



Laboratório - Automatizando o Fim das Instâncias na AWS

Resumo do laboratório

Neste laboratório, você aprenderá a criar e gerenciar políticas e funções no AWS, focando em automação e integração entre serviços. A seguir, você passará por uma série de etapas para criar uma política de IAM, que irá permitir terminar instâncias EC2. Em seguida, você criará uma função Lambda utilizando Python, associará essa função à política IAM e configurará os gatilhos para que ela seja executada automaticamente através do EventBridge (anteriormente CloudWatch Logs).

Objetivos

Ao concluir o lab, você aprenderá o seguinte:

- Criar uma política IAM para permitir a finalização de instâncias EC2
- Criar e configurar uma função Lambda para automatizar o encerramento de instâncias.
- Associar a função IAM à função Lambda, garantindo permissões adequadas.
- Implementar um gatilho no EventBridge para acionar a função Lambda automaticamente.
- Ajustar o tempo de execução da função, garantindo seu funcionamento adequado.

Início

Acesse o [console de gerenciamento da AWS](#)

Caso apresente a mensagem de erro abaixo, clique no texto em azul onde consta a informação “To logout, click here”.



Amazon Web Services Sign In

The credentials in your login link were invalid. Please contact your administrator.

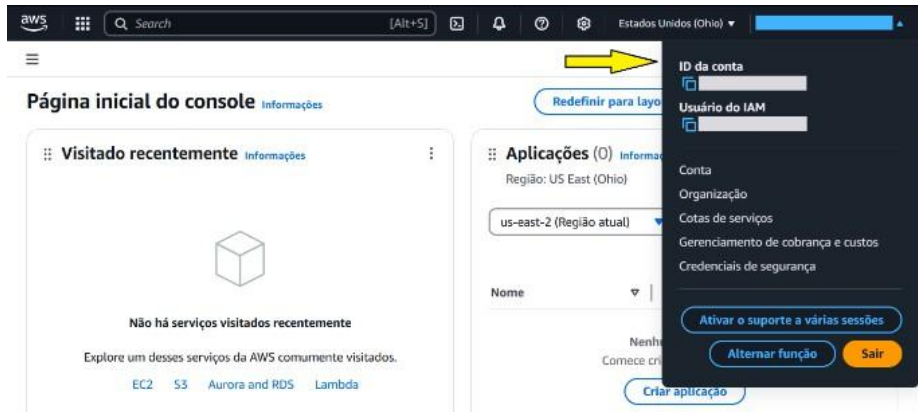
To logout, click here



Terms of Use Privacy Policy © 1996-2025, Amazon Web Services, Inc. or its affiliates.

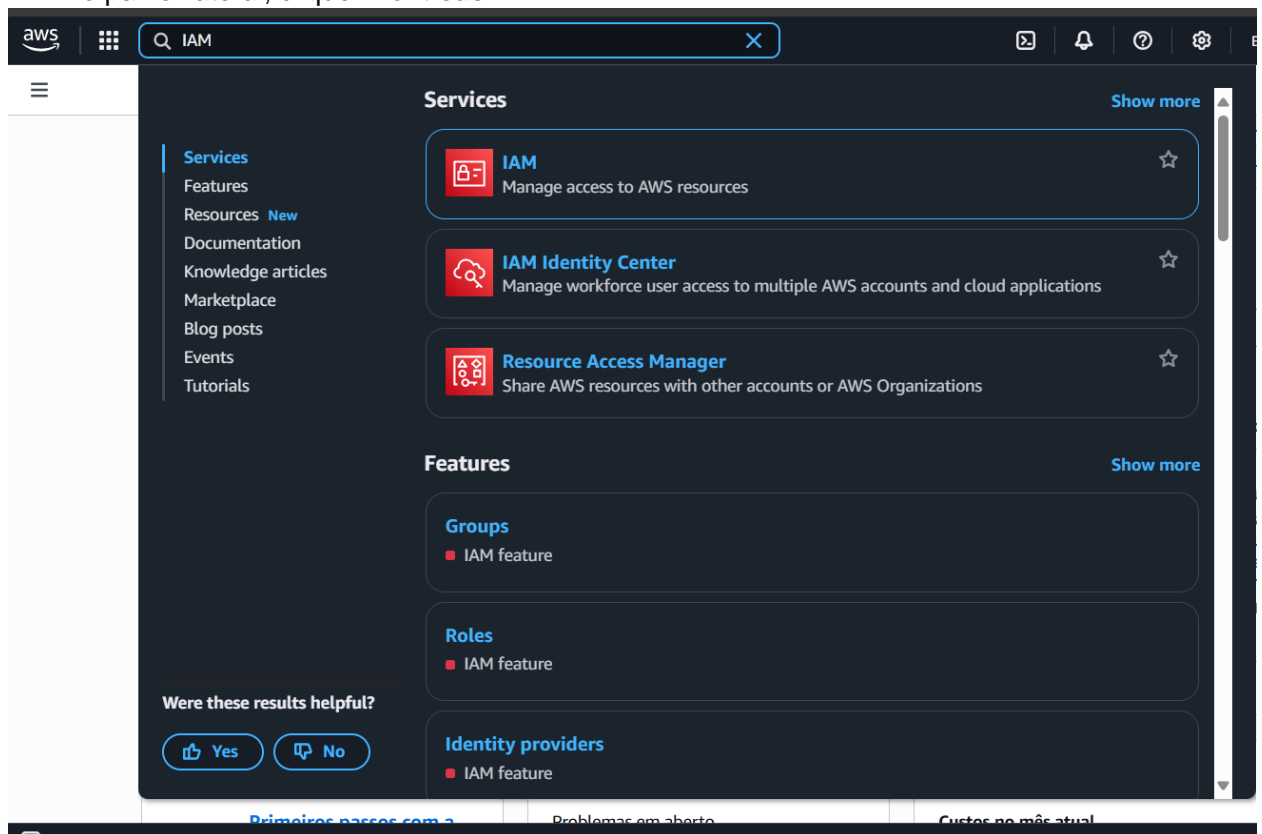
An amazon.com company

Atenção: Após efetuar login, irá mostrar o console de gerenciamento da AWS. Sempre confira, no canto superior direito do console, qual a conta está logada, para evitar acessar com a conta incorreta e evitar gastos desnecessários.



