



Hackathon

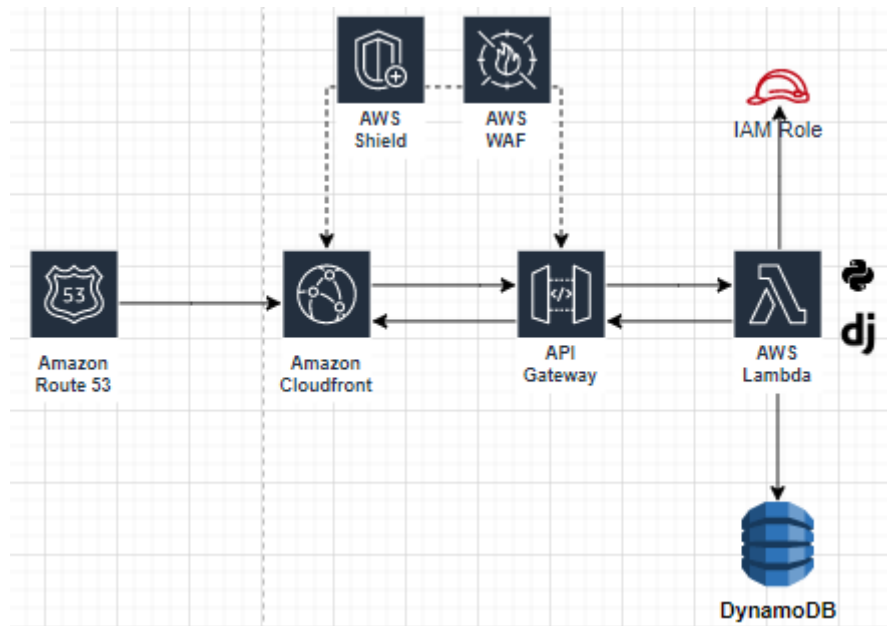
AWS

Grupo:

Alexandre Pires Martins
Guilherme Massaharu Hayashi de Almeida
Guilherme Viana Pereira
Matheus Lemes Tassara
Vitória Barbosa da Silva

São Paulo, 05 de maio de 2023

Neste documento, é possível encontrar toda documentação referente à implementação AWS que teve como referência o desenho de arquitetura abaixo.



Para desenvolvimento desta arquitetura foram implementados no ambiente AWS Academy somente os principais serviços, de forma que a integração AWS Lambda x DynamoDB não pôde ser realizada tendo em vista a falta de permissão para criação/edição de IAM Roles para acesso:

- ☒ **Amazon CloudFront**
- ☒ **API Gateway**
- ☒ **AWS Lambda**
- ☒ **DynamoDB**

Amazon CloudFront

O CloudFront foi criado com origem no API Gateway de destino, que está apontando ao path do endpoint default gerado pela AWS com a implementação do Gateway. Além disto, no CloudFront é possível fazer customizações de segurança tanto de restrição geográfica quanto a partir de regras que poderiam ser definidas pelo WAF para segurança da aplicação.

