Implantação ambiente de LAB para o DEV Experience

# Objetivo

Implantar ambientes de laboratório para o treinamento Developer Experience na conta da AWS eec-aws-br-eits-devhub-sandbox (071087690196)

Esses ambientes serão designados para grupos formados no treinamento para desenvolver projetos relacionados aos tópicos apresentados

# Premissas

PC:

Evitar que recursos disponibilizados para uma equipe não impactem nos recursos das outras

Não permitir publicação de serviços para Internet ou para a rede SERASA

Possibilitar acesso de qualquer parte da rede SERASA

Possibilitar acesso à Internet para instalação/atualização de serviços

Os serviços da AWS serão provisionados pelos membros das equipes

Avaliar a possibilidade de criação de VPCs distintas para as equipes para segregação de acesso aos recursos provisionados

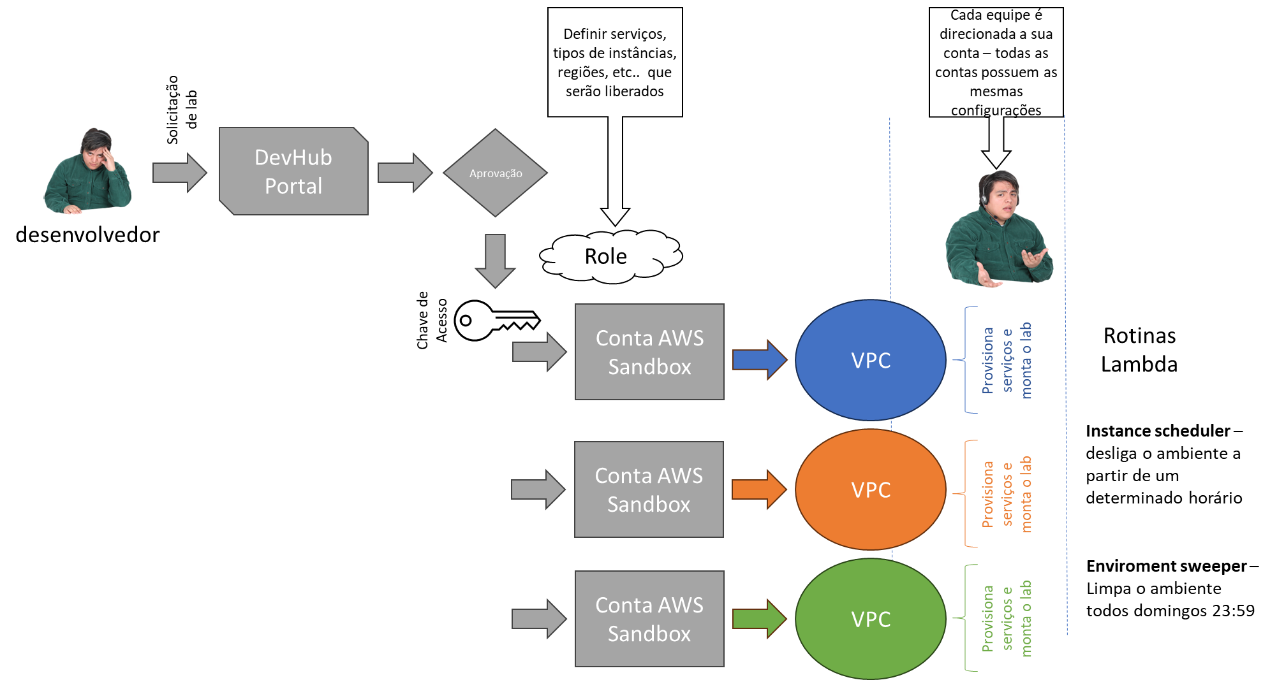
Laura:

Possibilitar a carga de dados de ambientes de UAT para testes com S3, EMR e AirFlow

