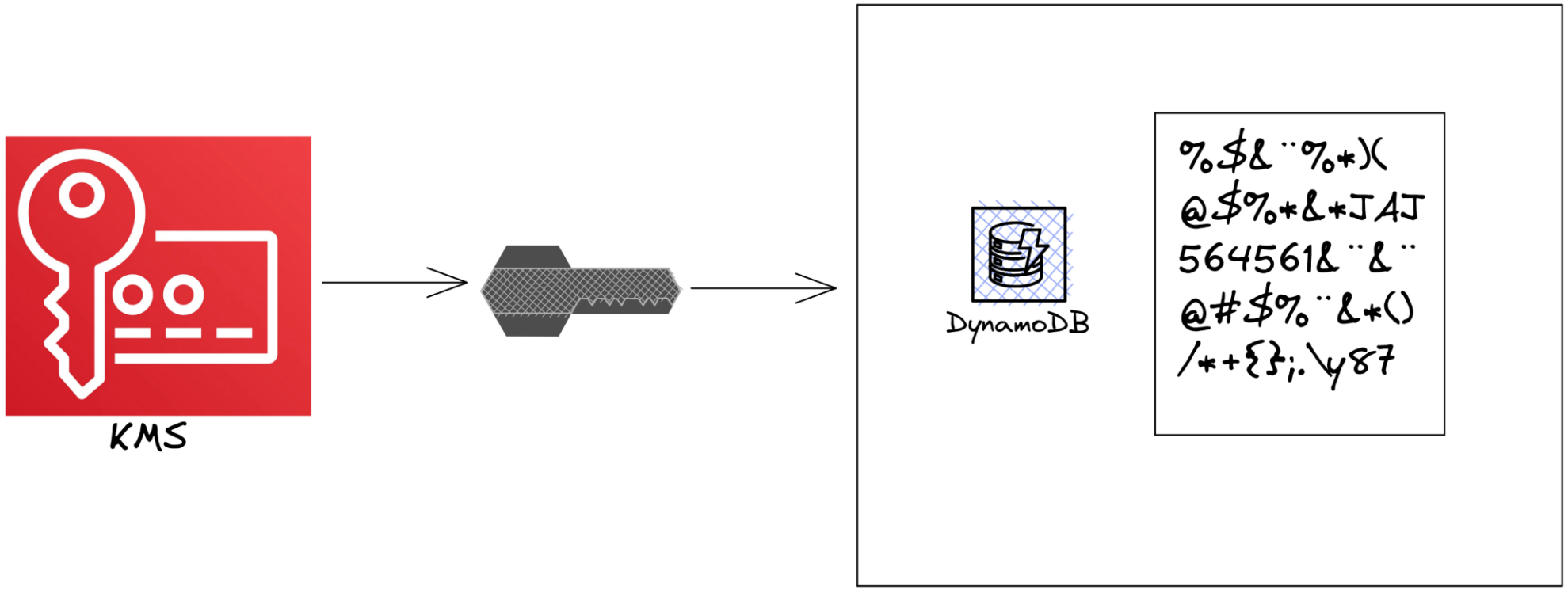
AWS Key Management Service

- KMS
- Gerenciado
- Gestão e controle de chaves criptográficas
- Controle de acesso e autorização

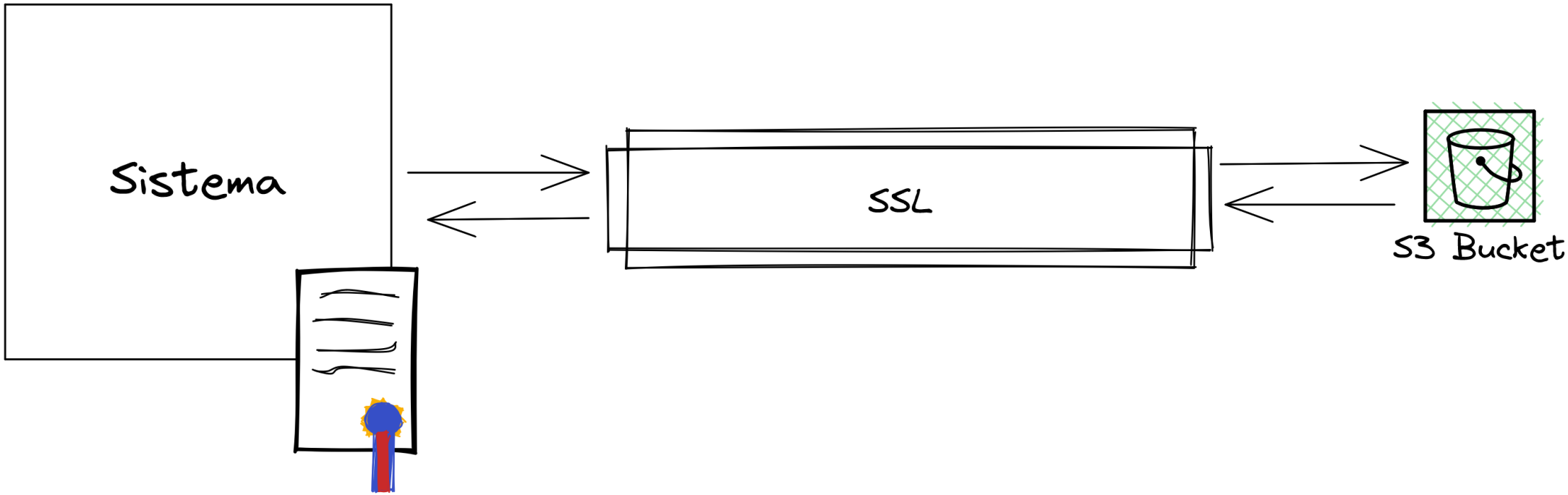
Criptografia em repouso com KMS



Criptografia em repouso com KMS



Criptografia em trânsito com KMS



Para saber mais

- https://aws.amazon.com/pt/what-is/cryptography/
- https://aws.amazon.com/pt/kms/
- https://aws.amazon.com/pt/kms/features/

Dúvidas?

> Fórum/Artigos

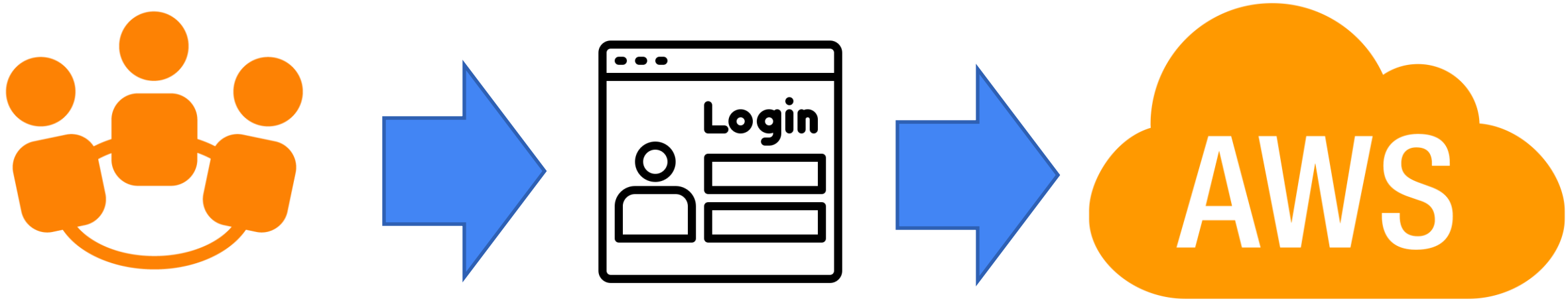
> Comunidade Online (Discord)