CloudFront > Distributions > E28SUEDNW4CSPK

E28SUEDNW4CSPK

View metrics

General

Origins

Behaviors

Error pages

Geographic restrictions

Invalidations

Tags

Details

Distribution domain name

d3enigcui5t4tx.cloudfront.net

ARN

arn:aws:cloudfront::126088035852:distribution/E28SUEDNW4CSPK

Last modified

April 30, 2023 at 2:03:57 AM UTC

CloudFront > Distributions > E28SUEDNW4CSPK

E28SUEDNW4CSPK

View metrics

General

Origins

Behaviors

Error pages

Geographic restrictions

Invalidations

Tags

Origins

Edit

Delete

Create origin

Filter origins by property or value

< 1 > ⚙

Origin name

Origin domain

Origin path

Origin type

Origin status

kq7rmnrgs3.execute-api.us-east-1.amazonaws.com/dev

kq7rmnrgs3.execute-api.us-east-1.amazonaws.com/dev

/dev

Custom Origin

-

CloudFront > Distributions > E28SUEDNW4CSPK

E28SUEDNW4CSPK

View metrics

General

Origins

Behaviors

Error pages

Geographic restrictions

Invalidations

Tags

Geographic restrictions

Type

Block list

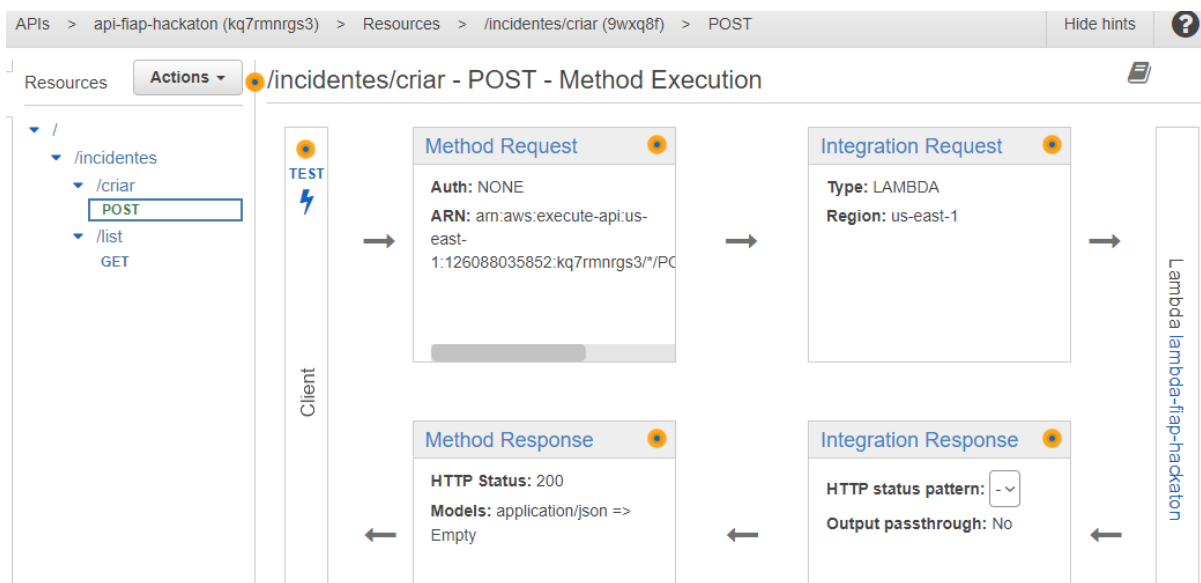
Countries

Russian Federation

API Gateway

O API Gateway criado possui 2 rotas que executam a Lambda responsável pelo backend da aplicação:

Rota	Método	Descrição
/incidentes/criar	POST	Criação de incidente
/incidentes/list	GET	Listagem de todos os incidentes criados



Acessando a rota /incidentes/criar, o seguinte formulário pode ser enviado:

Realize a criação da sua reclamação

Insira seus dados e envie a reclamação

Nome

Insira seu nome

Email

email@example.com

Número do Pedido

123456789

Selecione o Assunto:

☒ Pagamento

☐ Envio-Entrega

☐ Compra Protegida

☐ Outros

Descrição

Conte-nos o que aconteceu

Enviar reclamação

Lambda

lambda-fiap-hackaton

Controlar Copiar ARN Ações ▼

▼ Visão geral da função Informações

lambda-fiap-hackaton

Layers (0)

API Gateway (2)

+ Adicionar destino

+ Adicionar gatilho

Descrição

-

Última modificação

há 2 horas

ARN da função

arn:aws:lambda:us-east-1:126088035852:function:lambda-fiap-hackaton

URL da função [Informações](#)

-

Para a Lambda, foi desenvolvido o código python com django framework conforme o repositório: <https://github.com/vitoriabarbosas/pos/tree/main/hackaton-aws/app>.

Dynamo

Embora a integração não pudesse ser realizada via automação tendo em vista a impossibilidade de criação de IAM Roles para acesso, foi criado uma Tabela manualmente para visualização dos dados. Para testes locais, foi utilizado o SQL dentro do repositório github.

DynamoDB > Tabelas > table-fiap-hackaton

Tabelas (1)

Qualquer tag de tabela ▼

Localizar tabelas por nome de tabel

< 1 > ⚙

table-fiap-hackaton

table-fiap-hackaton

Atualizar Ações Explorar itens da tabela

< Visão geral Índices Monitorar Tabelas globais Backup >

Informações gerais

Chave de partição	Chave de classificação
id (String)	-
Modo de capacidade	Status da tabela
Provisionada	Ativo
Alarmes	Recuperação em um ponto anterior no tempo (PITR) Informações
Nenhum alarme ativo	Desativado

DynamoDB > Itens > table-fiap-hackaton

> **table-fiap-hackaton** Visualização automática Visualizar detalhes da tabela

► **Verificar ou consultar itens**
Expandir para consultar ou verificar itens.

Itens retornados (1/2) Atualizar Ações ▼ Criar item

< 1 > Configurar Selecionar

	id	assunto	descricao	email	name	numero_pedi...
<input type="checkbox"/>	567	Compra Protegida	Olá, no me...	matheusle...	Matheus	273647873
<input checked="" type="checkbox"/>	171	Pagamento	Boa tarde! ...	vitoriabarb...	Vitória	123812389

Para que a Lambda realizasse o input de dados no DynamoDB, seria necessário a criação de uma IAM Role com a seguinte policy anexada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SpecificTable",
      "Effect": "Allow",
      "Action": [
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:Update*",
        "dynamodb:PutItem"
      ],
      "Resource": "arn:aws:dynamodb:*:*:table/table-fiap-hackaton"
    }
  ]
}
```

Componentes de Segurança

Para trabalharmos com uma arquitetura de segurança um pouco mais robusta, podemos enfatizar os seguintes serviços AWS:

- **CloudFront**
- **AWS Shield**
- **AWS WAF**
- **IAM Roles**

Com o CloudFront, podemos definir restrições geográficas para acesso quanto também atrelar regras de WAF para proteção da aplicação a nível de aplicação. O AWS Shield e WAF, nos permitem proteção para ataques DDoS, além de poder integrar regras WAF não só com CloudFront quanto com API Gateway. Por fim, IAM Roles com privilégio mínimo de acesso entre as aplicações.