# Arquitetura técnica da conta

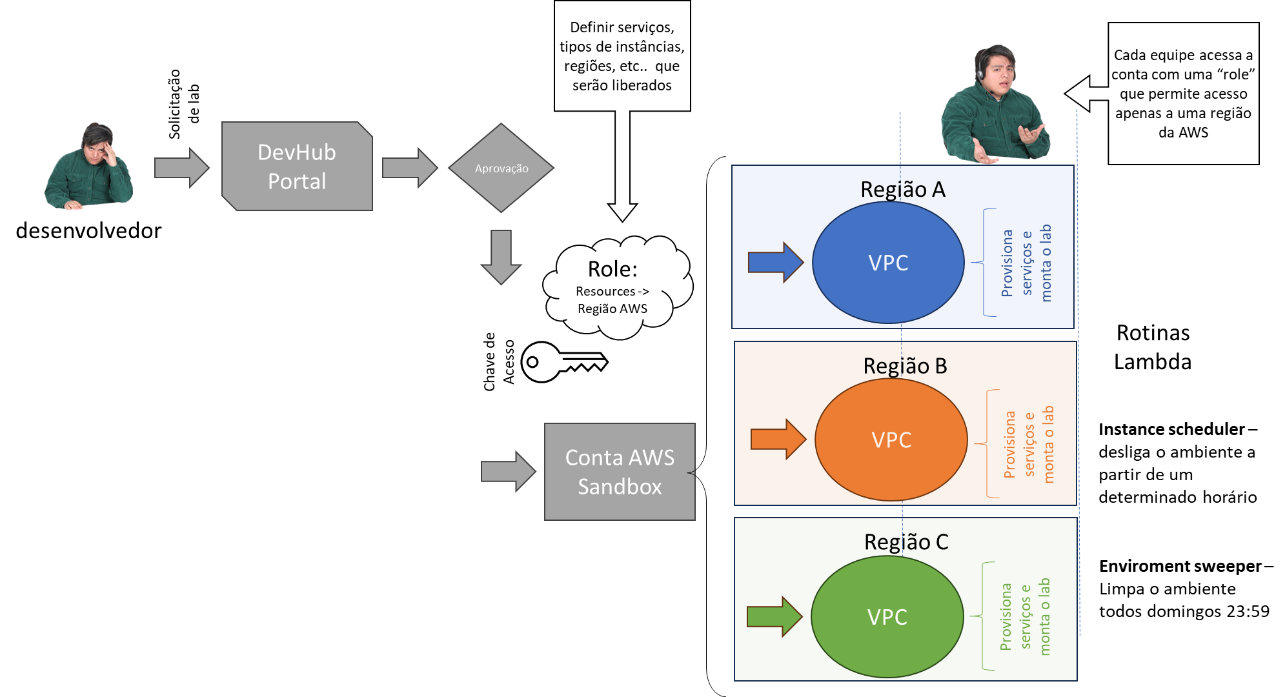
Estamos avaliando com o pessoal do EEC (Cloud Engineering) quais são os cenários que eles irão permitir para esse laboratório, apresentamos duas opções:

## Cenário múltiplas contas



Esse é o cenário mais simples de ser implementado, são criadas contas AWS para cada equipe e essas contas possuem configurações idênticas. As solicitações de acesso no IDC são direcionadas para que os usuários tenham acesso a mesma conta do demais membros da sua equipe