SCAN ME

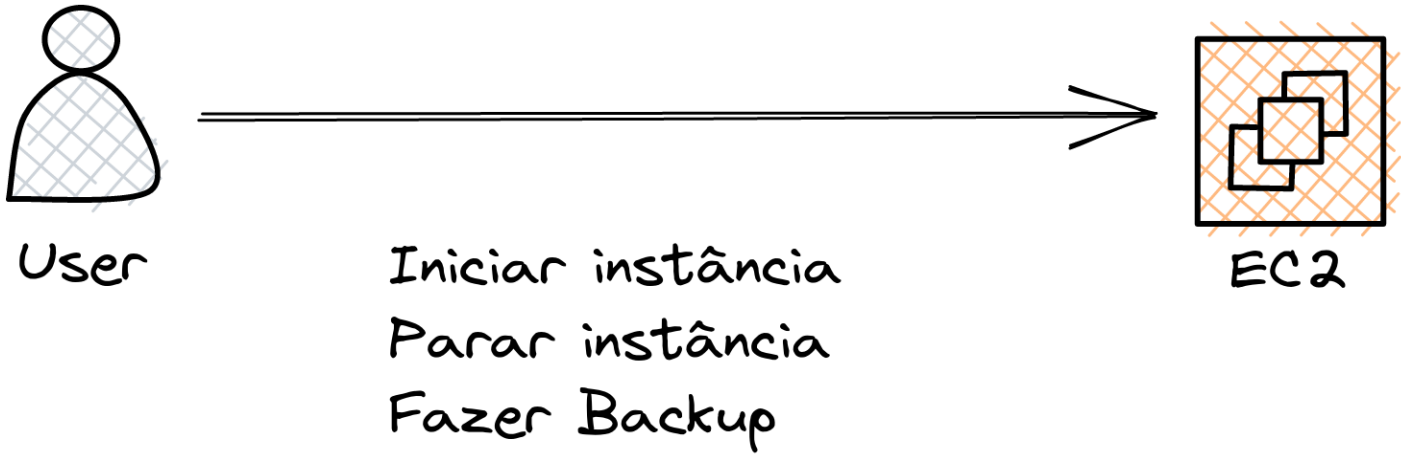
Etapa 3

Gerenciamento de acessos

Precisamos falar sobre acessos



É necessário entender que



AWS Identity and Access Management

AWS IAM

- Serviço disponibilizado gratuitamente
- Gerenciamento de acessos e identidades

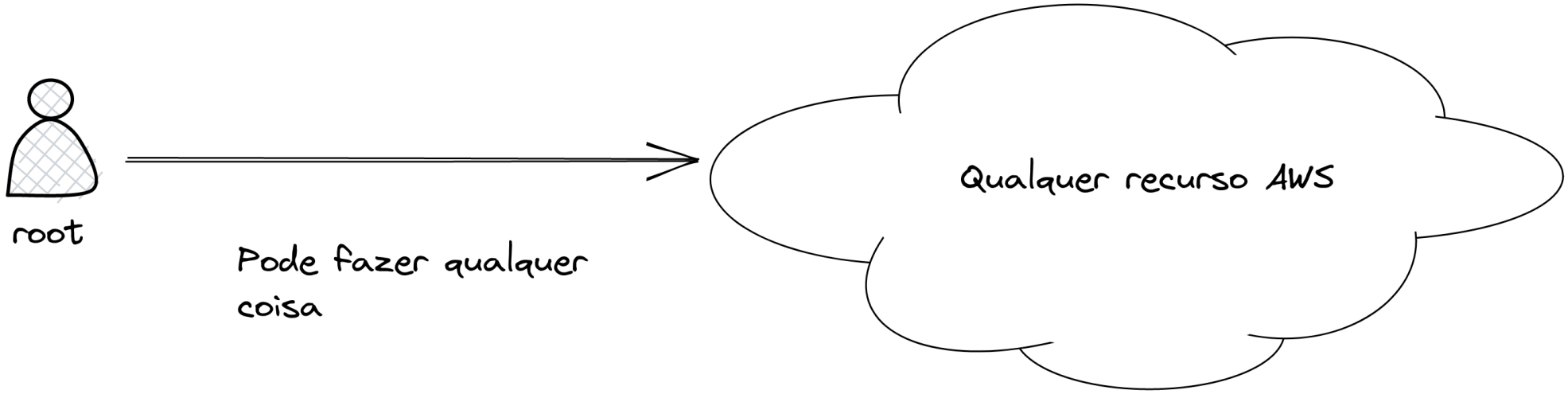
Recursos

- Criação de Usuários, grupos, políticas e roles
- Ativação de MFA
- Definir políticas de senha
- Suporte a federação

Usuários

- Representa uma identidade criada na AWS
- Pode ser uma pessoa ou aplicação
- Composto por nomes e credenciais
- Conceito do privilégio mínimo

Tudo começa com usuário root

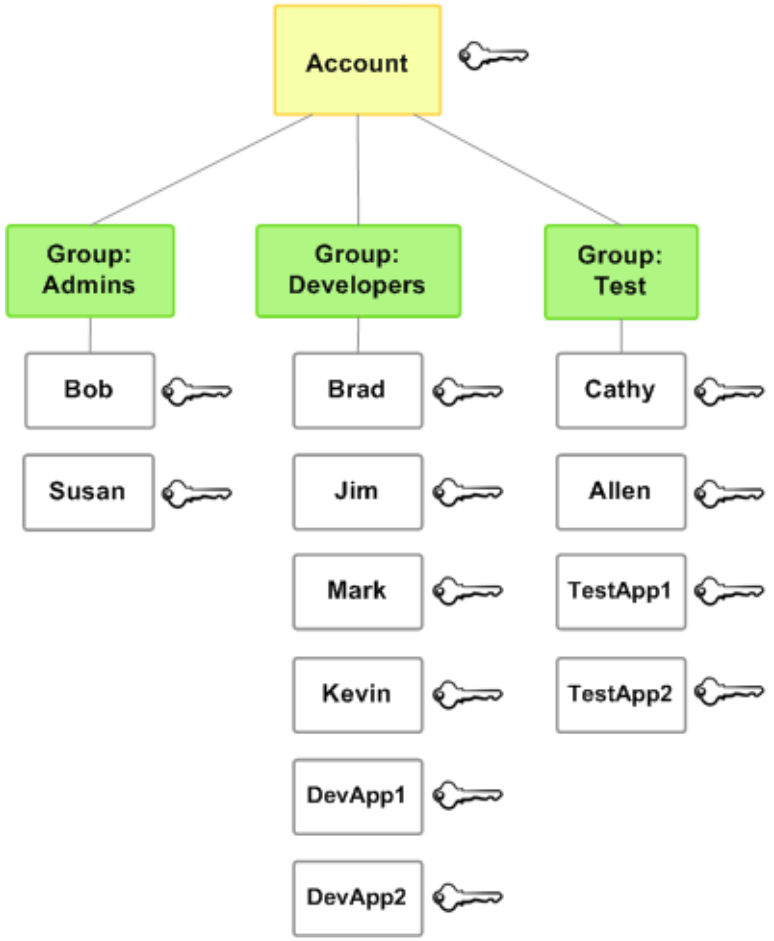


Recomendações

- Não utilize o usuário root
- MFA

Grupos

- Conjunto de usuários IAM
- Permite especificar várias permissões
- Um usuário pode pertencer a vários grupos
- Não podem ser aninhados



