Laboratório - Criação de tabela DynamoDB e operação CRUD com Python

Resumo

Este laboratório guiado apresenta o passo a passo completo para criar uma aplicação serverless que utiliza o Amazon DynamoDB como banco de dados e o AWS Lambda para executar operações CRUD (Create, Read, Update e Delete) com integração via API Gateway e interface web hospedada no Amazon S3. O aluno também configura monitoramento com o Amazon CloudWatch.

Observação: A interface do Console de Gerenciamento da AWS pode sofrer pequenas alterações visuais ao longo do tempo, mas os conceitos e a localização geral dos serviços permanecem consistentes. As instruções neste resumo seguem a estrutura geral das funcionalidades.

Objetivos do laboratório

Este laboratório ensina como:

- Criar uma role IAM com permissões adequadas para Lambda e DynamoDB;
- Criar uma tabela no DynamoDB;
- Desenvolver uma função Lambda em Python e integrá-la ao DynamoDB;
- Configurar o API Gateway com rotas para operações CRUD;
- Hospedar uma interface web no Amazon S3;
- Ativar monitoramento com CloudWatch;
- Validar o funcionamento da aplicação e realizar limpeza dos recursos utilizados.

Cenário

Você está construindo uma aplicação web simples de cadastro de produtos. O frontend estático será hospedado em um bucket do Amazon S3, enquanto as requisições de criação, leitura, atualização e exclusão serão processadas por uma função AWS Lambda. Essa função interage diretamente com uma tabela DynamoDB, e todas as chamadas passarão por um endpoint criado no API Gateway. O monitoramento da solução será feito via Amazon CloudWatch Logs.

Pré-requisitos

- Conta ativa na AWS com permissões de administrador;
- Conhecimentos básicos sobre Lambda, DynamoDB e S3;
- Noções de programação em Python;
- Familiaridade com o console de gerenciamento da AWS;
- Navegador web atualizado;
- Arquivos locais do frontend (index.html, style.css, script.js) e função Lambda (CRUD.zip).

Arquivos para Download

Os arquivos necessários para execução deste laboratório (frontend e função Lambda) estão disponíveis para download abaixo:

Baixar arquivos

Passo 1: Criação da Role (Lambda e DynamoDB)

1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço IAM.
2. No painel de navegação esquerdo, localize "Roles (Funções)" e clique em "Criar perfil".
3. Em "Tipo de entidade confiável", deixe marcada a caixa "Serviço da AWS". Role para baixo e, em "Caso de uso", selecione "Lambda". Clique em "Próximo".
4. Em "Adicionar permissões", pesquise pelas policies:
   4.1.AWSLambdaBasicExecutionRole
   4.2.AmazonDynamoDBFullAccess
   Adicione-as e depois clique em "Próximo".
5. Em "Nome do perfil", digite RoleCrud-seunome e clique em "Criar perfil".

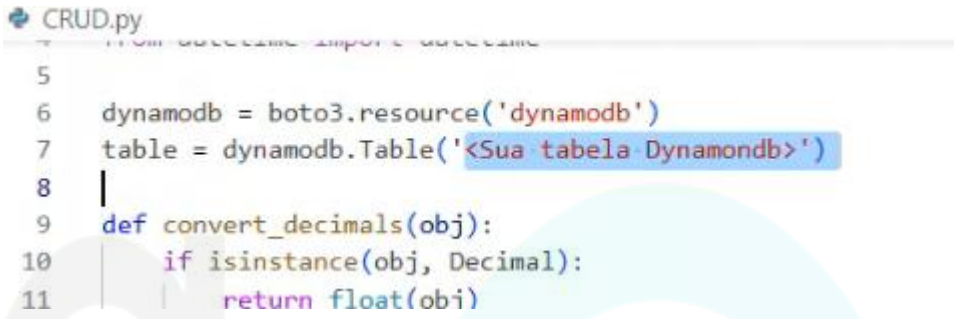
Passo 2: Criação de tabela no Dynamo

1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço DynamoDB.
2. Clique em "Criar tabela".
3. Digite o nome da tabela: Produtos-seunome.
4. No campo "Chave de partição", digite id. Ao lado, deixe selecionado "String".
5. Não altere mais nenhuma configuração nesta seção e clique em "Criar tabela".
6. Salve o nome da sua tabela em um bloco de notas para referência futura.

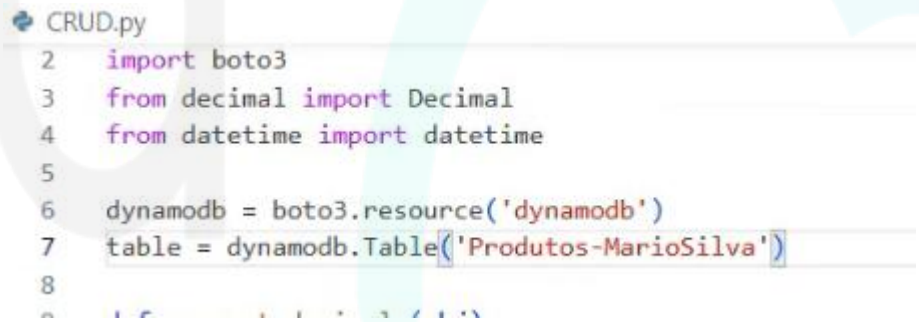
Passo 3: Criação da Função no Lambda

1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço Lambda.
2. Clique em "Criar função".
3. Selecione "Criar do zero".
4. Em "Nome da função", digite LambdaCrud-seunome.
5. No campo "Tempo de execução", selecione "Python 3.12".
6. Em "Alterar a função de execução padrão", selecione "Usar uma função existente".
7. No campo abaixo, em "Função existente", procure pela função que você criou no passo 1 (RoleCrud-seunome). Marque-a e depois clique em "Criar função".
8. Na aba "Código", você fará o upload do arquivo CRUD.zip. Clique em "Fazer upload". Selecione o arquivo e clique em "Salvar".
9. Depois, selecione o arquivo já importado (CRUD.py) no editor de código.
10. Role para baixo e procure pela seção "Configurações de tempo de execução". Clique em "Editar".