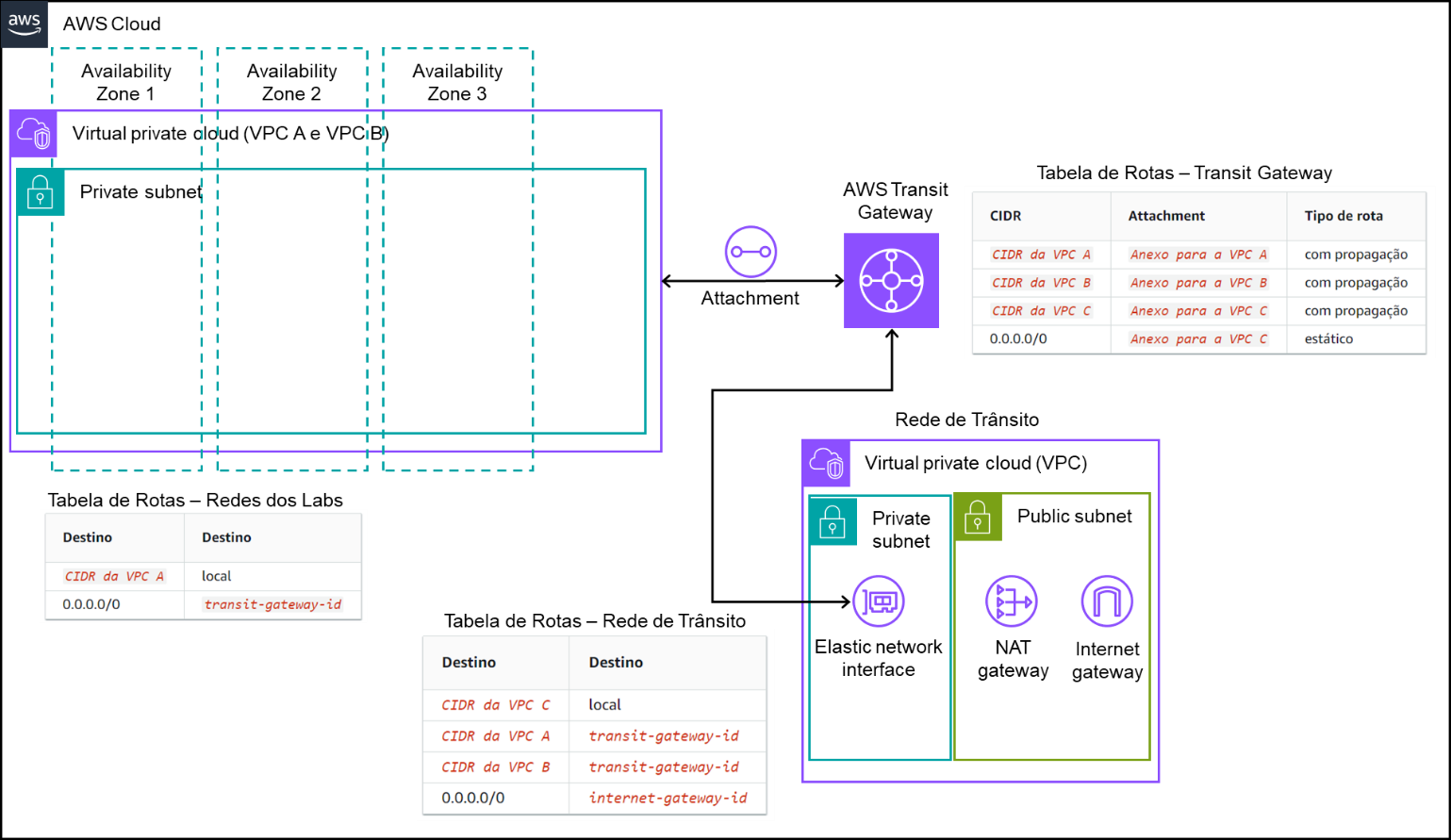
## Cenário com uma conta



Esse cenário usa apenas uma conta e direciona as equipes para VPCs em diferentes regiões da AWS. As solicitações de acessos dos usuários no IDC serão direcionadas à mesma conta da AWS e roles diferentes. Cada role possui uma policy que restringe o acesso exclusivamente à região que a equipe vai trabalhar, impedindo que um time tenha a possibilidade de alterar recursos de outros times.

Obs.: Existem serviços da AWS que são globais, tais como o ROUTE53, CLOUDFRONT etc., caso esses serviços façam parte dos projetos das equipes, eles podem ser impactados por alterações cruzadas dos times.

# Arquitetura da rede



A estrutura da rede para cada conta é criada através de uma VPC (landing-zone), contendo 2 CIDRs, um bloco de endereços roteáveis na rede SERASA e outro apenas para PODs do ambiente do EKS. As conexões externas são realizadas via TRANSIT GATEWAYS

Os CIDRs são blocos de endereços:

1. 10.120.x.x/25 – endereços roteáveis na rede SERASA e com saída para Internet
2. 100.64.0.0/16 – endereços internos para o cluster do EKS para comunicação entre PODs

As subnets são criadas nas zonas de disponibilidades, conforme detalhamento a seguir:

1. Subnets roteáveis - aws-landing-zone-PrivateSubnetxA – 10.120.x.x/27 – esse CIDR permite até 4 subnets e 27 endereços IPs (existem 5 endereços reservados)
2. Subnets para pods - pod-subnet-xA - 100.64.x.0/18 – esse CIDR permite até 4 subnets e 16379 endereços IPs (existem 5 endereços reservados)

# Serviços a serem disponibilizados nos labs

1. Aplication Load Balancer
2. API Gateway
3. EKR e ECR
4. S3
5. EMR
6. Apache AirFlow
7. Provavelmente vamos ter algum serviço de mensageria, por exemplo, MSK
8. Algum serviço de banco de dados (RDS ou DinamoDB), bigdata (Redshift) ou cache (REDIS)
9. Avaliar uso de Lambda para processamento de eventos ou de demandas desacopladas