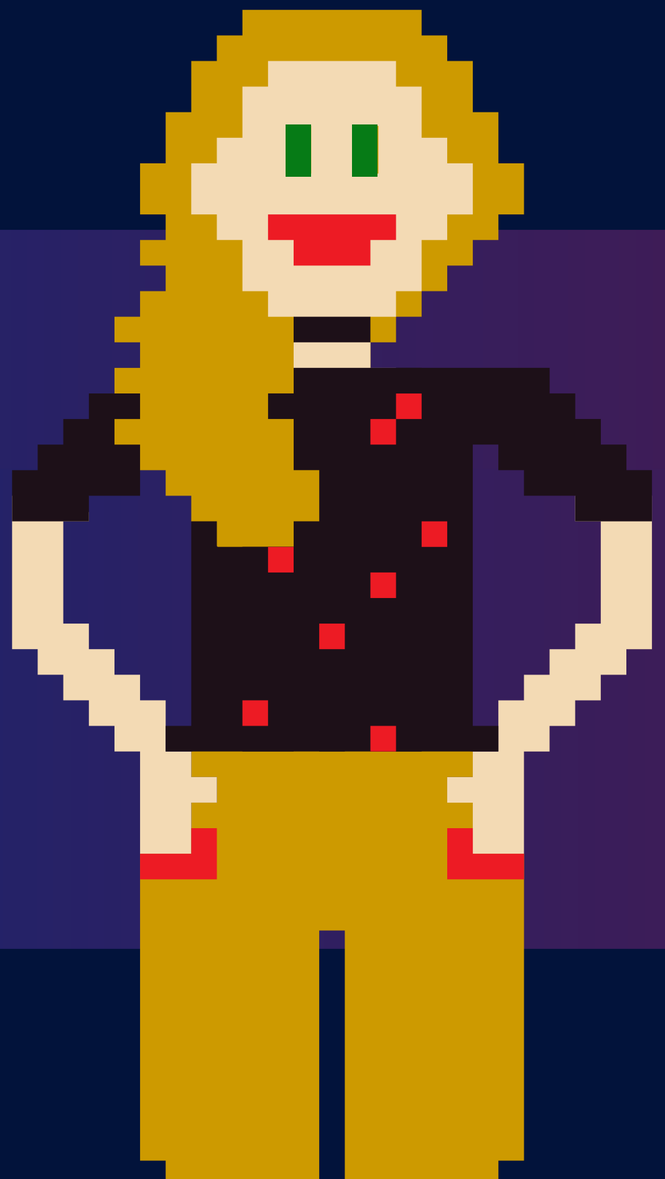
DESMISTIFICANDO O IAM

QUEM SOU EU?



PALOMA

ROCAMBOLE

REFERÊNCIAS

Leandro Damascena

@LeoCDamascena

RELEVÂNCIA

1BI DE CHAMADAS POR SEGUNDO

O QUE É O IAM?

- Conceito global, não veio da AWS
- Controle de autenticação e autorização
- Suporte a usuários, grupos, roles, MFA, politicas de permissão, SSO, etc.
- Firewall do seu ACESSO