Políticas IAM

- Criadas e anexadas as identidades IAM ou a recursos
- É um objeto que define as permissões
- São armazenadas na AWS como documentos JSON
- Alto nível de granularidade

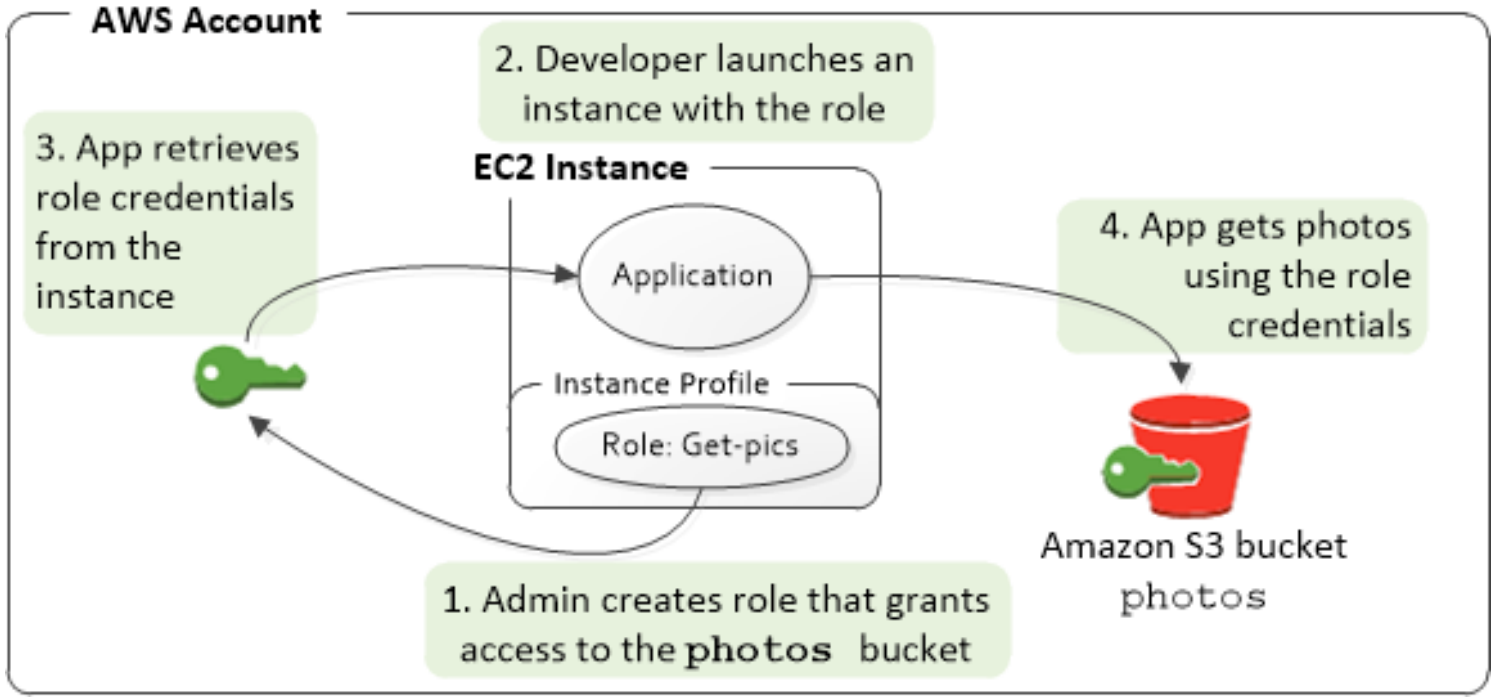
Exemplo

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

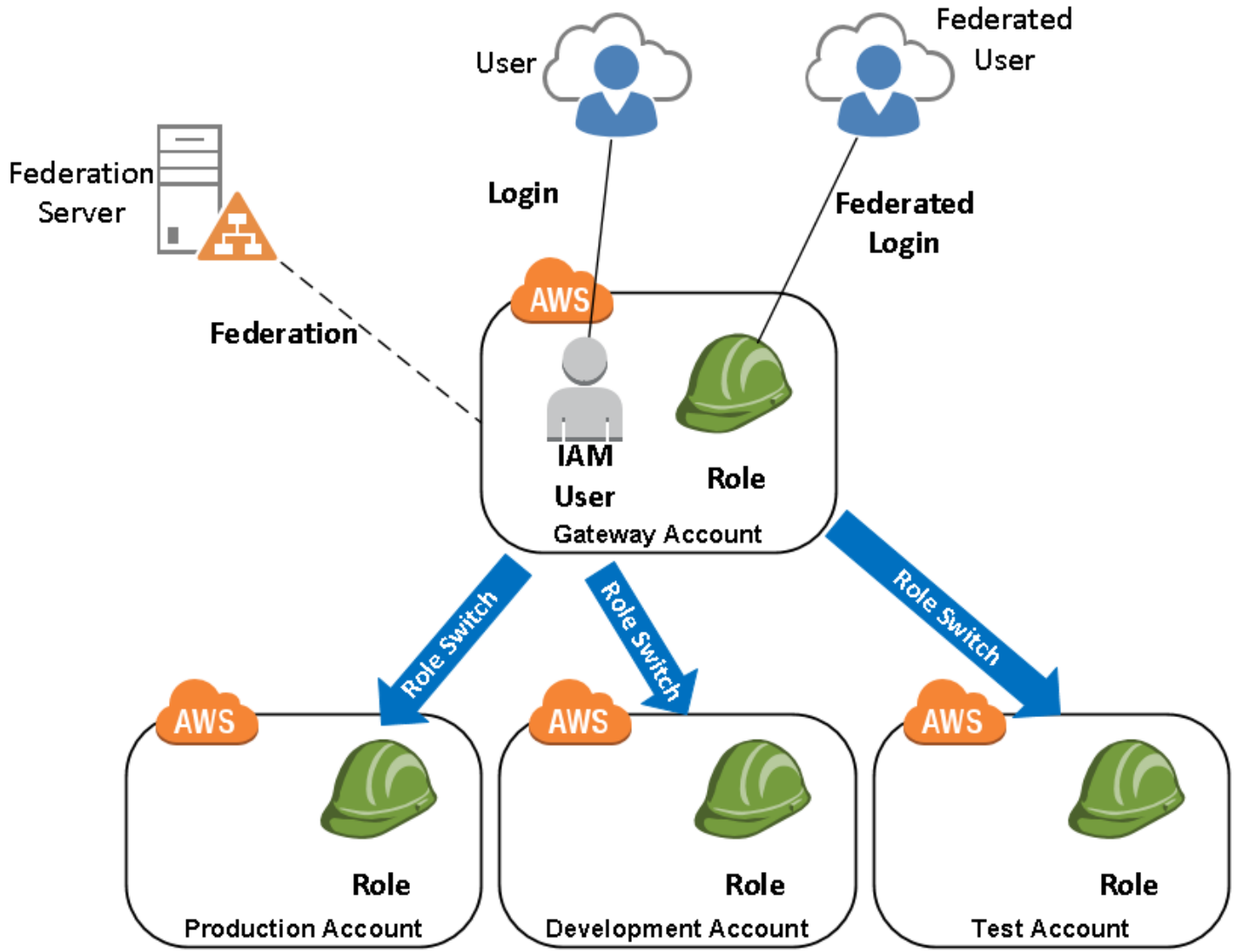
Roles

- Pode ser entendido como uma função, "um chapéu"
- Identidade IAM com permissões específicas
- Semelhante ao usuário, porém é uma identidade que pode ser assumida por vários usuários
- Usuários, aplicativos ou serviços podem utilizar roles