1. Cria política IAM

1.1. Acesse o IAM no console da AWS. No canto superior esquerdo, clique no menu e, no painel lateral, clique "Políticas".



Identity and Access Management (IAM)

Painel

Gerenciamento de acesso

- Grupos de usuários
- Usuários
- Funções
- Políticas**
- Provedores de identidade
- Configurações da conta
- Gerenciamento de acesso raiz

Relatórios de acesso

- Access Analyzer
- Acesso externo
- Acesso não utilizado
- Configurações do Analyzer

Painel do IAM

Recomendações de segurança

- Adicionar MFA para você
- Seu usuário, [sabrina.idev@outlook.com](#), não tem chaves de acesso ativas que não tenham sido utilizadas há mais de um ano.

Recursos do IAM

Grupos de usuários	Usuários	Funções	Políticas	Provedores de identidade
2	66	7	8	0

Novidades

Atualizações para recursos no IAM

Políticas (1359)

Uma política é um objeto na AWS que define permissões.

Filtrar por Tipo

Todos os tipos

Nome da política	Tipo	Usado como	Descrição
AccessAnalyzerServiceRole	Gerenciadas pela AWS	Nenhum	Allow Access Analyzer to analyze resou...
AdministratorAccess	Gerenciadas pela AWS - função de t...	Política de permissões (3)	Provides full access to AWS services an...
AdministratorAccess-Ampl...	Gerenciadas pela AWS	Nenhum	Grants account administrative permissi...
AdministratorAccess-AWS...	Gerenciadas pela AWS	Nenhum	Grants account administrative permissi...
AIOpsAssistantPolicy	Gerenciadas pela AWS	Nenhum	Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy	Gerenciadas pela AWS	Nenhum	Grants full access to Amazon AI Opera...
AIOpsOperatorAccess	Gerenciadas pela AWS	Nenhum	Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess	Gerenciadas pela AWS	Nenhum	Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSe...	Gerenciadas pela AWS	Nenhum	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	Gerenciadas pela AWS	Nenhum	Grants full access to AlexaForBusiness ...

1.2. No canto direito, clique em "Criar política".

Especifique permissões

Adicione permissões selecionando serviços, ações, recursos e condições. Crie instruções de permissão usando o editor JSON.

Editor de políticas

Visual JSON Ações

Selecione um serviço

Especifique quais ações podem ser executadas em recursos específicos em um serviço.

Serviço

Escolher um serviço

+ Adicionar mais permissões

Cancelar Próximo

1.3. No canto superior esquerdo, ao lado de "Editor de Políticas", selecione a opção "JSON".

1.4. Na mesma atividade em que você acessou, procure e baixe o arquivo "Política IAM". Abra o arquivo com o Bloco de Notas. Copie a política e cole no "Editor de Políticas" e clique em "Próximo".

aws Search [Alt+S] Global sabrina.idv

IAM > Políticas > Criar política

Etapa 1
● **Especifique permissões**
○ Etapa 2
○ Revisar e criar

Especifique permissões Informações

Adicione permissões selecionando serviços, ações, recursos e condições. Crie instruções de permissão usando o editor JSON.

Editor de políticas

Visual JSON

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": [],  
8       "Resource": []  
9     }  
10  ]  
11 }
```

Editar instruções

Statement1

Adicionar ações

Escolher um serviço

Disponível

- AI Operations
- AMP
- API Gateway
- API Gateway V2
- ARC Zonal Shift
- ASC
- Access Analyzer
- Account

CloudShell Comentários

© 2025, Amazon Web Services, Inc. ou suas afiliadas. Privacidade

IAM > Políticas > Criar política