MODELO DE POLÍTICA

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1687378695333",
      "Action": "ec2:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:SourceIp": "172.10.10.10"
        }
      }
    }
  ]
}
```

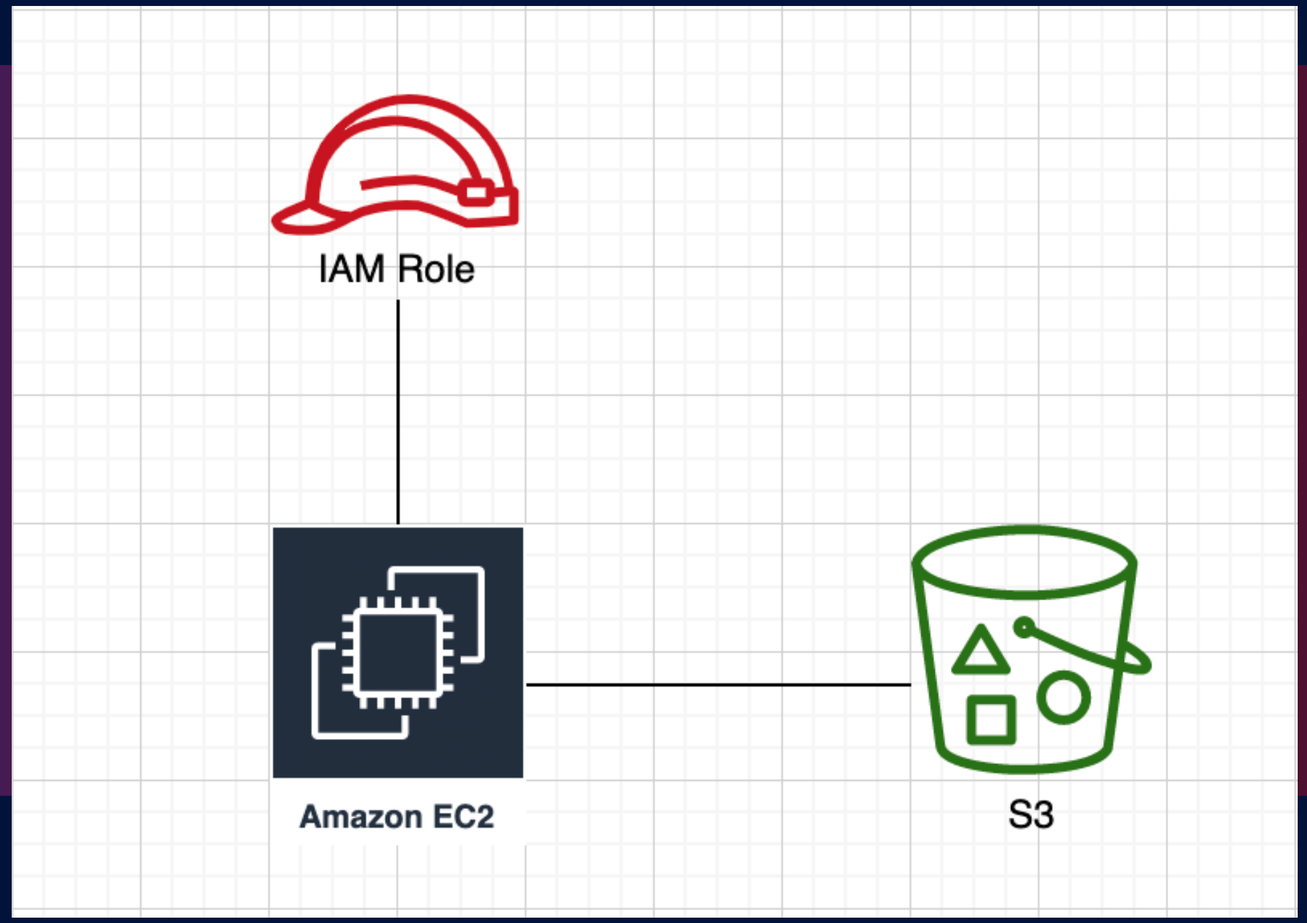
- Version
- Statement
- Sid
- Action
- Effect
- Resource
- Condition

MODELO DE POLÍTICA

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1687378695333",
      "Action": "ec2:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:SourceIp": "172.10.10.10"
        }
      }
    }
  ]
}
```