Exemplo


AWS Account
2. Developer launches an instance with the role
3. App retrieves role credentials from the instance
EC2 Instance
Application
Instance Profile
Role: Get-pics
4. App gets photos using the role credentials
Amazon S3 bucket
photos
1. Admin creates role that grants access to the photos bucket

Exemplo


User
Federated User
Federation Server
Login
Federated Login
Federation
AWS
IAM User
Role
Gateway Account
Role Switch
Role Switch
Role Switch
AWS
Role
Production Account
AWS
Role
Development Account
AWS
Role
Test Account

Para saber mais

- Página do produto - https://aws.amazon.com/pt/iam/
- https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/id_root-user.html
- https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/id_users.html
- Como funciona o IAM - https://www.youtube.com/watch?v=m9O8FwYnduA

Para saber mais

- https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/id_groups.html
- https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/access_policies.html
- https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/id_roles.html

Dúvidas?

> Fórum/Artigos

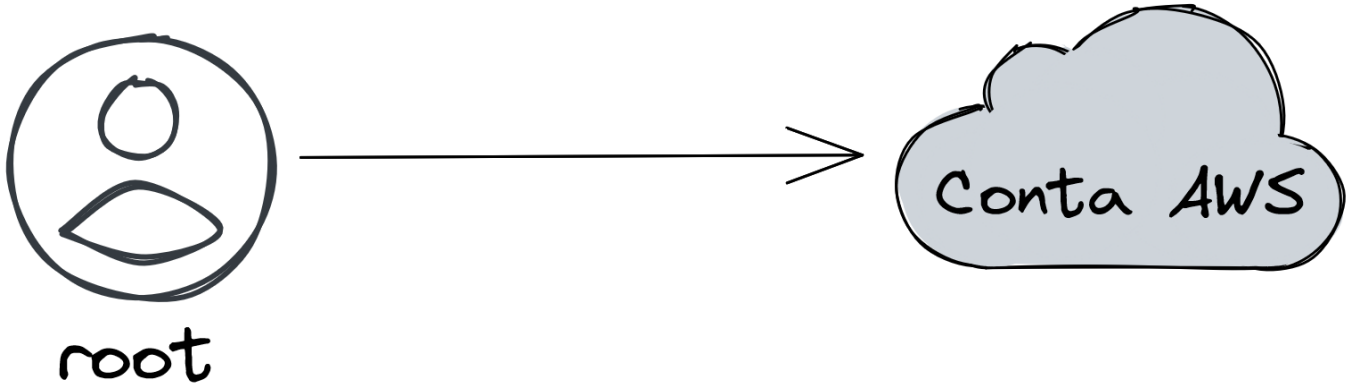
> Comunidade Online (Discord)