```
11   "ec2:TerminateInstances",  
12   "ec2:DescribeRegions"  
13 },  
14 "Resource": "*" ]  
15 }  
16 ]  
17 }
```

Selecione uma instrução existente na política ou adicione uma nova instrução.

+ Adicionar nova instrução

+ Adicionar nova instrução

JSON Ln 17, Col 1 5925 de 6144 caracteres restantes

Segurança: 0 Erros: 0 Avisos: 0 Sugestões: 0

Cancelar **Próximo**

O objetivo dessa política é conceder permissões para a função Lambda gerenciar instâncias EC2. Ela permite que a função Lambda realize ações específicas, como descrever e terminar instâncias EC2, além de criar e manipular logs no CloudWatch. Com essa política, a função Lambda será capaz de automatizar a terminação de instâncias EC2 em diversas regiões da AWS de forma segura e controlada, de acordo com as permissões atribuídas.

IAM > Políticas > Criar política

Nome da política

Insira um nome significativo para identificar esta política.

PolíticaTerminarEC2

Máximo de 128 caracteres. Use caracteres alfanuméricos e '+-=,@-._'.

Descrição — opcional

Adicione uma breve explicação para esta política.

Laboratório para automacao de finalizar uma instancia EC2

Máximo de 1.000 caracteres. Use caracteres alfanuméricos e '+-=,@-._'.

Permissões definidas nesta política Informações

Editar

As permissões definidas neste documento de política especificam quais ações são permitidas ou proibidas. Para definir permissões para uma identidade do IAM (usuário, grupo de usuários ou função), anexe uma política a ela.

Pesquisar

Permitir (2 de 440 serviços)Mostrar os 438 serviços restantes

Serviço	Nível de acesso	Recurso	Condição da solicitação
CloudWatch Logs	Limitado: Gravação	Todos os recursos	None
EC2	Limitado: Lista, Gravação	Todos os recursos	None

IAM > Políticas > Criar política

Permissões definidas nesta política Informações

Editar

As permissões definidas neste documento de política especificam quais ações são permitidas ou proibidas. Para definir permissões para uma identidade do IAM (usuário, grupo de usuários ou função), anexe uma política a ela.

Pesquisar

Permitir (2 de 440 serviços)Mostrar os 438 serviços restantes

Serviço	Nível de acesso	Recurso	Condição da solicitação
CloudWatch Logs	Limitado: Gravação	Todos os recursos	None
EC2	Limitado: Lista, Gravação	Todos os recursos	None

Adicionar tags - opcional Informações

Nenhuma tag associada ao recurso.

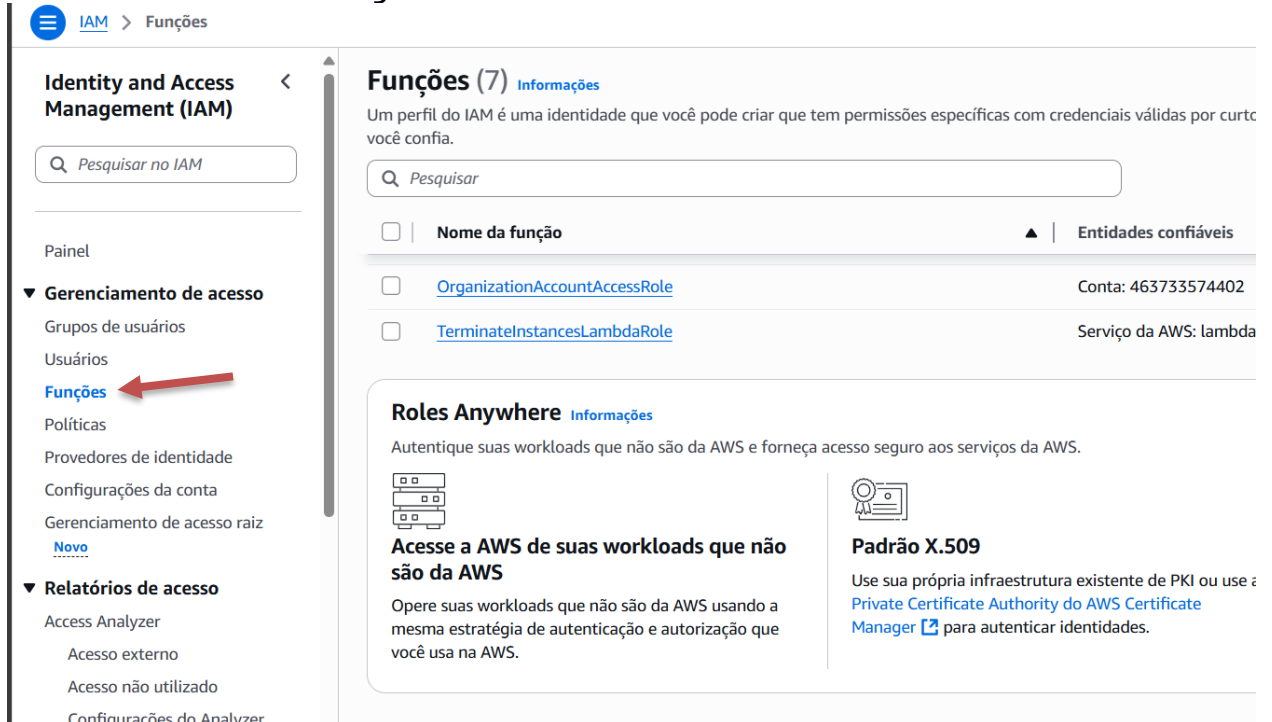
Adicione uma nova tag

Você pode adicionar até mais 50 tags.

CancelarAnteriorCriar política

1.6. Role para baixo e clique em **"Criar política"**.

2. Criar role/Funções



Identity and Access Management (IAM)

Painel

- ▼ Gerenciamento de acesso
 - Grupos de usuários
 - Usuários
 - Funções**
 - Políticas
 - Provedores de identidade
 - Configurações da conta
 - Gerenciamento de acesso raiz
 - [Novo](#)
- ▼ Relatórios de acesso
 - Access Analyzer
 - Acesso externo
 - Acesso não utilizado
 - Configurações do Analyzer

Funções (7) [Informações](#)

Um perfil do IAM é uma identidade que você pode criar que tem permissões específicas com credenciais válidas por curto período de tempo.

[Pesquisar](#)

<input type="checkbox"/>	Nome da função	Entidades confiáveis
<input type="checkbox"/>	OrganizationAccountAccessRole	Conta: 463733574402
<input type="checkbox"/>	TerminateInstancesLambdaRole	Serviço da AWS: lambda

Roles Anywhere [Informações](#)

Autentique suas workloads que não são da AWS e forneça acesso seguro aos serviços da AWS.

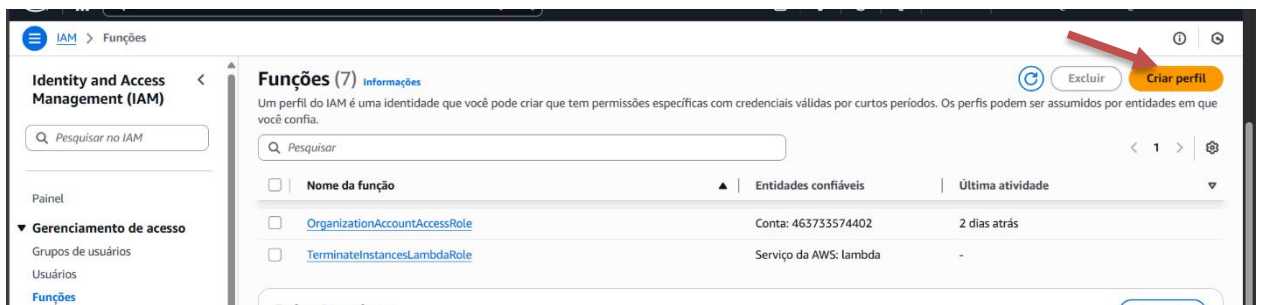
Acesse a AWS de suas workloads que não são da AWS

Opere suas workloads que não são da AWS usando a mesma estratégia de autenticação e autorização que você usa na AWS.

Padrão X.509

Use sua própria infraestrutura existente de PKI ou use o [Private Certificate Authority do AWS Certificate Manager](#) para autenticar identidades.

2.1. No console do IAM, no menu lateral, selecione **"Funções"** e clique em **"Criar perfil"**. A criação de uma função (role) no IAM é necessária para associar permissões específicas a uma entidade, como uma função Lambda ou EC2. A função define o que a entidade pode fazer dentro da AWS, garantindo que os serviços ou recursos possam acessar apenas os recursos necessários de forma controlada e segura.



Identity and Access Management (IAM)

Painel

- ▼ Gerenciamento de acesso
 - Grupos de usuários
 - Usuários
 - Funções**
 - Políticas
 - Provedores de identidade
 - Configurações da conta
 - Gerenciamento de acesso raiz
 - [Novo](#)
- ▼ Relatórios de acesso
 - Access Analyzer
 - Acesso externo
 - Acesso não utilizado
 - Configurações do Analyzer

Funções (7) [Informações](#)

Um perfil do IAM é uma identidade que você pode criar que tem permissões específicas com credenciais válidas por curtos períodos. Os perfis podem ser assumidos por entidades em que você confia.