- Negativas de politicas
- AWS PolicyGen

ROLES



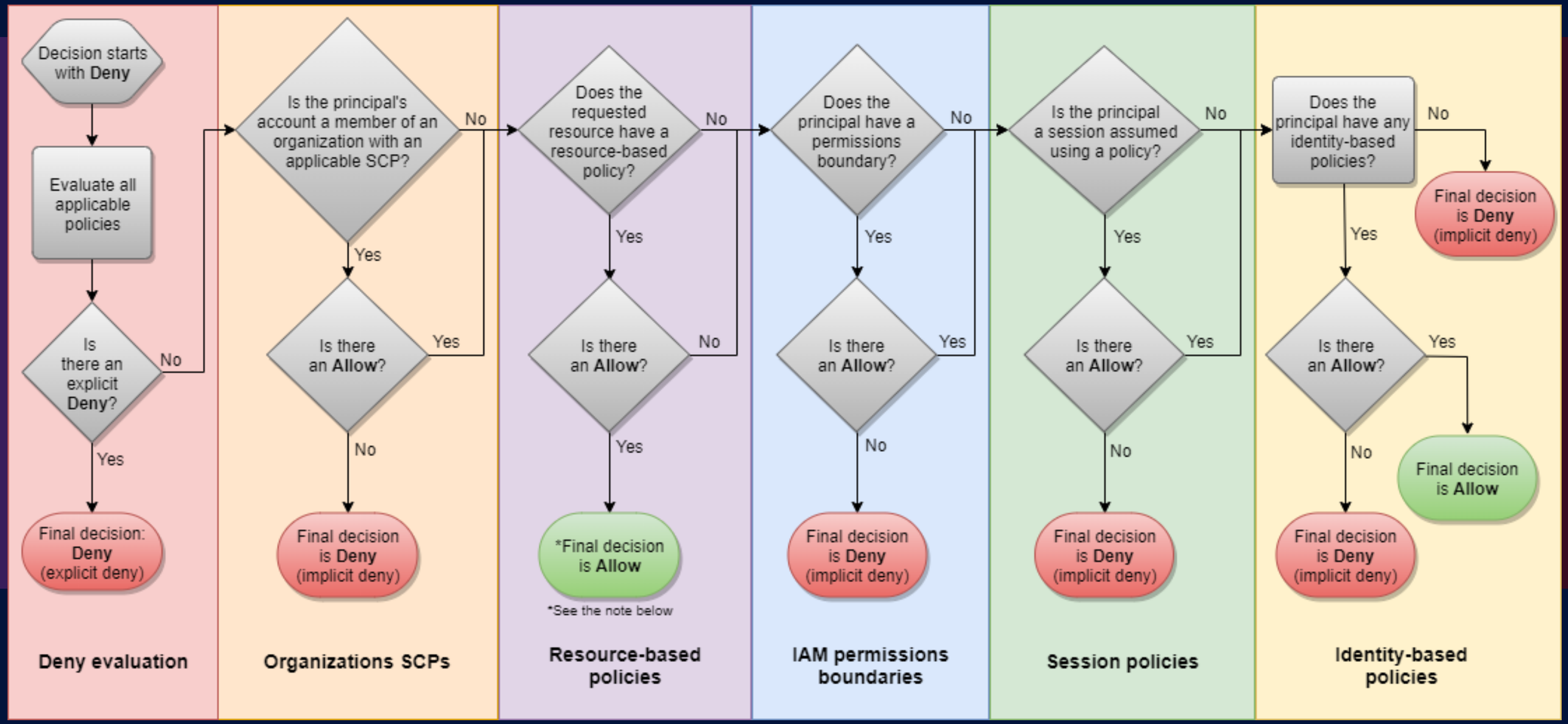
AUTENTICAÇÃO E AUTORIZAÇÃO

Aplicar políticas

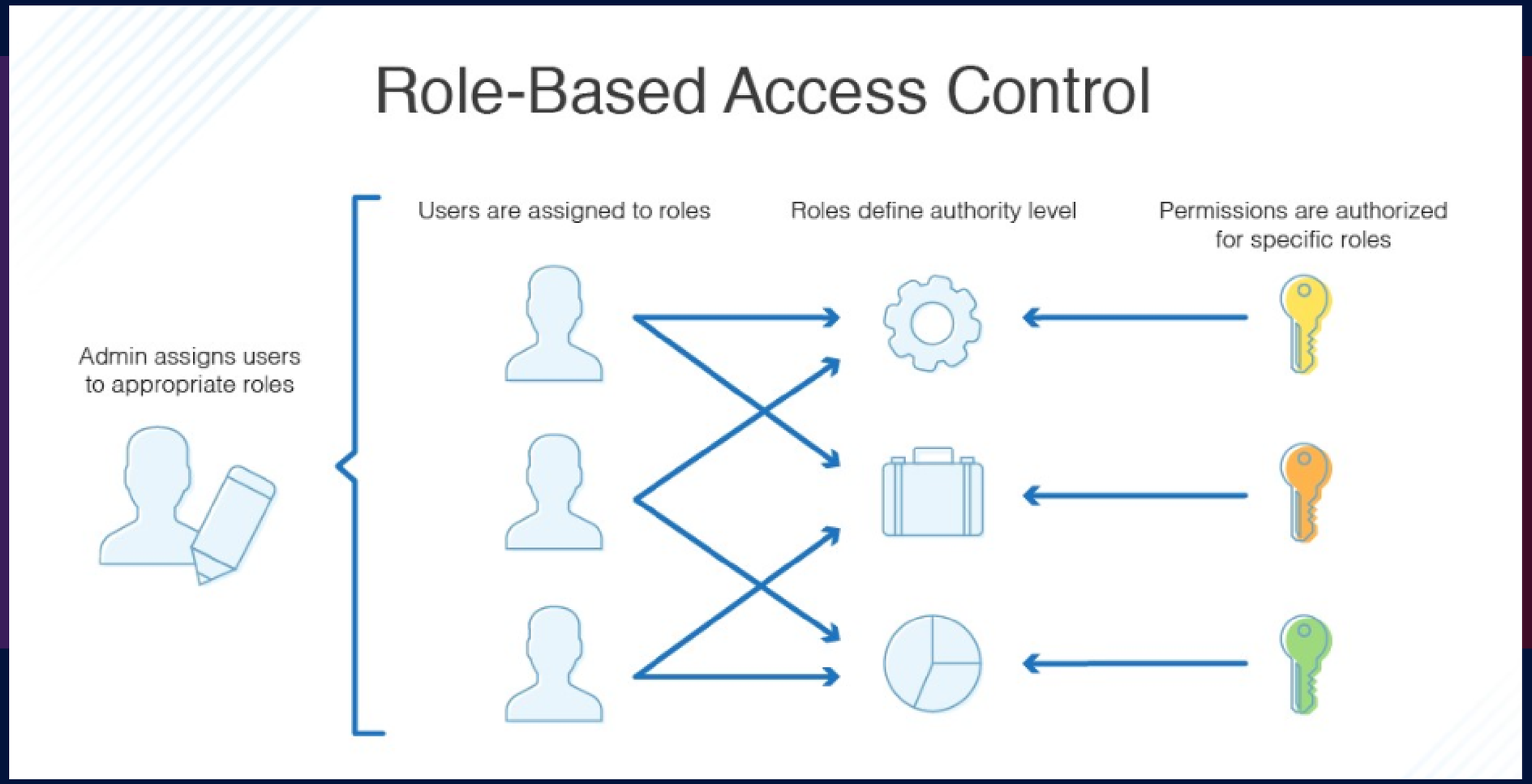
Analisar políticas

Decisão

LÓGICA DA AVALIAÇÃO DA POLÍTICA