SCAN ME

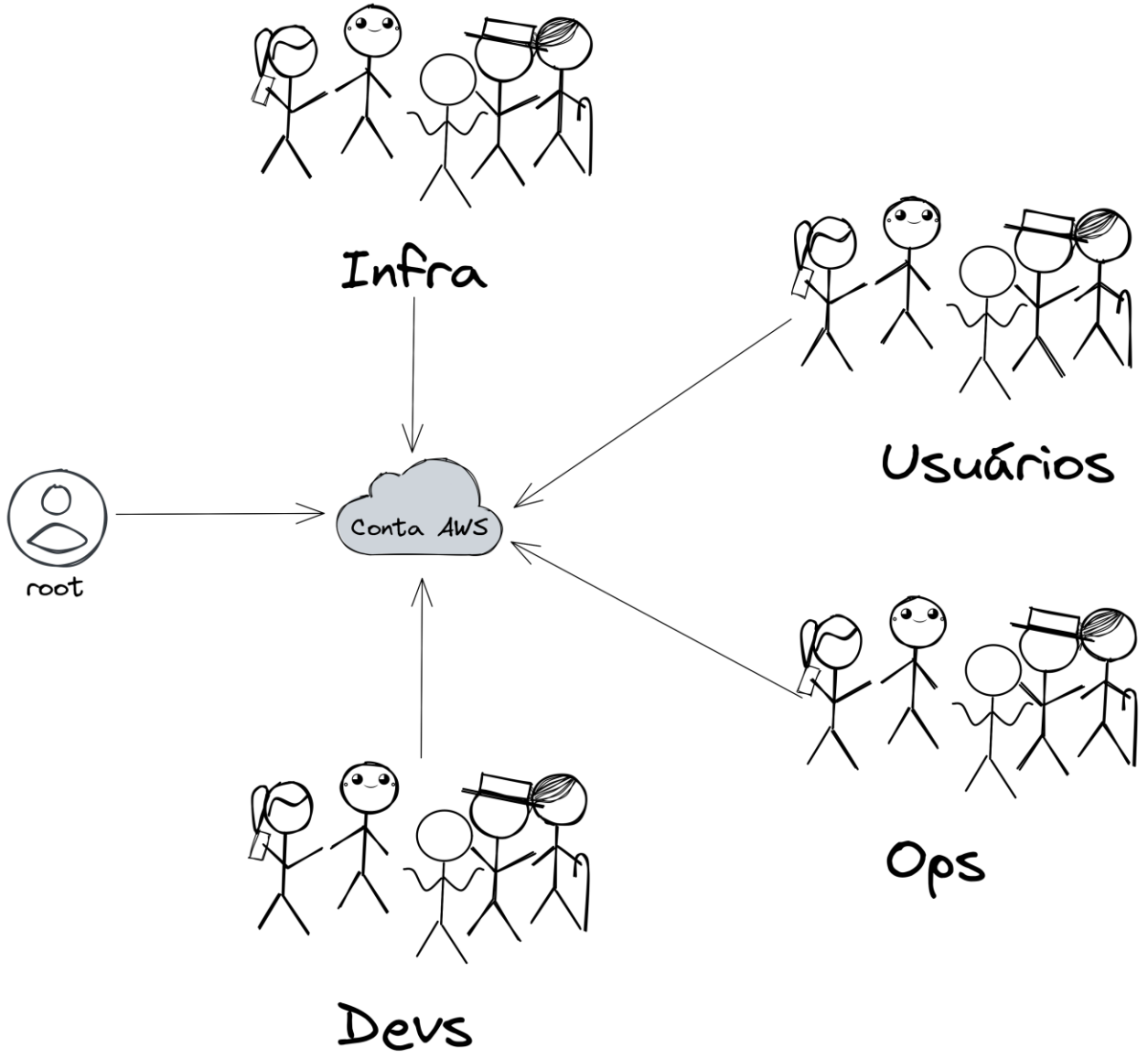
Etapa 4

AWS Organizations

Tudo começa com uma conta AWS



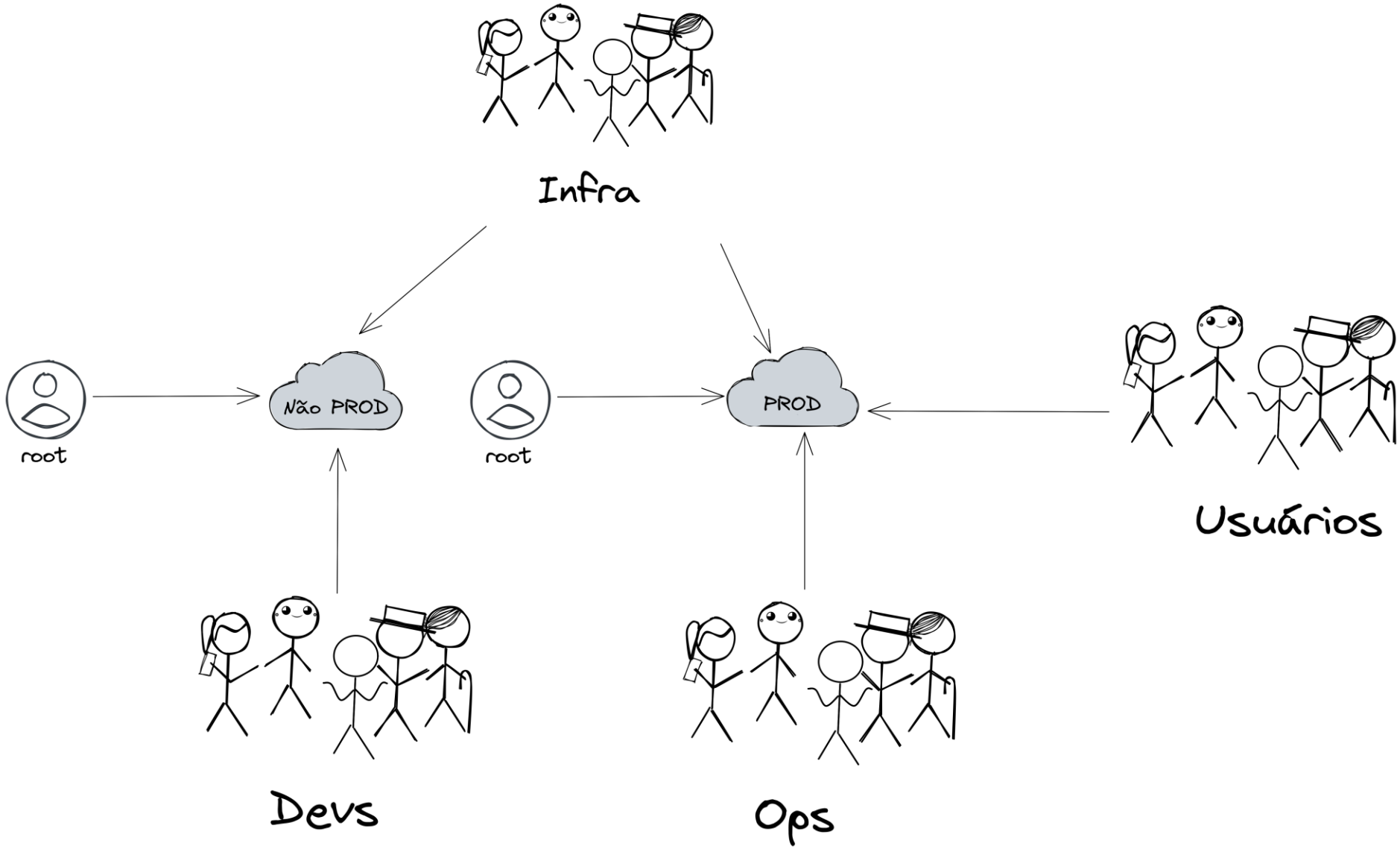
Mais e mais usuários



Problemas que podem surgir

- Dificuldade em gerenciar custos
- Soft e hard limits na AWS

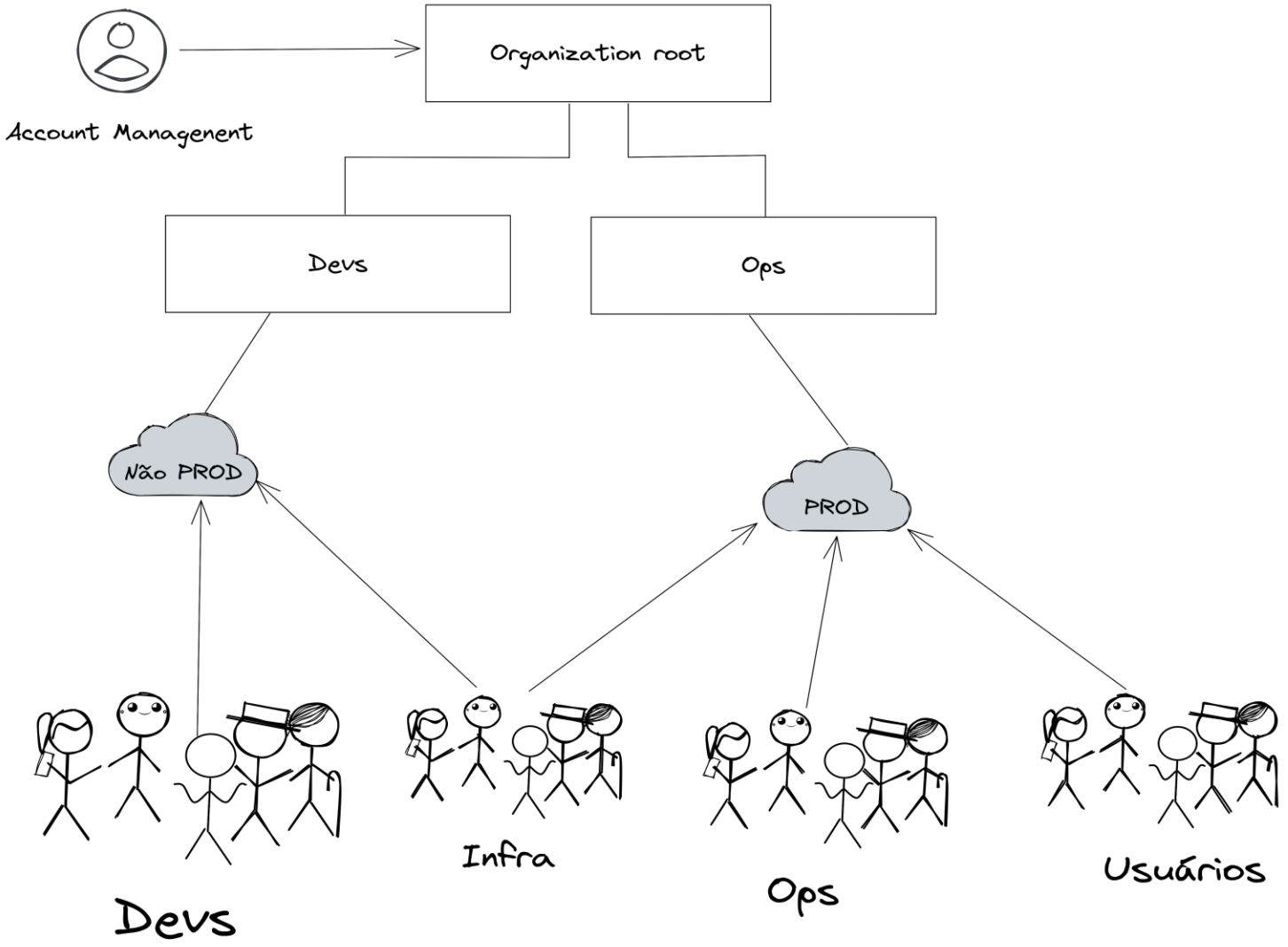
Separando contas



Tá quase legal!