[Pesquisar](#)

<input type="checkbox"/>	Nome da função	Entidades confiáveis	Última atividade
<input type="checkbox"/>	OrganizationAccountAccessRole	Conta: 463733574402	2 dias atrás
<input type="checkbox"/>	TerminateInstancesLambdaRole	Serviço da AWS: lambda	-

Roles Anywhere [Informações](#)

Autentique suas workloads que não são da AWS e forneça acesso seguro aos serviços da AWS.

Acesse a AWS de suas workloads que não são da AWS

Opere suas workloads que não são da AWS usando a mesma estratégia de autenticação e autorização que você usa na AWS.

Padrão X.509

Use sua própria infraestrutura existente de PKI ou use o [Private Certificate Authority do AWS Certificate Manager](#) para autenticar identidades.

2.2. No campo **"Tipo de entidade confiável"**, selecione **"Serviço da AWS"** e, em seguida, escolha **"Lambda"** no campo **"Serviço ou caso de uso"** e por fim clique em **"Próximo"**. Ao selecionar **"Serviço da AWS"** e **"Lambda"**, você está permitindo

que a função Lambda assuma essa role para executar tarefas automatizadas, como terminar instâncias EC2.

Etapa 1 > IAM > Funções > Criar perfil

Etapa 1
● Seleccionar entidade confiável

Etapa 2
○ Adicionar permissões

Etapa 3
○ Nomear, revisar e criar

Seleccionar entidade confiável

Informações

Tipo de entidade confiável

- ☒ **Serviço da AWS**
Permitir que serviços da AWS, como o EC2, Lambda ou outros executem ações nessa conta.
- ☐ **Conta da AWS**
Permitir que entidades em outras contas da AWS pertencentes a você ou a terceiros executem ações nessa conta.
- ☐ **Identidade Web**
Permite que os usuários federados pelo provedor de identidade da Web externo especificado assumam essa função para executar ações nessa conta.
- ☐ **Federação SAML 2.0**
Permitir que os usuários federados com o SAML 2.0 de um diretório corporativo executem ações nessa conta.
- ☐ **Política de confiança personalizada**
Crie uma política de confiança personalizada para permitir que outras pessoas executem ações nessa conta.

Caso de uso
Permitir que um serviço da AWS, como o EC2, o Lambda ou outros executem ações nessa conta.

Serviço ou caso de uso
Escolha um serviço ou caso de uso

Caso de uso
Permitir que um serviço da AWS, como o EC2, o Lambda ou outros executem ações nessa conta.

Serviço ou caso de uso
Lambda

Escolha um caso de uso para o serviço especificado.

Caso de uso
☒ **Lambda**
Allows Lambda functions to call AWS services on your behalf.

Cancelar Próximo

2.3. Na próxima etapa, pesquise pela política "**PolíticaTerminarEC2-<seu nome e sobrenome>**" que você criou na etapa 1.

Etapa 1 > IAM > Funções > Criar perfil

Etapa 1
● Seleccionar entidade confiável

Etapa 2
● Adicionar permissões

Etapa 3
○ Nomear, revisar e criar

Adicionar permissões

Informações

Políticas de permissões (1/1055) Informações

Escolha uma ou mais políticas para anexar à sua nova função.

Filtrar por Tipo
Todos os tipos 4 correspondências

Política

	Nome da política	Tipo	Descrição
<input type="checkbox"/>	PolíticaTerminarEC2-...	Gerenciadas pelo cliente	-
<input type="checkbox"/>	PolíticaTerminarEC2-...	Gerenciadas pelo cliente	-
<input type="checkbox"/>	PolíticaTerminarEC2-...	Gerenciadas pelo cliente	-
<input checked="" type="checkbox"/>	PolíticaTerminarEC2-...	Gerenciadas pelo cliente	Laboratorio para automocao de finaliz...

Definir limite de permissões - opcional

Cancelar Anterior Próximo

2.4. Selecione a política e clique em "**Próximo**". Ao anexar a política ao role, você está garantindo que a função Lambda tenha as permissões necessárias para terminar instâncias EC2 e interagir com outros serviços, conforme definido na política criada.

2.5. Por último, no campo "**Nome da função**", digite "**RoleTerminarEC2-<seu nome e sobrenome>**"

Etapa 1
● Selecionar entidade confiável

Etapa 2
● Adicionar permissões

Etapa 3
● **Nomear, revisar e criar**

Nomear, revisar e criar

Detalhes da função

Nome da função
Insira um nome significativo para identificar esta função.

RoleTerminarEC2

Máximo de 64 caracteres. Use caracteres alfanuméricos e "+,=,@,-,.". Máximo de 64 caracteres. Use caracteres alfanuméricos e "+,=,@,-,.".

Descrição
Adicione uma breve explicação para esta função.

Allows Lambda functions to call AWS services on your behalf.

Máximo de 1000 caracteres. Use letras (A-Z e a-z), números (0-9), tabulações, novas linhas ou qualquer um dos seguintes caracteres: "_+=, @-/\[\]{}\$%^&*~". Máximo de 1000 caracteres. Use letras (A-Z e a-z), números (0-9), tabulações, novas linhas ou qualquer um dos seguintes caracteres: "_+=, @-/\[\]{}\$%^&*~".

Etapa 1: Selecionar entidades confiáveis Editar

Política de confiança