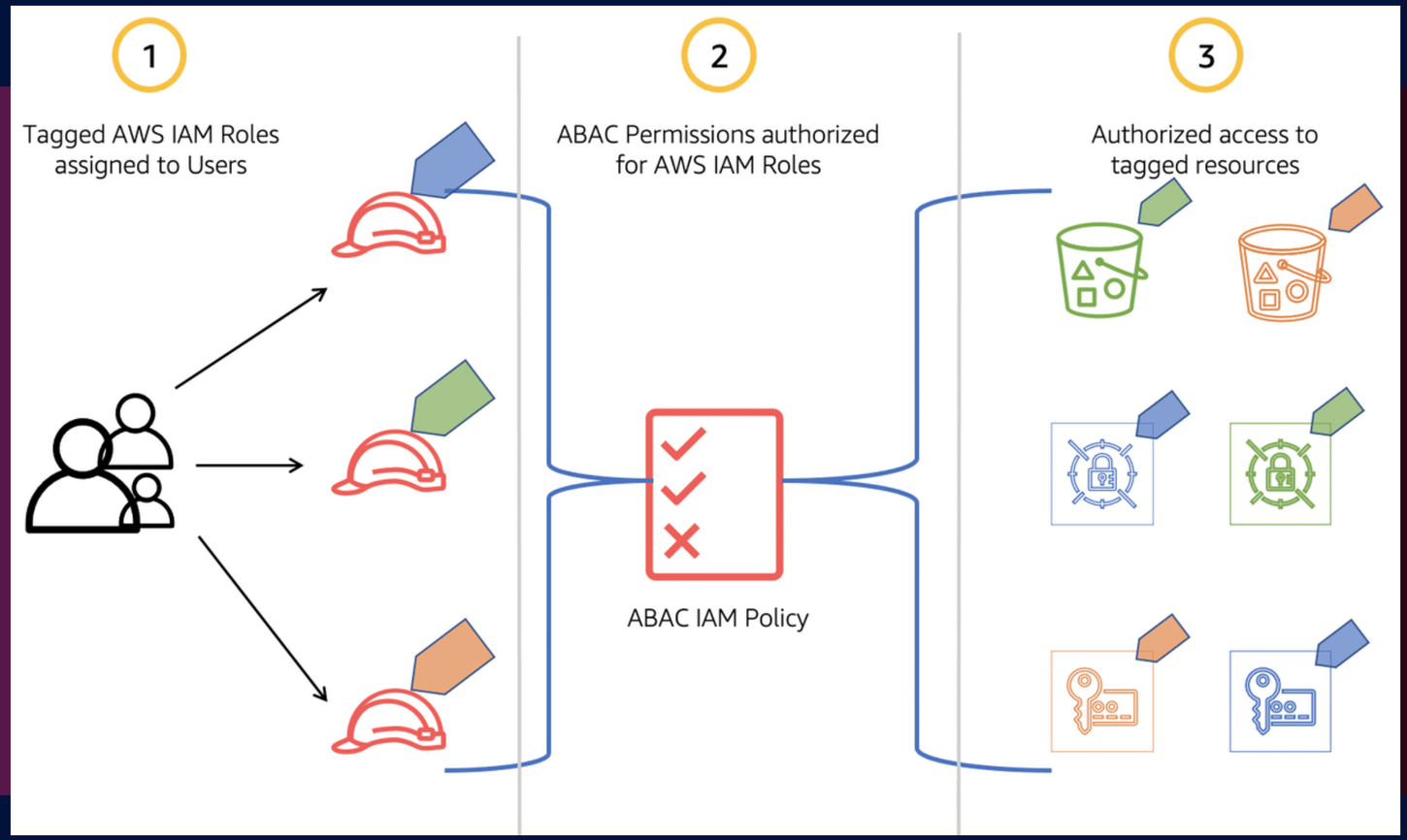


MODELO TRADICIONAL - RBAC

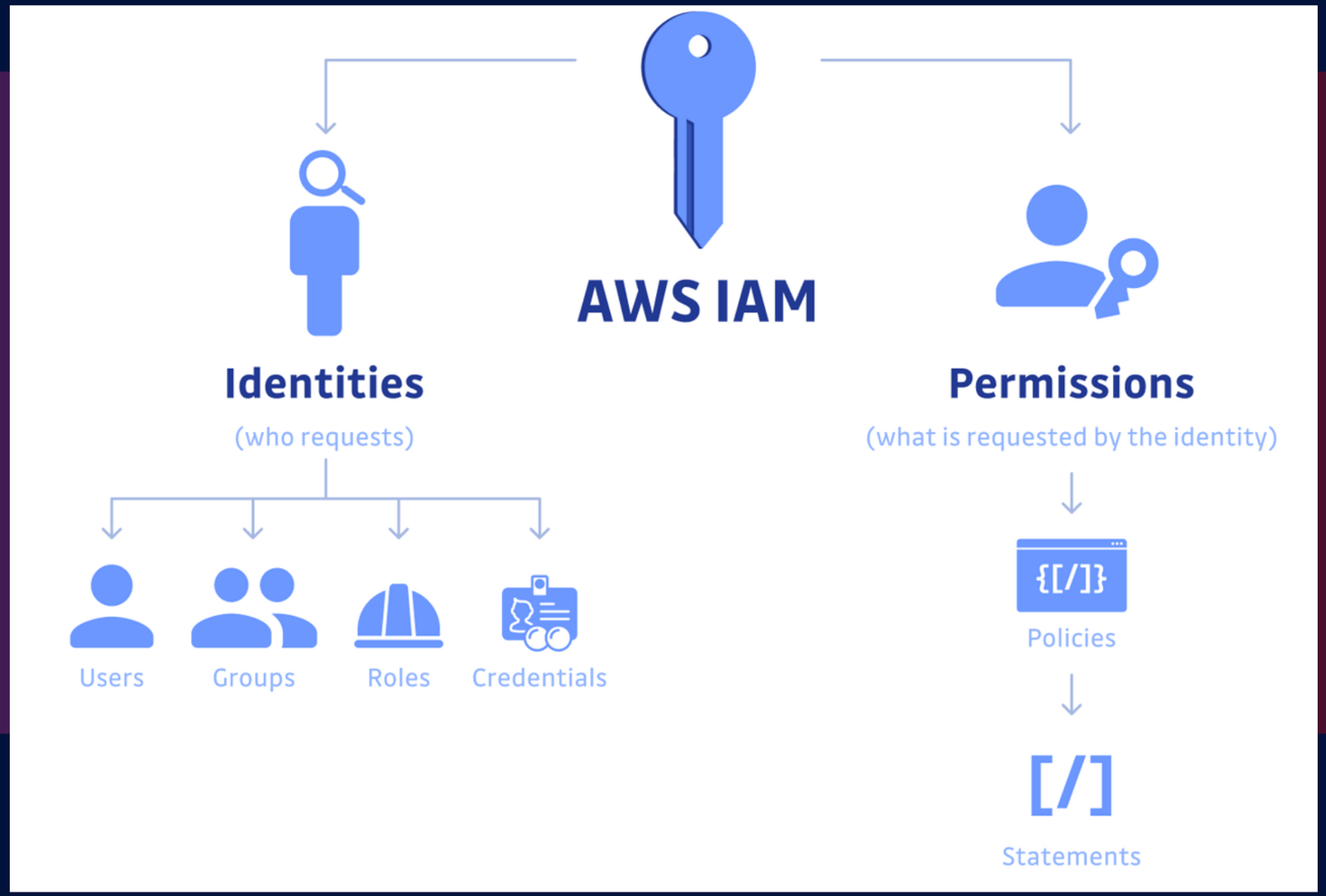


MODELO ESCALÁVEL - ABAC

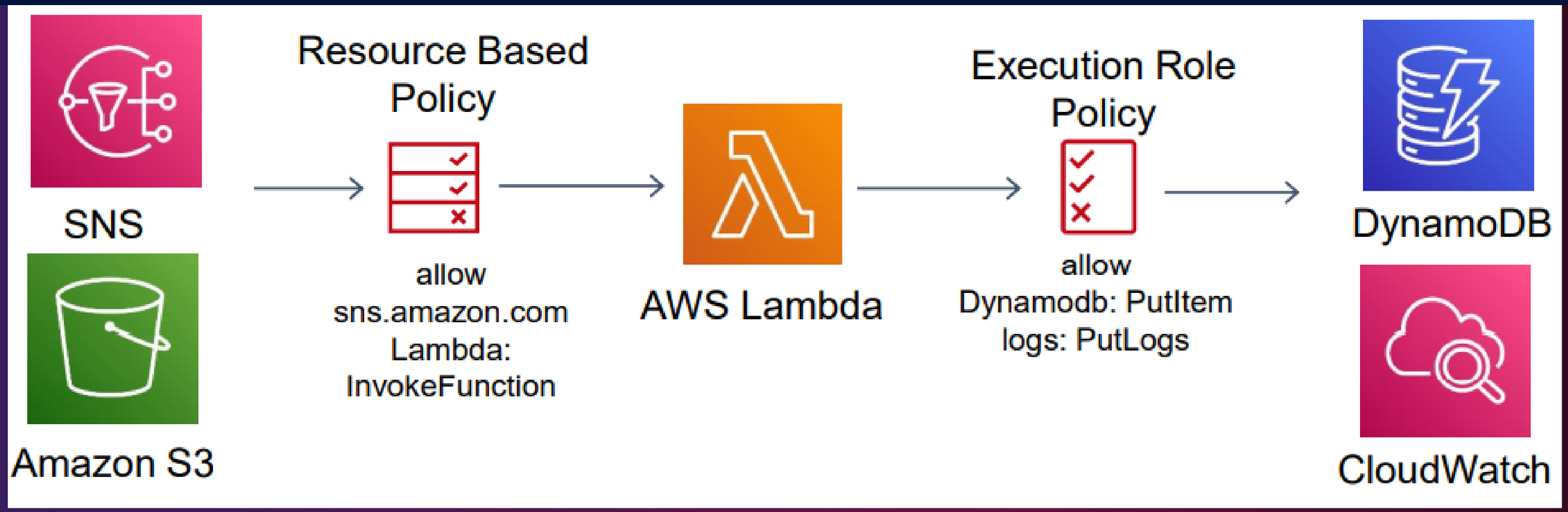
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalTag/Department": "Development",