- Dificuldade em gerenciar custos
- ~~Soft e hard limits na AWS~~

AWS Organizations



AWS Organizations

- Serviço gratuito
- Gerenciamento centralizado de contas
- Faturamento Consolidado
- Agrupamento hierárquicos
- Possibilita utilizar políticas de controle de serviço (SCPs)

Para saber mais

- https://docs.aws.amazon.com/pt_br/organizations/latest/userguide/orgs_introduction.html
- https://www.youtube.com/watch?v=DkasgrLCKAk

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

SCAN ME

Etapa 5

Conformidade e suporte

Seu negócio pode passar por uma auditoria

Para cada área, existe uma regulação

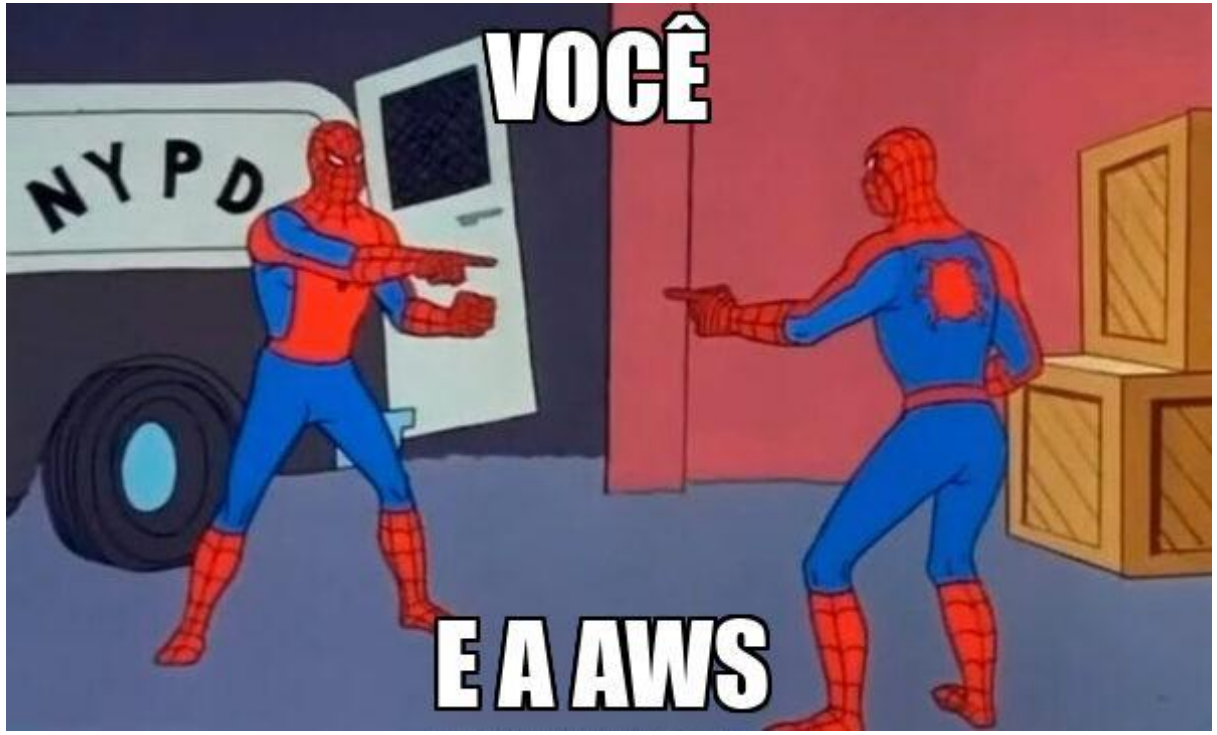
LGPD
Lei Geral de Proteção
de Dados Pessoais

HIPAA

FINTECH

Quem é responsável pela conformidade?

Resposta



Conformidade é responsabilidade compartilhada!

AWS Artifact

AWS Artifact

- AWS Artifact Agreements
- AWS Artifact Reports

Para saber mais

- Página de Conformidade - https://aws.amazon.com/pt/compliance/
- Certificações que a AWS está em conformidade - https://aws.amazon.com/pt/compliance/programs/
- AWS Artifact - https://aws.amazon.com/artifact/
- Centro de Conformidade - https://aws.amazon.com/compliance/customer-center/
- Para que serve o AWS Artifact - https://www.youtube.com/watch?v=WXCBsZhPOyY