11. No campo "Handler" (Manipulador), apague o nome lambda_function.lambda_handler e digite CRUD.lambda_handler. Clique em "Salvar".
12. Volte para a aba "Código". Dentro do código importado (CRUD.py), localize a linha similar a table = dynamodb.Table(‘<sua tabela dynamodb>’) (geralmente na linha 7, mas pode variar). Apague <sua tabela dynamodb> e digite o nome exato da sua tabela que você salvou no bloco de notas (do Passo 2).
    - *Observação:* Lembre-se de apagar os símbolos < > ao digitar o nome da sua tabela.
13. **Exemplo antes da alteração:**



14. **Exemplo depois da alteração:**

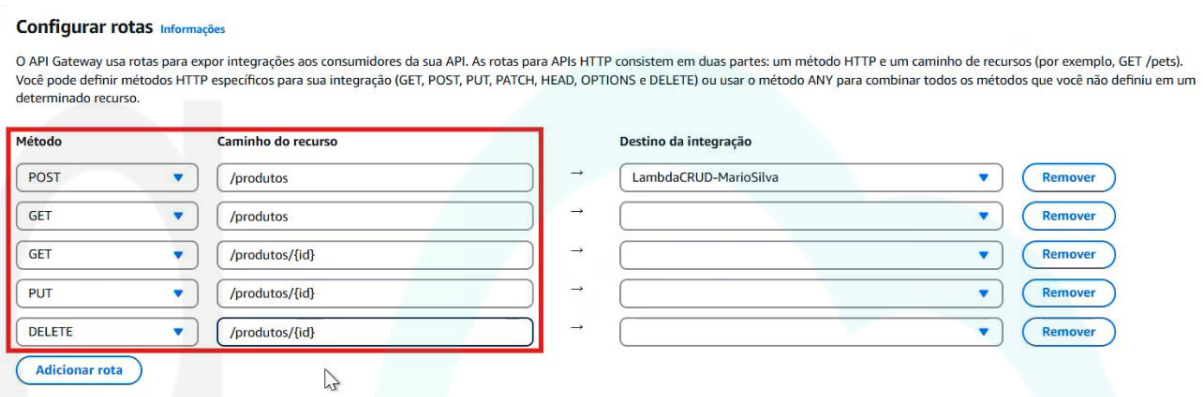


15. Após realizar a alteração do nome da tabela no código, clique no botão Deploy para validar suas mudanças e salvar a função.
16. Navegue até a aba Configuração.
17. Clique em Editar.
18. Altere o campo Memória para 256 MB.
19. Altere o campo Tempo limite para 10 segundos.
20. Depois clique em Salvar.

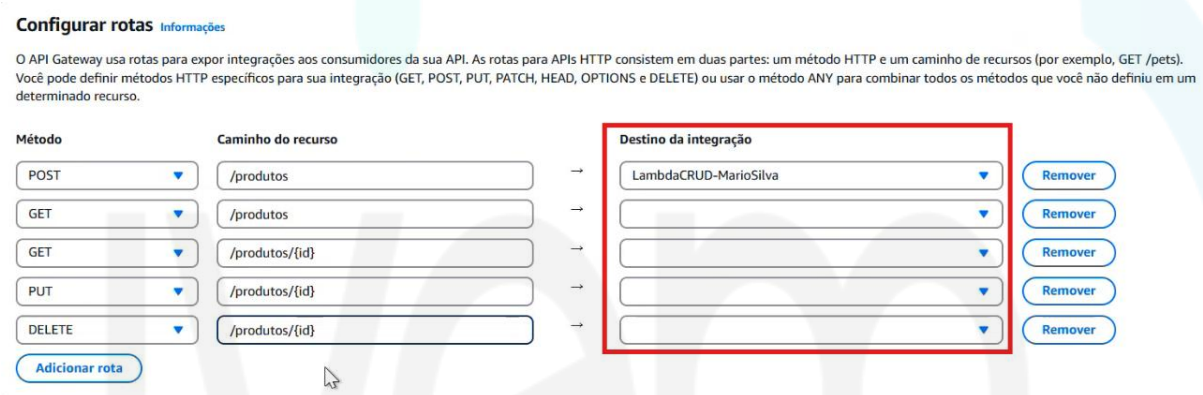
Passo 4: Criação do API Gateway

1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço API Gateway. Clique em "Criar uma API".
2. Na seção "API HTTP", clique em "Compilar".

3. Digite o nome da API: APICRUD-seunome.
4. Clique em "Adicionar integração".
5. Selecione "Lambda".
6. No campo "Função do Lambda", selecione a função criada no passo 3 (LambdaCrud-seunome).
7. Clique em "Avançar".
8. Na tela "Configurar rotas", você precisará adicionar 5 rotas. Clique no botão "Adicionar rota" para cada uma.
9. Para cada rota adicionada, digite as informações nos campos "Método" e "Caminho do recurso", conforme especificado na sua documentação ou imagem de referência (já que os métodos e caminhos específicos não foram listados no texto fornecido), conforme mostrado na imagem de referência. abaixo:

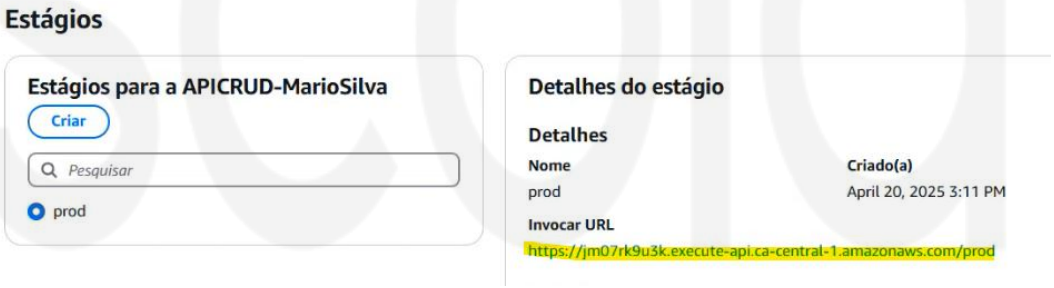


10. Em seguida, no campo Destino da integração, selecione a função Lambda que você criou no passo 3 (LambdaCrud-seunome), conforme mostrado na imagem de referência. abaixo:

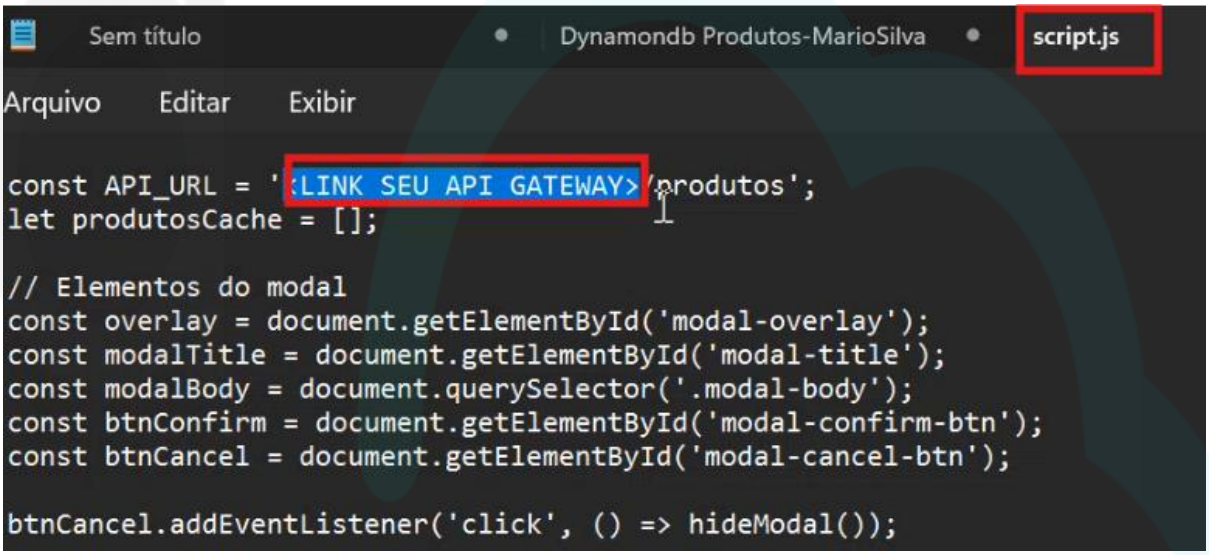


11. Depois clique em Avançar.
12. Em Configurar estágios, digite: prod.
13. Deixe marcada a caixa Implantação automática.
14. Clique em Avançar.
15. Será exibido um resumo das configurações. Clique em Criar.
16. Após finalizar a criação da API:
17. No painel de navegação esquerdo, clique em Deploy.

18. Em seguida, clique em Stages.
19. Selecione o estágio prod.
20. Copie a URL “Invocar URL”



21. Abra o arquivo script.js.
22. Localize o trecho no código onde a URL da API deve ser inserida "const API_URL".
23. Apague <LINK SEU API GATEWAY>
24. Cole a URL que você copiou do API Gateway anteriormente neste local indicado. Conforme a imagem de referência a seguir:

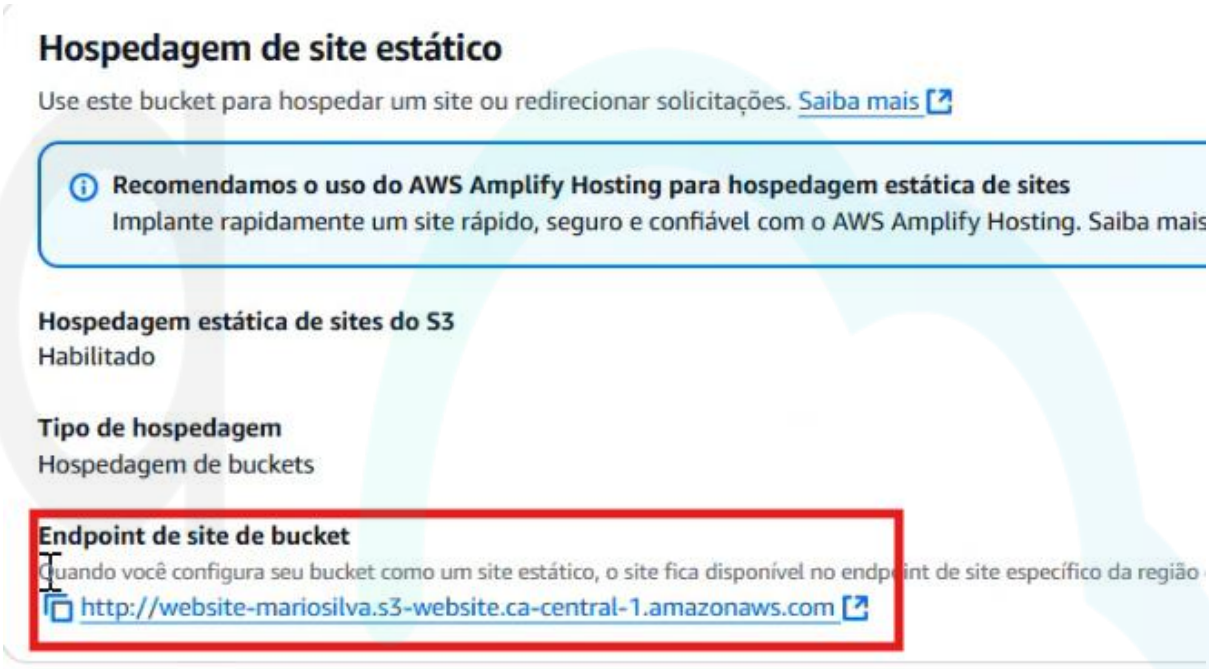


25. Salve o arquivo script.js com a alteração.

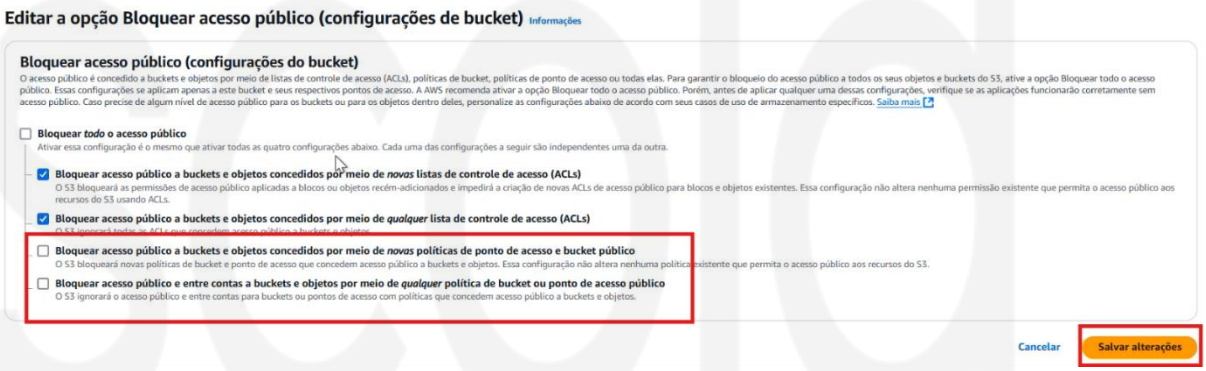
Passo 5: Criação de um Bucket (S3)

1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço S3. Clique em "Criar bucket".
2. Digite o nome do seu bucket: website-seunome.
3. Mantenha as demais configurações padrão e clique em "Criar bucket".
4. Após a criação, acesse o bucket que você acabou de criar.
5. Clique no botão "Carregar".
6. Clique no botão "Adicionar arquivos" e selecione os arquivos:
    1.1.script
    1.2.style
    1.3.index

7. Role para baixo e clique em "Carregar".
8. Após finalizar o upload, clique em fechar.
9. Na tela do seu bucket, selecione a aba "Propriedades".
10. Role para baixo até encontrar a seção "Hospedagem de site estático". Clique em "Editar".
11. Marque a caixa para "Ativar" a hospedagem de site estático.
12. No campo "Documento de índice", digite index.html.
13. Role para baixo e clique em "Salvar alterações".
14. De volta na seção "Hospedagem de site estático", no campo "Endpoint de site de bucket", copie a URL.
15. Salve esta URL em um bloco de notas. Você usará esta URL para acessar o site (conforme mostrado na imagem de referência abaixo).



16. Agora, vamos configurar as permissões para liberar o acesso ao site. Na aba Permissões do seu bucket, procure pela seção Bloquear acesso público (configurações de bucket).
17. Clique em Editar.
18. Em seguida, desmarque as duas últimas opções [conforme mostra a imagem abaixo].



19. Clique em Salvar alterações.
20. Será solicitado que você digite confirmar para confirmar a mudança. Digite confirmar e clique em Confirmar.
21. Role um pouco mais para baixo na aba Permissões até encontrar a seção Política do bucket.
22. Clique em Editar (no lado direito da seção).
23. Antes de seguir, copie o ARN do seu bucket, conforme imagem abaixo:

24. Cole no seu bloco de notas, você precisará dessa informação em seguida.
25. Em seguida, clique no botão Gerador de política (também no lado direito).

26. Na nova aba que será aberta (o Gerador de Política).

- **Observação:** Certifique-se de que o navegador esteja em inglês antes de iniciar a configuração. Se o seu navegador traduzir a página automaticamente, é altamente recomendável voltar ao idioma original (inglês). A tradução automática pode alterar a sintaxe da regra e causar erros no seu laboratório.

27. **Step 1: (SELECT TYPE OF POLICY)**: Marque a opção S3 Bucket Policy.
28. **Step 2: (ADD STATEMENT)**:
    - Em "Effect", marque Allow.
    - Em "Principal", digite * (isso permite acesso público).
    - Em "Actions", procure e selecione GetObject.

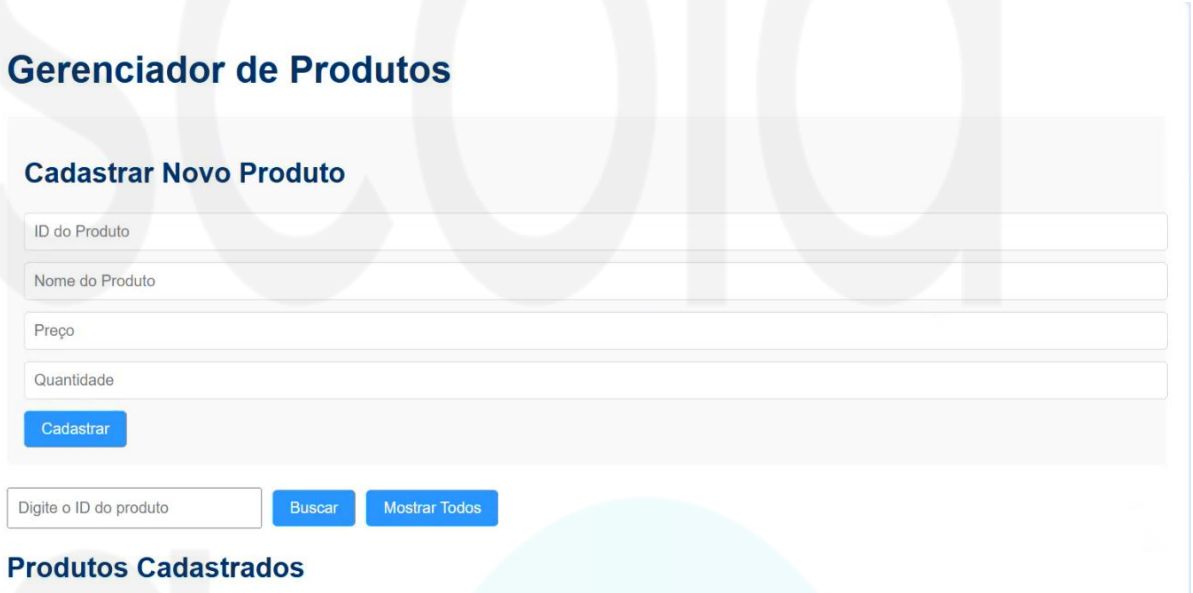
- Em "Amazon Resource Name (ARN)", cole o ARN do seu bucket S3 (que você documentou no seu bloco de notas no passo anterior). **É crucial adicionar /* ao final do ARN do bucket**. Por exemplo, se o ARN for arn:aws:s3:::seu-nome-do-bucket, você deve colar arn:aws:s3:::seu-nome-do-bucket/* .