```

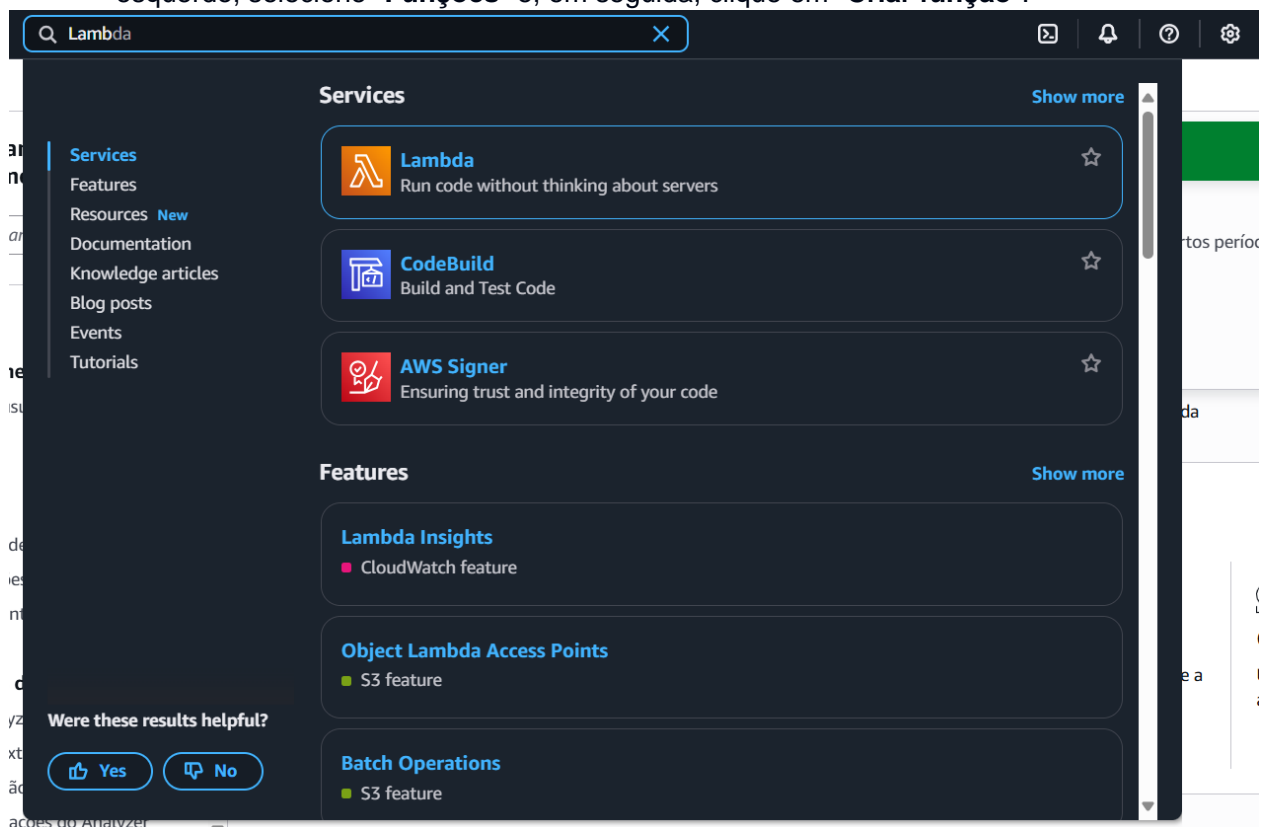
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {

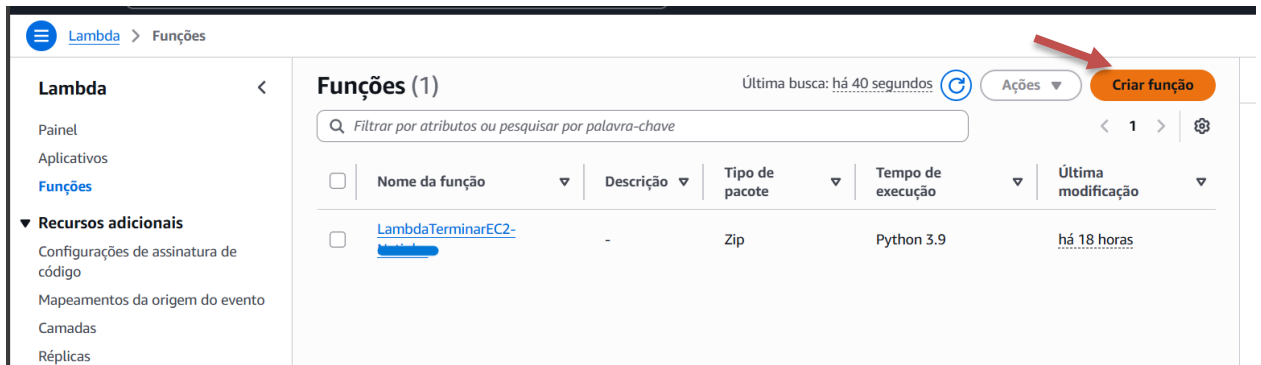
```

2.6. Role para baixo e clique em **"Criar perfil"** para finalizar a criação do role.

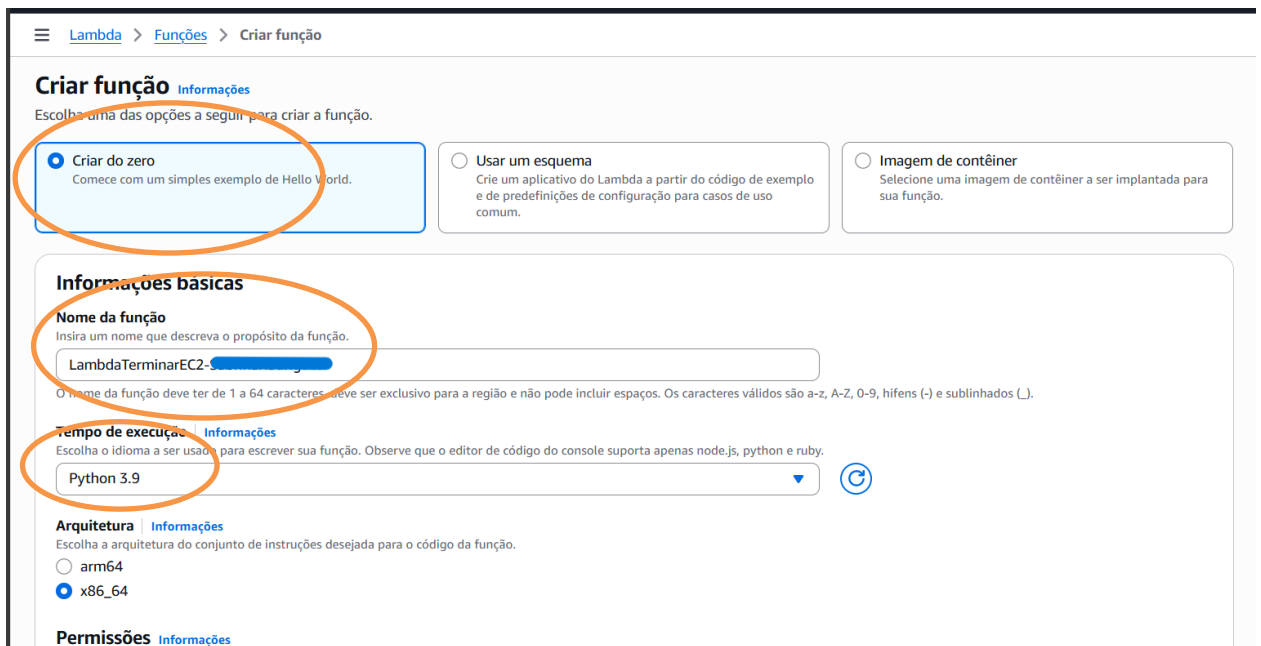
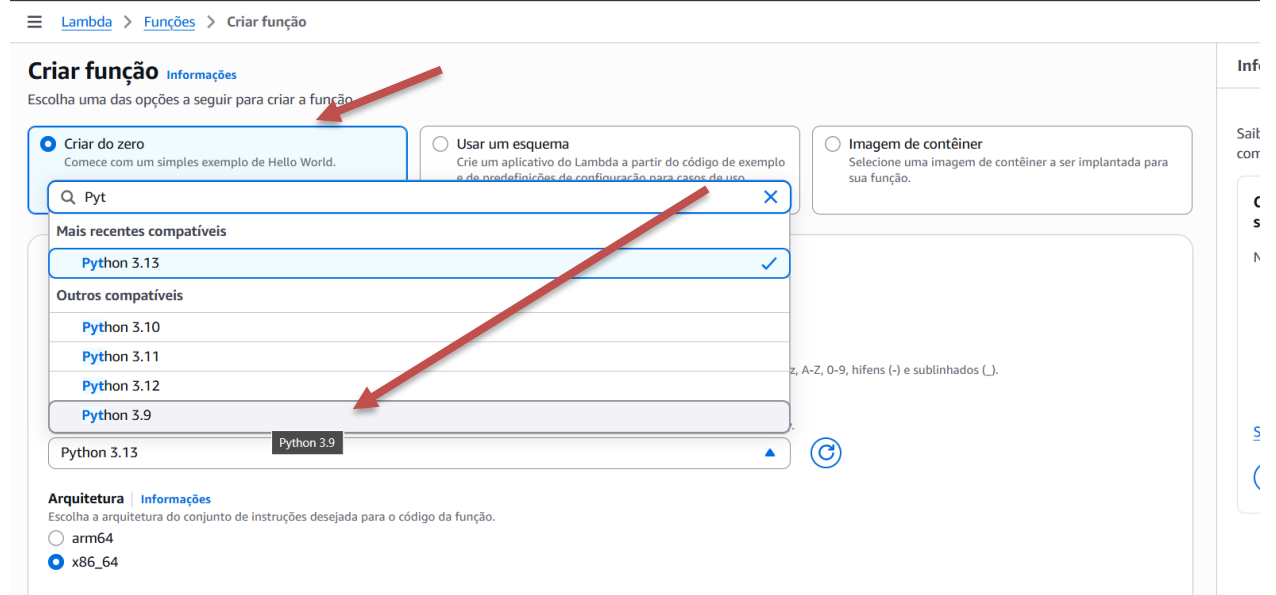
3. Criação de uma função do Lambda

3.1. Acesse o serviço Lambda no console da AWS e clique em **"Criar função"**. Caso já tenha funções Lambda criadas, clique no menu hambúrguer no canto superior esquerdo, selecione **"Funções"** e, em seguida, clique em **"Criar função"**.





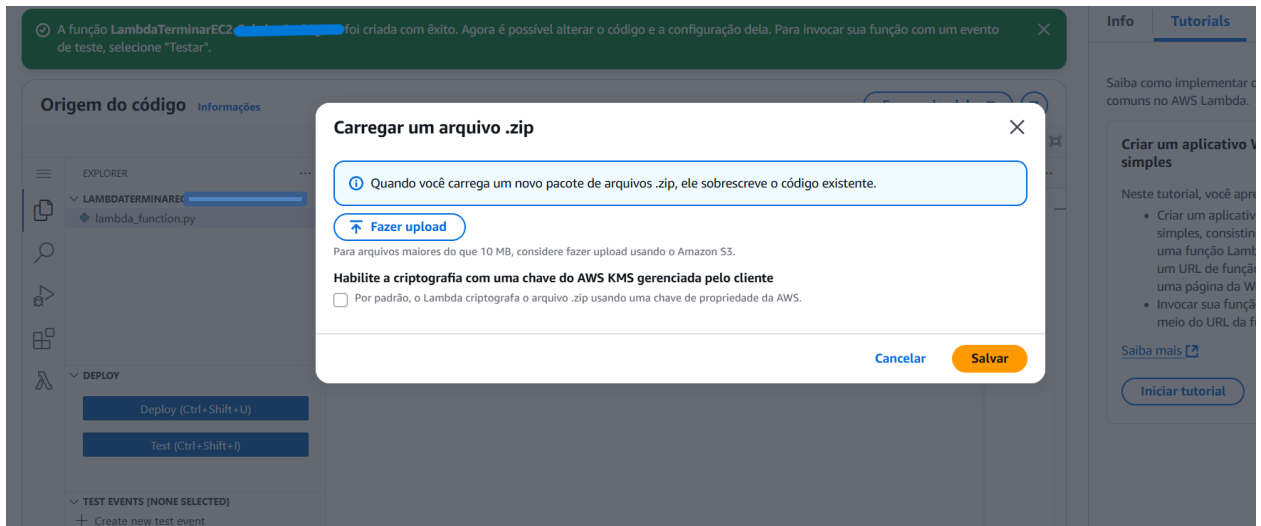
3.2. Na tela de "Criar função", selecione a opção "Criar do zero"



- 3.3. No campo "Nome da função", digite "LambdaTerminarEC2-<seu nome e sobrenome>"
- 3.4. Em "Tempo de execução", selecione "Python 3.9"
- 3.5. Em seguida, expanda a opção "Alterar a função de execução padrão", selecione "Usar uma função existente" e, no campo exibido "Função existente", escolha a função "RoleTerminarEC2-<seu nome e sobrenome>" que foi criada anteriormente. Essas etapas garantem que a função Lambda seja criada com o nome adequado e as permissões corretas para interagir com os recursos da AWS.

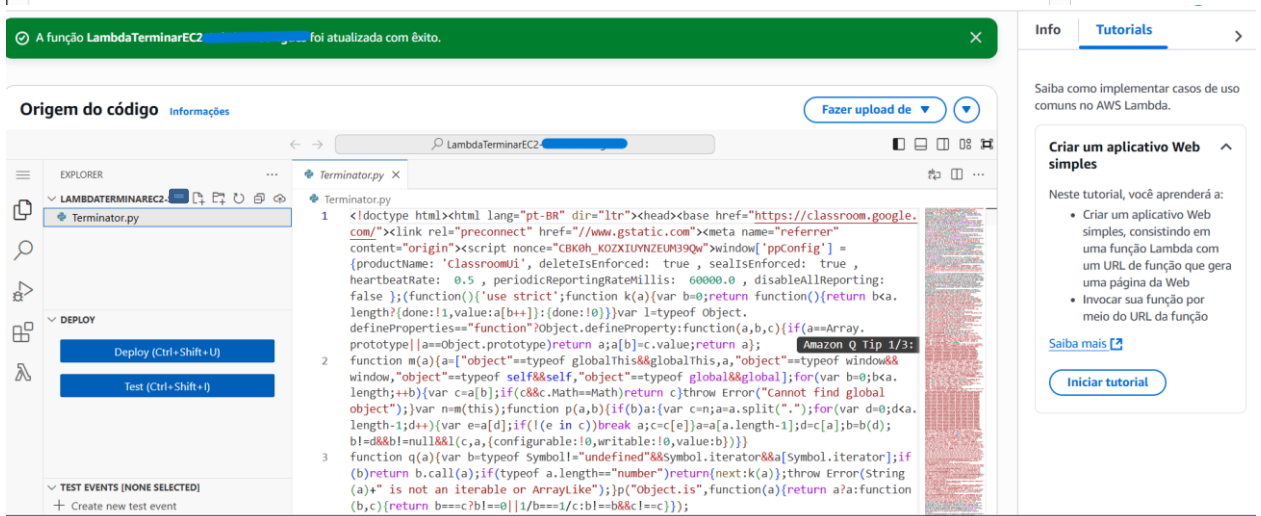
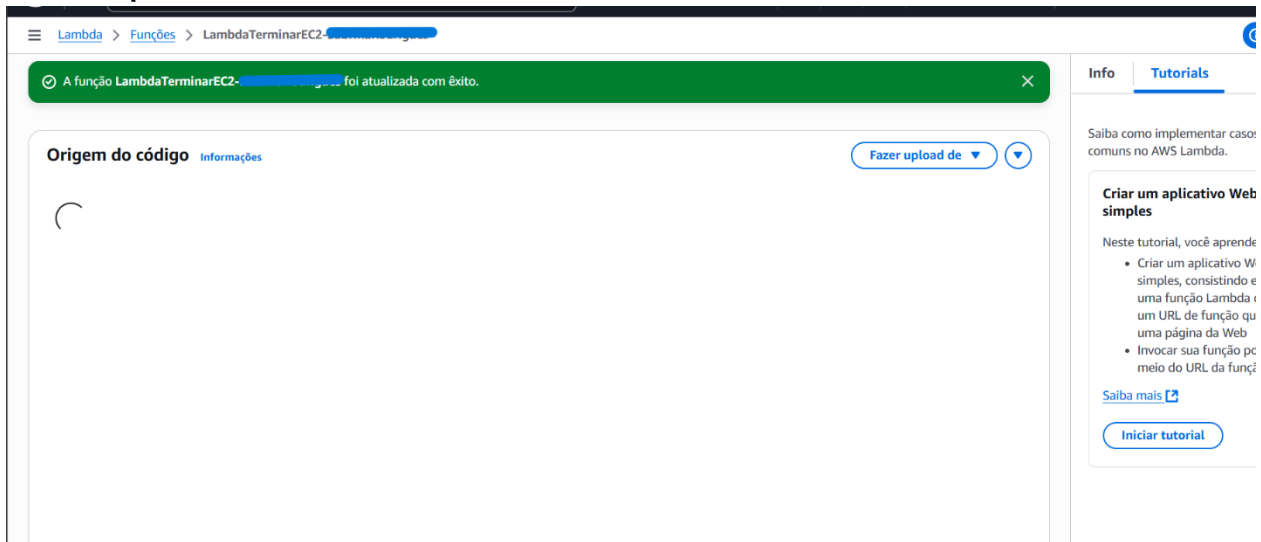
- 3.6. Baixe o script "Terminator", está disponível no Google Salas de aula. O mesmo contém o código necessário para deletar as instâncias EC2.