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

SCAN ME

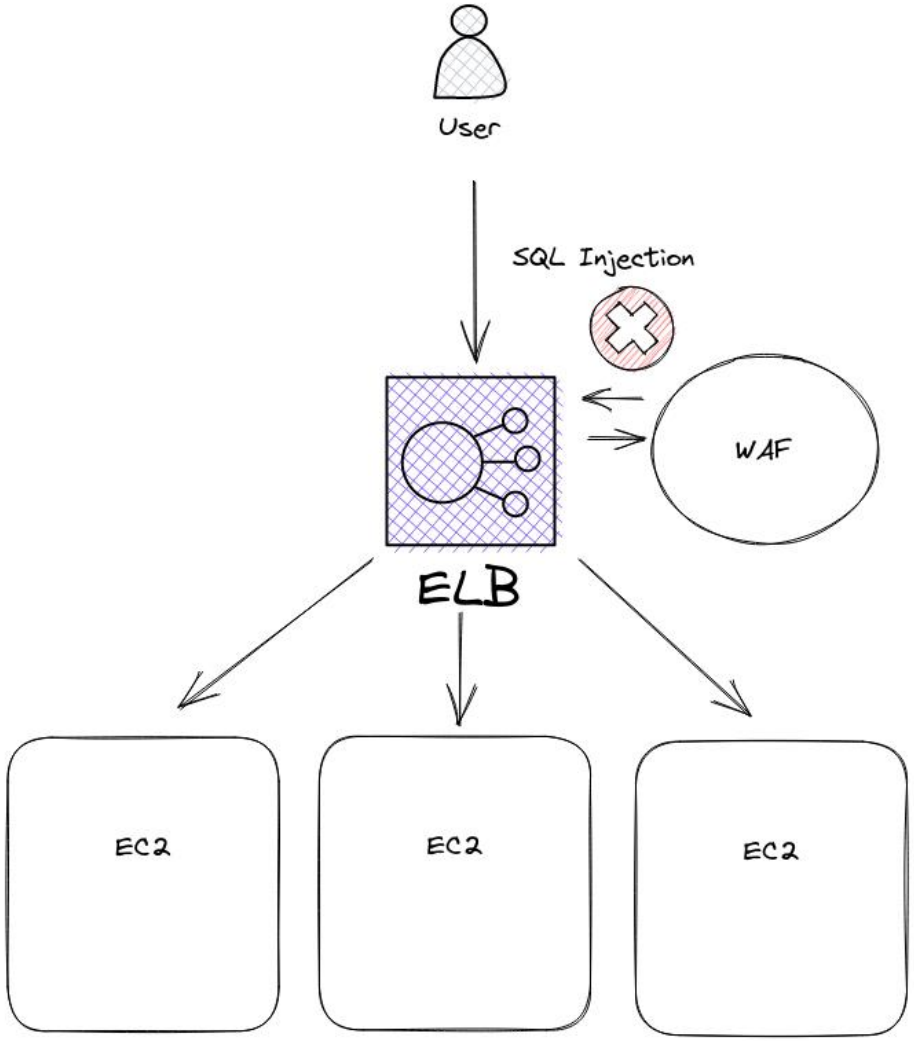
Etapa 6

Serviços adicionais

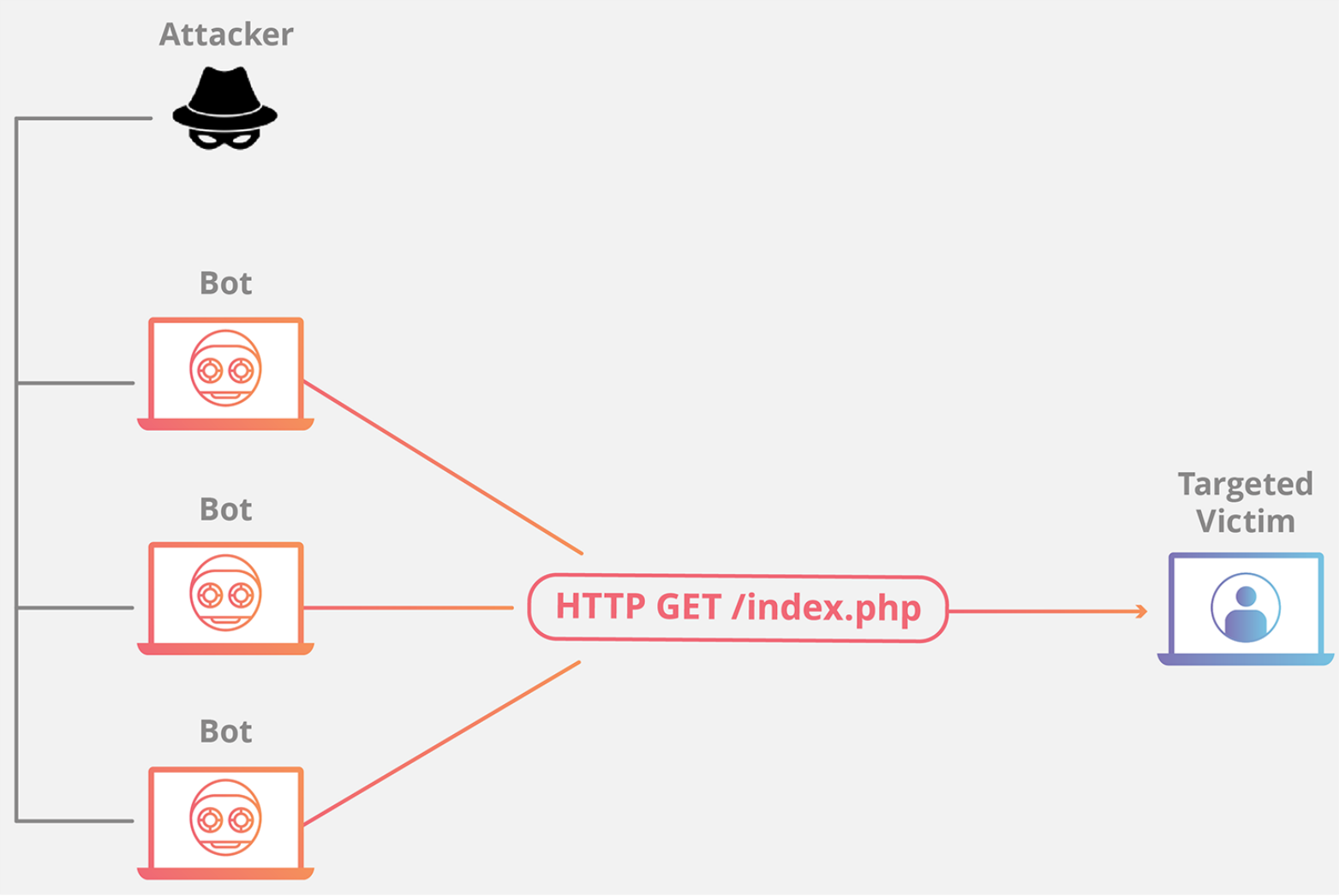
AWS WAF

- Web Application Firewall
- Tráfego HTTP/HTTPS
- Gerenciado
- Protege aplicações web contra exploits, como: SQL Injection, Cross-site scripting
- Regras default e customizadas
- Integra nativo com serviços AWS como: ELB, EC2,API Gateway

AWS WAF



Ataques DDoS



AWS Shield

- Serviço gerenciado de proteção contra DDoS para proteger aplicações que rodam na AWS
- Categoria Standard e Advanced

AWS Shield Standard

- Sem custo adicional
- Proteção contra ataques DDoS mais comuns
- Usa técnicas de análise para detectar tráfego mal intencionado em tempo real

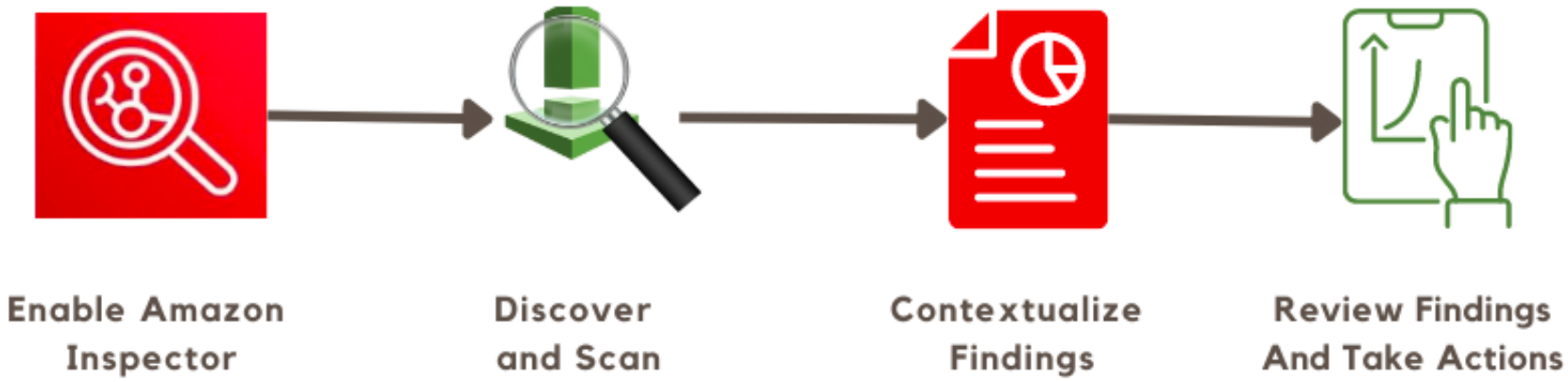
AWS Shield Advanced

- Serviço pago
- Fornece diagnósticos detalhados de ataques
- Fornece proteção para ataques mais elaborados
- Fornece integração com AWS WAF
- Equipe de suporte