- Isso concederá a ação GetObject (ler objetos/arquivos) para qualquer principal (*) dentro de qualquer caminho (/*) do seu bucket S3.
- Clique em "Add Statement".

29. Depois de adicionar a instrução, clique em "Generate Policy".
30. Na caixa de texto que aparece no Gerador de Política, selecione e copie a política JSON gerada.
31. Volte para a aba do Console da AWS onde você estava editando a Política do bucket (onde clicou em "Editar").
32. Cole a política JSON que você copiou do gerador na caixa de texto do editor de política do bucket, conforme mostrado na imagem de referência abaixo:

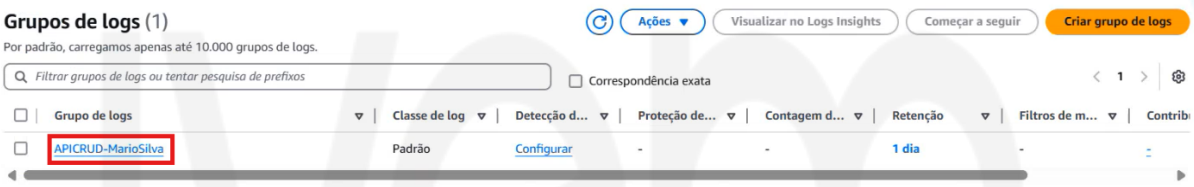
33. Depois de colar a política, role para baixo e clique em Salvar alterações.
34. Pegue a URL do "Endpoint de site de bucket" que você copiou no Passo 5 -> 15.
35. Abra esta URL em um navegador web novamente.

36. Verifique se o site carrega corretamente e se a aparência é similar à mostrada na imagem de referência abaixo.



Passo 6: Criação de Grupos de Logs no CloudWatch

1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço CloudWatch.
2. No painel de navegação esquerdo, navegue até **Logs** e, em seguida, clique em **Grupos de logs**.
3. Clique no botão **Criar grupo de logs**.
4. Agora, insira as seguintes informações:
    - No campo **Nome do grupo de logs**, digite: APICRUD-seunome
    - No campo **Configuração de retenção**, selecione: 1 dia
    - No campo **Classe de log**, deixe selecionado: Padrão
5. Depois, clique em **Criar**.
6. Após a criação, acesse o grupo de logs que foi criado:



37. Copie o **ARN** (Amazon Resource Name) do grupo de logs e salve-o no bloco de notas, pois ele será necessário posteriormente. Conforme mostrado na imagem de referência abaixo:

38. Cole no seu bloco de notas, você precisará dele a seguir.

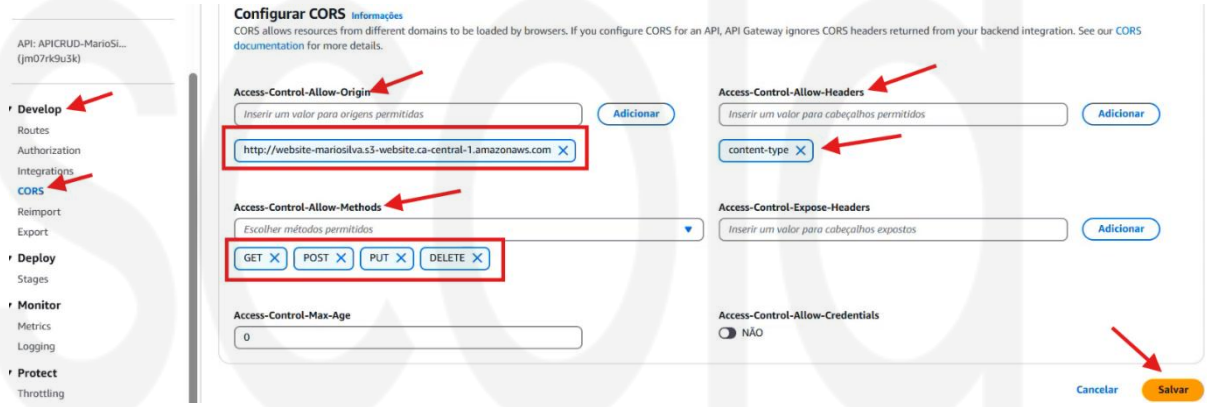
Passo 7: Retorne para o console do API Gateway

Habilitando o log no API Gateway:

39. Volta lá no console do API Gateway.
40. No painel de navegação esquerdo, navegue até Monitor
41. Clique em Logging.
42. No canto superior direito da tela, clica em Editar.
43. Agora ativa a opção de “Registro em log de acesso”.
44. No campo Destino do log, cola o ARN que a gente copiou lá do CloudWatch Logs.
45. Em Formato do log, seleciona JSON.
46. Por fim, clica em Salvar.