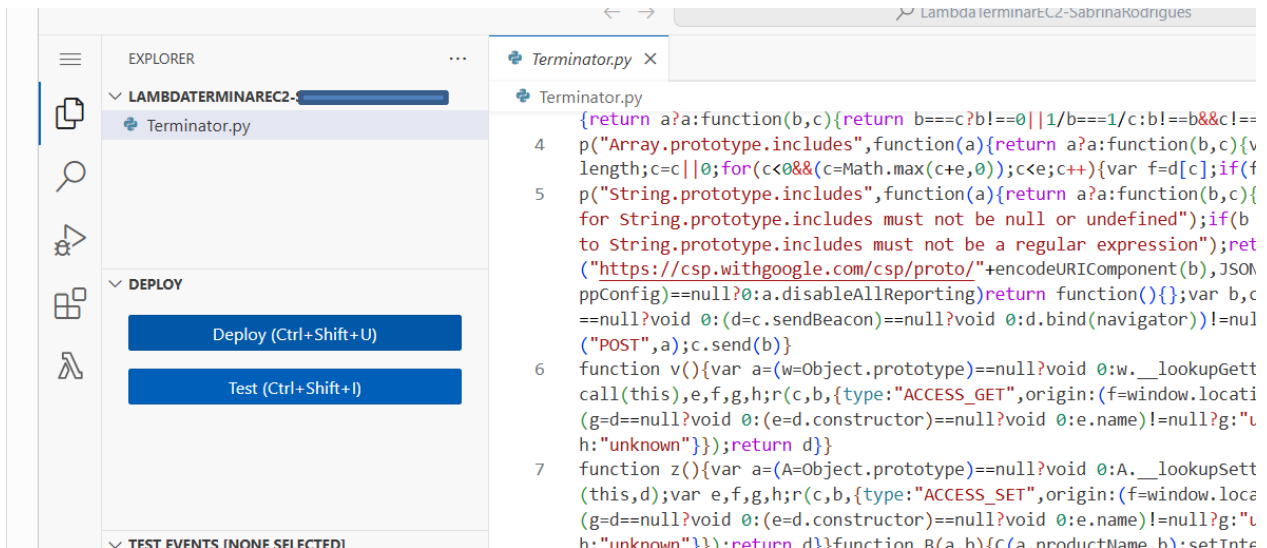
4. Script lambda



4.1. Na seção "Origem do código", no canto direito, clique em "Fazer upload de".

4.2. Será aberta uma opção de seleção. Escolha "Arquivos .zip" e clique em "Fazer upload".



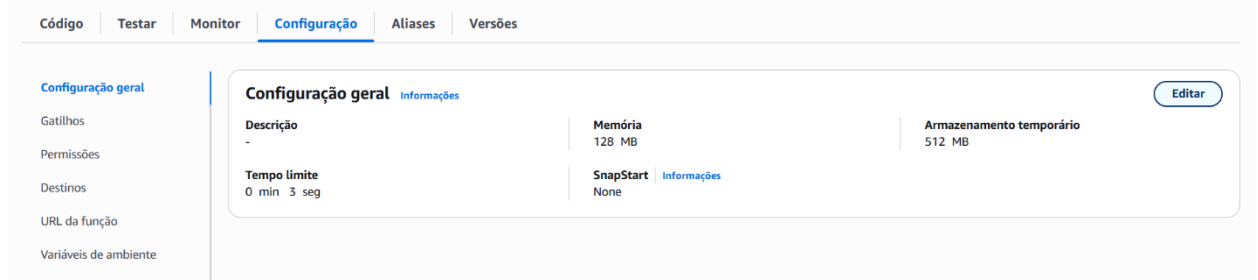


4.3. Procure no seu computador o script **"Terminator"** que foi baixado anteriormente.

4.4. Após selecionar o arquivo, clique em **"Salvar"**.

4.5. Abaixo de **"Origem do código"**, selecione o arquivo **"Terminator.py"** para que o código seja exibido. Após verificar o código, clique no botão **"Deploy"** para garantir que as alterações foram realizadas com sucesso.

4.6. Acima da seção **"Origem do código"**, há um menu de opções. Selecione **"Configuração"**. Abaixo, um menu inferior será exibido. Clique em **"Configuração geral"** e, ao lado direito, clique em **"Editar"** para modificar as configurações da função Lambda.



4.7. No final das configurações, localize o campo **"Tempo limite"** e altere o valor de **3 segundos** para **10 segundos**. O tempo limite define quanto tempo a função Lambda pode executar antes de ser interrompida. Aumentar o tempo limite para 10 segundos é necessário porque a função que você está utilizando pode precisar de mais tempo para terminar o processo de terminação das instâncias