                    "aws:ResourceTag/CreatedBy": "${aws:username}"
                }
            }
        }
    ]
}
```



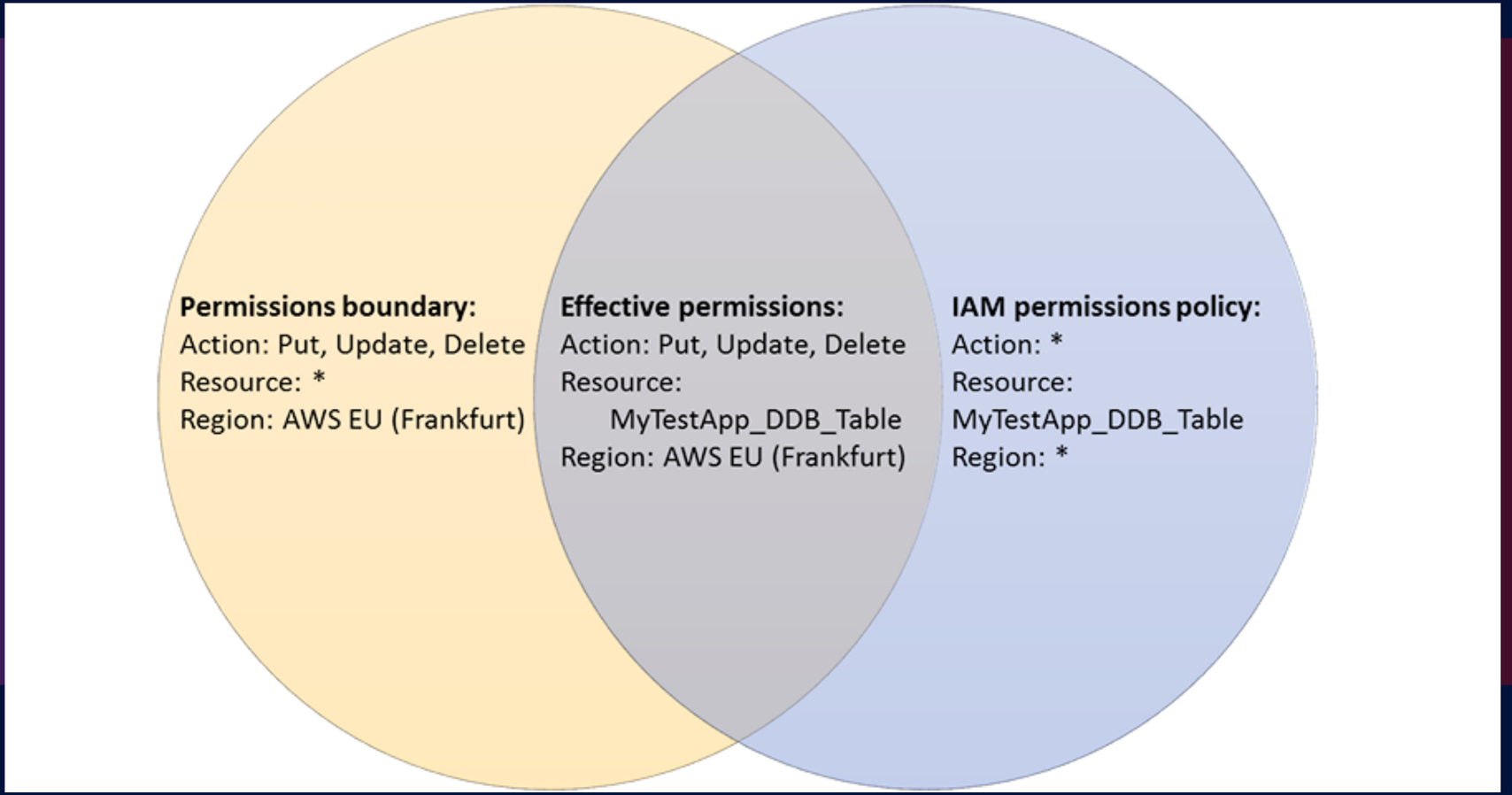
IDENTITY-BASED POLICY



RESOURCE-BASED POLICY



PERMISSIONS BOUNDARY



BOAS PRÁTICAS