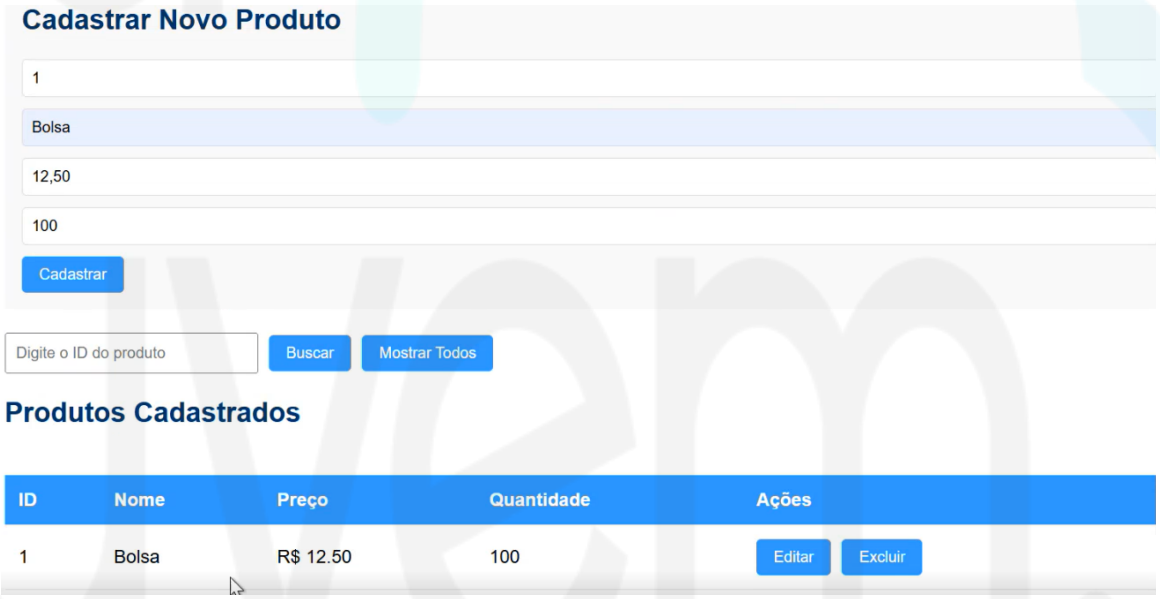
Ativando o CORS no API Gateway:

47. No painel de navegação esquerdo, navegue até Develop.
48. Clique em CORS.
49. No lado superior direito, clique em Configurar.
50. Na tela de configuração do CORS, preencha os campos exatamente conforme a imagem:
    - Access-Control-Allow-Origin: Cole a URL do "Endpoint de site de bucket" que você copiou do seu bucket S3 no Passo 5 -> 15. Depois de colar, clique em Adicionar.
    - Access-Control-Allow-Headers: Digite content-type e clique em Adicionar.
    - Access-Control-Allow-Methods: Adicione os seguintes métodos clicando no dropdown e selecionando-os (ou digite e clique em "Adicionar", dependendo da interface): GET, POST, PUT, DELETE. Certifique-se de que todos apareçam como "botões" adicionados abaixo do campo.
    - Access-Control-Expose-Headers: Deixe este campo vazio.
    - Access-Control-Max-Age: Deixe 0.
    - Access-Control-Allow-Credentials: Padrão “NÃO”.
51. Após configurar todos os, conforme mostrado na imagem de referência abaixo, clique em Salvar.



Passo 8: Cadastrando produtos no nosso site

1. Abra a URL do site que você copiou no Passo 5 (o "Endpoint de site de bucket") no seu navegador.
2. Você deverá ver a interface do site CRUD.
3. Para cadastrar o primeiro produto, preencha os campos da seguinte forma:
    - ID DO PRODUTO: Digite 1
    - NOME DO PRODUTO: Digite Bolsa
    - PREÇO: Digite 12.50 (use ponto, não vírgula, é o formato esperado em programação/JSON)
    - QUANTIDADE: Digite 100
4. Clique no botão Cadastrar.
5. Verifique se o item que você acabou de cadastrar (ID 1) aparece na seção "Produtos Cadastrados" abaixo do formulário.



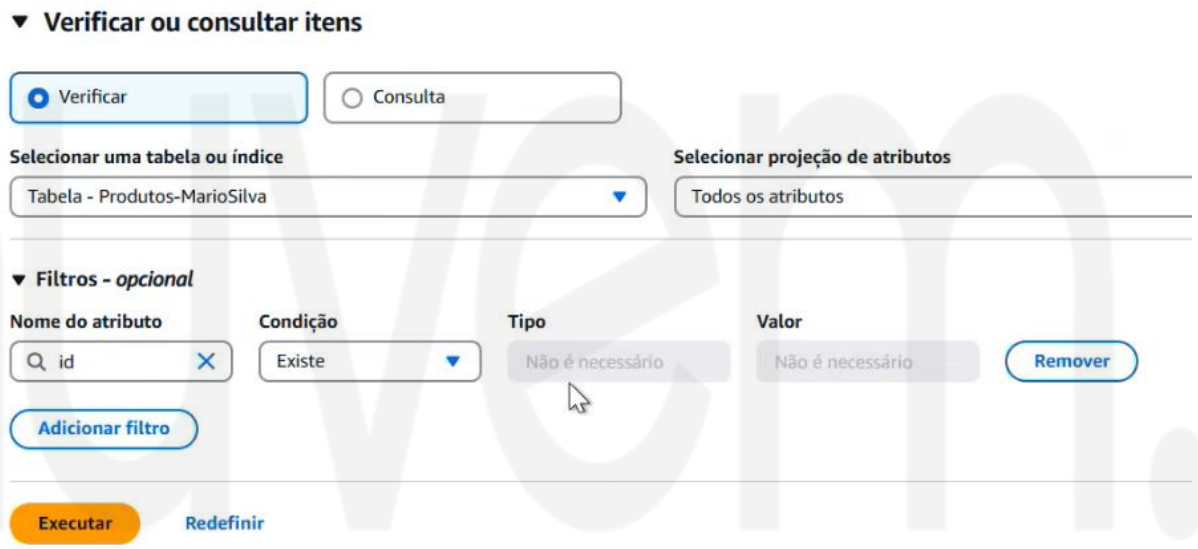
6. Repita o processo de preencher o formulário e clicar em "Cadastrar" para os outros produtos, utilizando os dados (ID, Nome, Preço, Quantidade) mostrados na imagem de referência para os demais itens (IDs 2, 3 e 4).

7. Após cadastrar todos os 4 itens, a lista completa na seção "Produtos Cadastrados" deverá estar igual à mostrada na imagem abaixo, contendo todos os produtos que você adicionou.