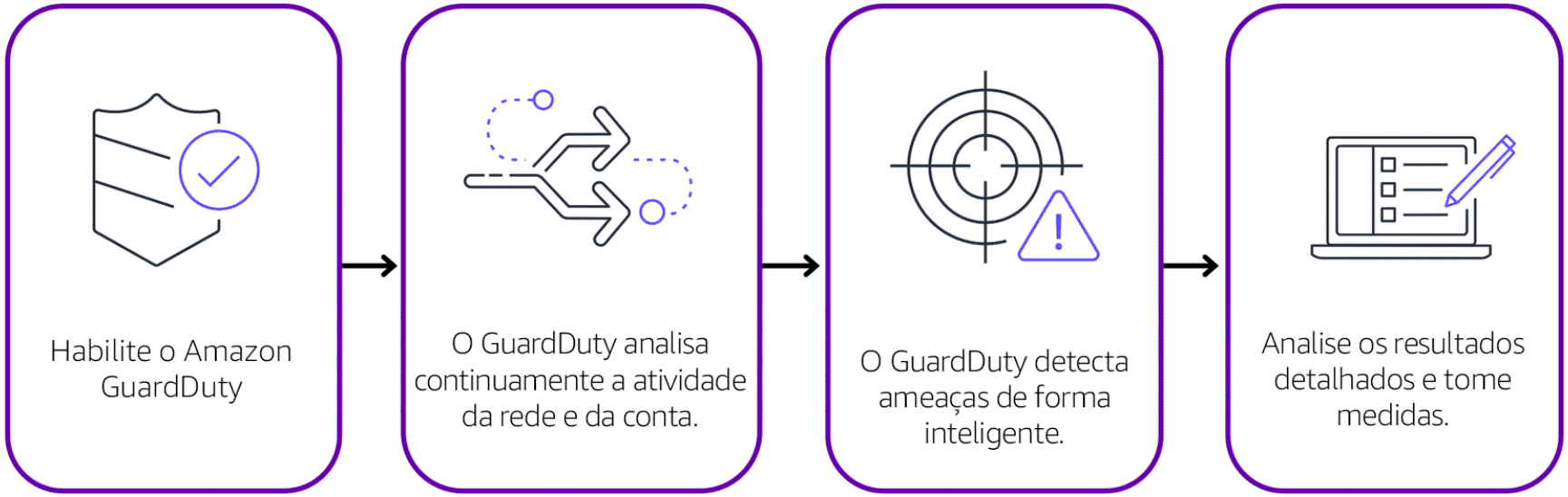
Amazon Inspector

- Ferramenta de segurança
- Serviço gerenciado
- Verifica atualização mediante vulnerabilidades descobertas por CVE, CIS Benchmark
- Ajuda em processos de auditoria

Amazon Inspector



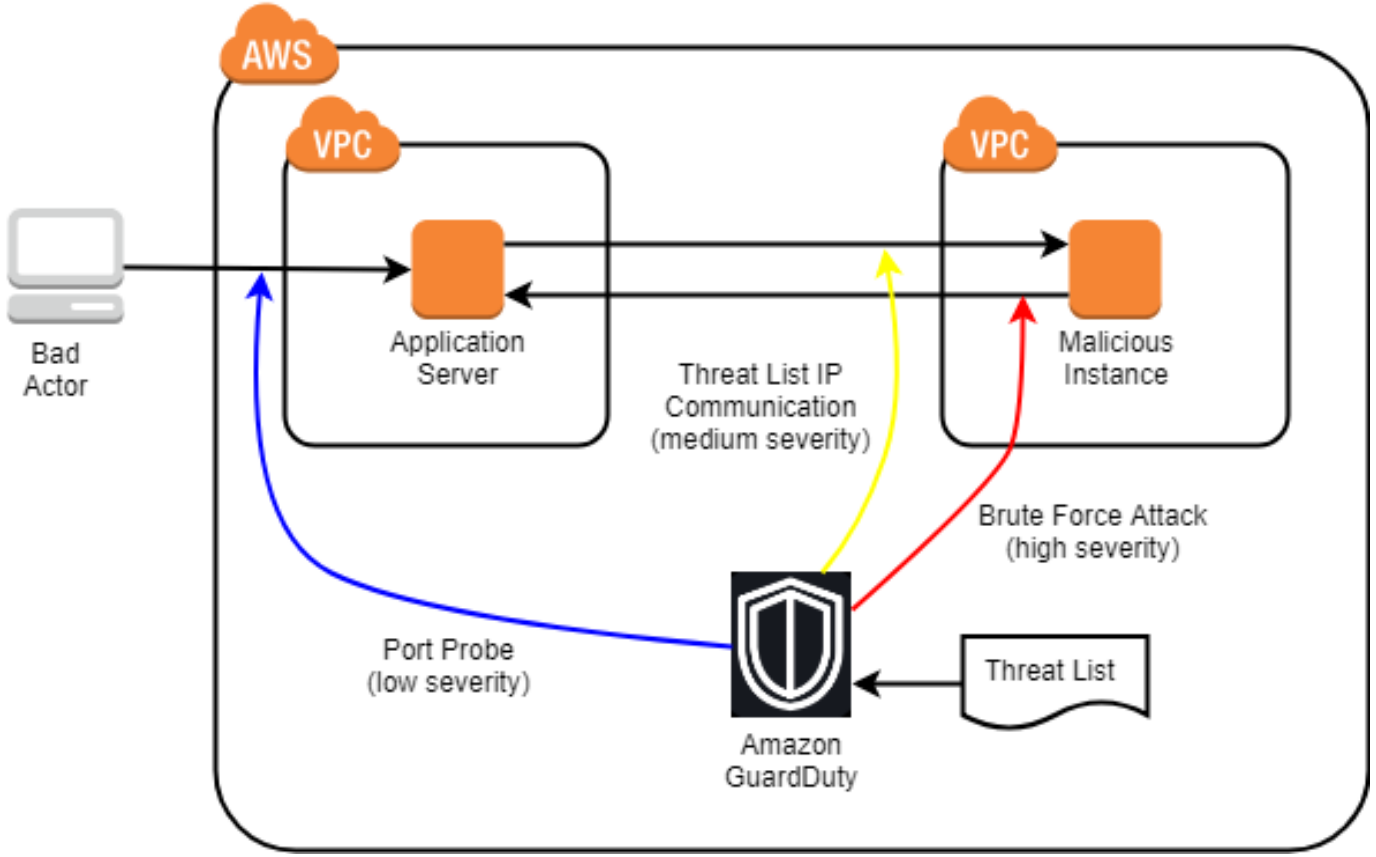
Amazon GuardDuty



Amazon GuardDuty

- Detecção inteligente de ameaças no ambiente AWS
- Analisa e processa diversas fontes de dados para monitorar a infraestrutura
- Fontes: Logs DNS, VPC, Eventos CLoudTrail, registros no S3, dados em volumes EBS, atividades de login do RDS entre outras
- Usa Machine Learning para prever atividades inesperadas

Amazon GuardDuty



Para saber mais

- **AWS Shield - https://aws.amazon.com/pt/shield/**
- **AWS WAF - https://aws.amazon.com/pt/waf/**
- **Amazon Inspector - https://aws.amazon.com/inspector/**
- **O que é Amazon Inspector - https://www.youtube.com/watch?v=wlQmeyZrYJk**
- **Amazon GuardDuty - https://docs.aws.amazon.com/pt_br/guardduty/latest/ug/what-is-guardduty.html**

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

SCAN ME