- BLOQUEAR AS CHAVES DE ACESSO DE ROOT ACCOUNT
- CRIAR USUÁRIOS INDIVIDUAIS DO IAM
- UTILIZAR GRUPOS DE USUÁRIOS PARA ATRIBUIR PERMISSÕES A USUÁRIOS DO IAM
- CONCEDER PRIVILÉGIO MÍNIMO
- CONCEITOS BÁSICOS DO USO DE PERMISSÕES COM POLÍTICAS GERENCIADAS PELA AWS
- VALIDAR SUAS POLÍTICAS
- CONFIGURAR UMA POLÍTICA DE SENHA FORTE PARA SEUS USUÁRIOS
- HABILITAR MFA
- USAR FUNÇÕES PARA APLICAÇÕES QUE SÃO EXECUTADAS EM INSTÂNCIAS DO AMAZON EC2
- USAR FUNÇÕES PARA DELEGAR PERMISSÕES
- NÃO COMPARTILHAR AS CHAVES DE ACESSO
- ALTERNAR CREDENCIAIS REGULARMENTE E REMOVER CREDENCIAIS DESNECESSÁRIAS
- USAR CONDIÇÕES DE POLÍTICA PARA SEGURANÇA EXTRA
- MONITORAR ATIVIDADES NA CONTA DA AWS

RELEVÂNCIA

1BI DE CHAMADAS POR SEGUNDO

NO IAM TUDO É PROIBIDO, EXCETO O QUE É LIBERADO!

Paloma Lataliza

@shescloud_