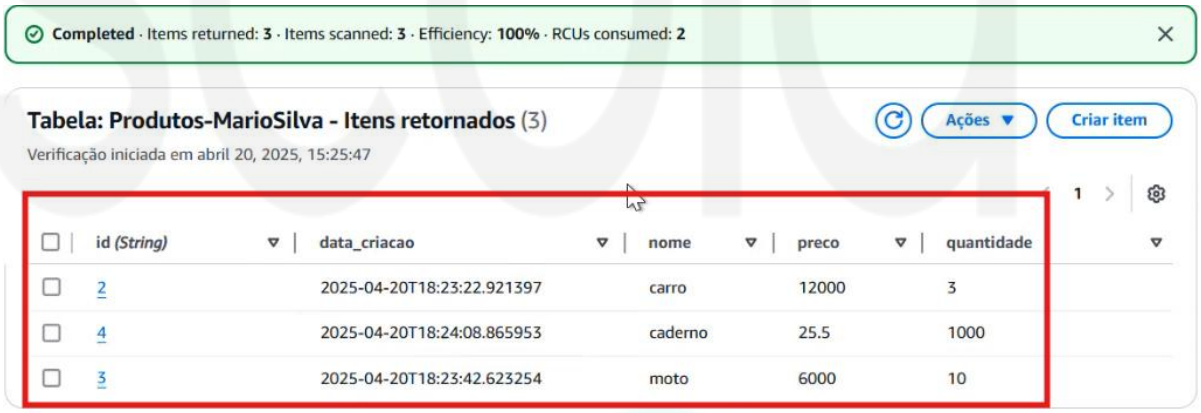
Observação: Na seção "Produtos Cadastrados" do site, você pode utilizar as opções no campo **Ações** para **Editar** ou **Excluir** os produtos, caso precise realizar alguma alteração.

Agora, vamos verificar se os produtos cadastrados foram armazenados corretamente no DynamoDB:

52. Acesse o Console de Gerenciamento da AWS e navegue de volta para o serviço DynamoDB.
53. No painel de navegação esquerdo, clique em Explorar itens.
54. Selecione a sua tabela (Produtos-seunome).
55. Para filtrar os resultados, na seção **Filtros**, informe:
    - No campo Nome do atributo, digite id.
    - No campo Condição, selecione existe.
    - Clique em Executar.

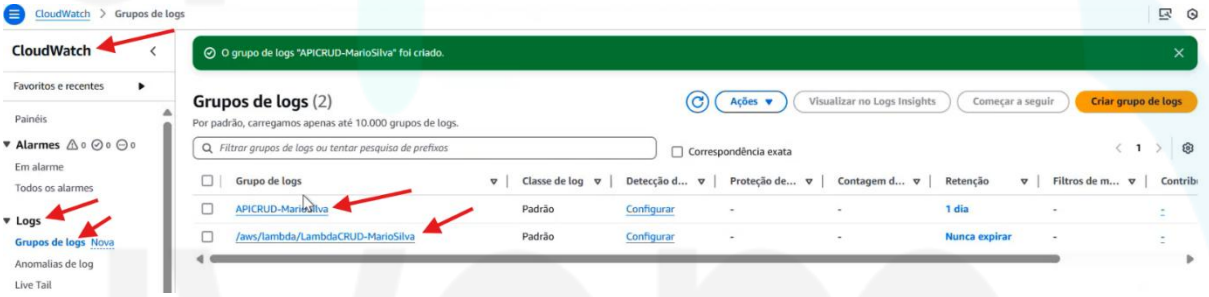


56. Abaixo, você visualizará os itens que foram cadastrados através do site e armazenados na sua tabela DynamoDB. A lista deverá conter os 4 produtos que você adicionou, conforme mostrado na imagem de referência abaixo.

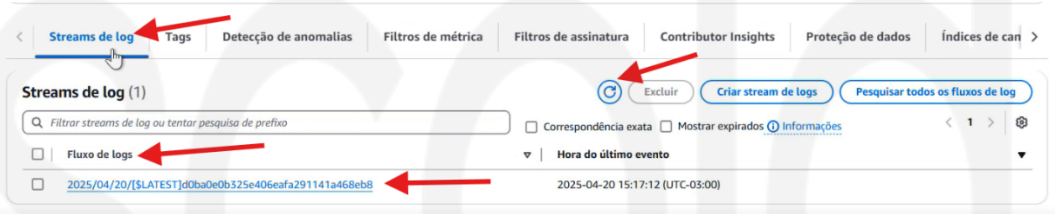


Passo 9: Verificando os logs no CloudWatch

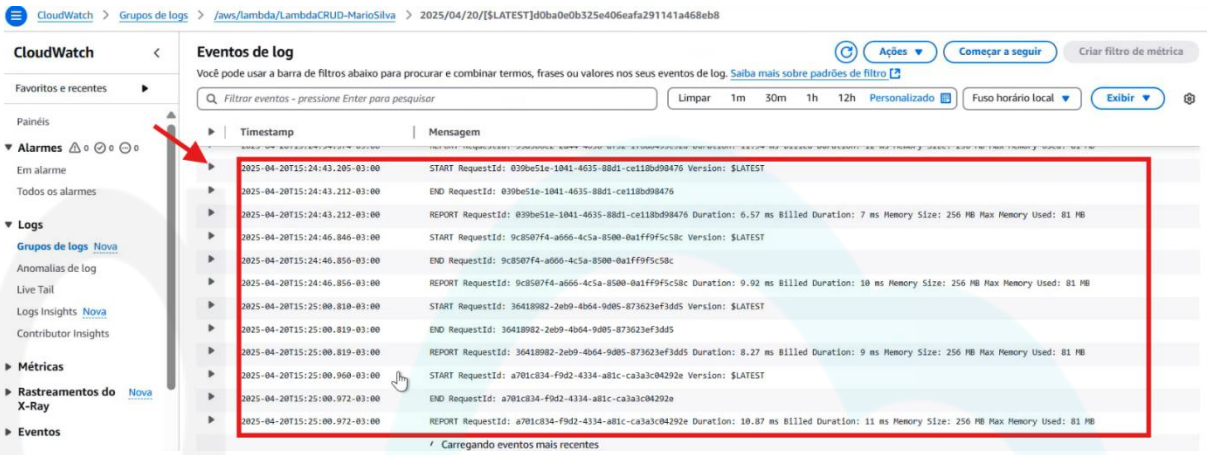
1. Acesse o Console de Gerenciamento da AWS e navegue de volta para o serviço CloudWatch.
2. No painel de navegação esquerdo, navegue até **Logs** e, em seguida, clique em **Grupos de logs**.
3. Nesta lista de grupos de logs, procure por **dois** grupos:
   - O grupo que você criou manualmente no Passo 6 para os logs do API Gateway: **APICRUD-seunome**
   - O grupo que o Lambda criou automaticamente para a sua função: **/aws/lambda/LambdaCrud-seunome**.



4. **Clique em cada um desses grupos de logs** para acessá-los.
5. Dentro de cada grupo de logs, você verá uma lista de "Streams de log". Clique em um stream de log recente.
6. Dentro do stream de log, você verá os eventos de log:
   - No grupo **APICRUD-seunome**, você deverá ver os logs formatados em JSON, registrando as chamadas HTTP (GET, POST) que foram feitas para a sua API a partir do site.
2. Clique no botão/ícone de **Atualizar** (refresh) no canto superior direito da lista, se necessário, para garantir que os streams mais recentes apareçam.



3. Em **Streams de log -> Fluxo de logs** que aparecer (geralmente um nome que inclui a data e um identificador único). Clique nele.
4. Dentro deste stream, você poderá **visualizar os logs gerados** pela sua função Lambda a cada execução (por exemplo, informações de início/fim da execução, mensagens de erro, ou saídas que você tenha configurado no código Python).



5. Clique na **seta de expansão**. O cursor na imagem aponta exatamente para essa seta.
6. Ao clicar na seta, o conteúdo completo (e às vezes formatado) daquele evento de log será exibido, fornecendo mais informações detalhadas sobre a execução ou o evento registrado. Isso é especialmente útil para logs JSON ou logs com múltiplas linhas.

Repita o passo 9 ->6.

7. Volte para o serviço CloudWatch:
8. No painel de navegação esquerdo, navegue até **Logs** e, em seguida, clique em **Grupos de logs**.
9. Nesta lista de grupos, localize e clique no grupo de logs que você criou especificamente para o API Gateway no Passo 6: **APICRUD-seunome**.
10. Ao entrar neste grupo, você verá a lista de **Streams de log** relacionados às chamadas da API.
11. Clique no botão/ícone de **Atualizar** (refresh) se necessário.
12. No campo **Streams de log**, clique no **nome do stream** que aparecer.
13. Dentro deste stream, você poderá **visualizar os logs gerados pelas chamadas HTTP** que foram feitas para a sua API Gateway a partir do site. Como você

configurou o formato JSON no passo anterior, os logs devem aparecer nesse formato, contendo informações sobre as requisições (método, caminho, status, etc.).

Excelente! Parabéns por chegar até o final e concluir este laboratório!

Você navegou por diversos serviços da AWS, configurou permissões, implantou código, criou APIs e verificou logs. Dominar esses passos é fundamental para construir aplicações serverless na nuvem.

Agora, para evitar custos contínuos na sua conta AWS, é **EXTREMAMENTE IMPORTANTE** realizar a limpeza dos recursos criados. Siga os passos abaixo:

Limpeza de Recursos (IMPORTANTE para evitar custos):

É fundamental excluir todos os recursos que você criou neste laboratório para garantir que não haverá cobranças inesperadas.

1. **Excluir o CloudWatch:**
    1.1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço CloudWatch.
    1.2. No painel de navegação esquerdo, vá em **Logs** > **Grupos de logs**.
    1.3. Localize os dois grupos de logs relacionados ao laboratório (APICRUD-seunome e /aws/lambda/LambdaCrud-seunome).
    1.4. Marque as caixas ao lado dos nomes desses dois grupos.
    1.5. Clique no botão **Ações** e selecione **Excluir grupo de logs**.
    1.6. Confirme a exclusão.
2. **Excluir o S3:**
    2.1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço S3.
    2.2. Localize o bucket que você criou (website-seunome).
    2.3. **Antes de excluir o bucket, você precisa esvaziá-lo.** Clique no nome do bucket, depois na aba **Objetos**. Marque todos os objetos (ou selecione por página), clique em **Ações** e selecione **Excluir**. Digite excluir permanentemente para confirmar.

2.4. Após esvaziar o bucket, volte para a lista de buckets S3.
2.5. Marque a caixa ao lado do nome do seu bucket (website-seunome).
2.6. Clique no botão **Excluir**.
2.7. Digite o nome do bucket para confirmar a exclusão e clique em **Excluir bucket**.

3. **Excluir o API Gateway:**
   3.1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço API Gateway.
   3.2. No painel de navegação esquerdo, clique em **APIs HTTP**.
   3.3. Localize a sua API (APICRUD-seunome).
   3.4. Marque a caixa ao lado do nome da API.
   3.5. Clique no botão **Ações** e selecione **Excluir**.
   3.6. Digite excluir para confirmar e clique em **Excluir**.
4. **Excluir o Lambda:**
   4.1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço Lambda.
   4.2. No painel de navegação esquerdo, clique em **Funções**.
   4.3. Localize a função que você criou (LambdaCrud-seunome).
   4.4. Marque a caixa ao lado do nome da função.
   4.5. Clique no botão **Ações** e selecione **Excluir**.
   4.6. Digite excluir para confirmar e clique em **Excluir**.
5. **Excluir o DynamoDB:**
   5.1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço DynamoDB.
   5.2. No painel de navegação esquerdo, clique em **Tabelas**.
   5.3. Localize a tabela que você criou (Produtos-seunome).
   5.4. Marque a caixa ao lado do nome da tabela.
   5.5. Clique no botão **Ações** e selecione **Excluir**.
   5.6. Marque a caixa "Excluir todos os backups, se houver." e clique em **Excluir tabela**.
6. **Excluir a Role (IAM):**
   6.1. Acesse o Console de Gerenciamento da AWS e navegue até o serviço IAM.
   6.2. No painel de navegação esquerdo, clique em **Perfis (Roles)**.
   6.3. Procure pelo nome da Role que você criou no Passo 1 (RoleCrud-seunome).
   6.4. Clique no nome da Role para acessá-la.
   6.5. No canto superior direito, clique no botão **Excluir perfil**.
   6.6. Digite o nome da Role para confirmar e clique em **Excluir**.

Ao seguir todos esses passos de limpeza, você garantirá que os recursos criados durante este laboratório não gerarão custos inesperados.