EC2, especialmente se houver muitas instâncias ou se a resposta da AWS demorar um pouco mais. Com um tempo maior, a função terá mais tempo para concluir a execução sem ser interrompida prematuramente.

Defina a memória entre 128 MB e 10240 MB

Armazenamento temporário | [Informações](#)

Você pode configurar até 10 GB de armazenamento temporário (/ tmp) para sua função. [Visualizar preço](#)

512 MB

Defina o armazenamento temporário (/ tmp) com um valor entre 512 MB e 10.240 MB.

SnapStart | [Informações](#)

Reduza o tempo de inicialização configurando o Lambda para armazenar em cache um snapshot da função após a inicialização dela. Para avaliar se o código da função é SnapStart. Para visualizações Python e .NET, [veja os preços](#).

None

Tempos de execução compatíveis: .NET 8 (C#/F#/PowerShell), Java 11, Java 17, Java 21, Python 3.12, Python 3.13.

Tempo limite

0 min 10 seg

Papel de execução

Escolha uma função que defina as permissões da sua função. Para criar uma função personalizada, acesse o [console do IAM](#).

☒ Usar uma função existente

☐ Criar uma função a partir da política da AWS templates

Função existente

Escolha uma função existente que você criou para ser usada com esta função do Lambda. A função deve ter permissão para fazer upload de logs no Amazon CloudWatch

RoleTerminarEC2

4.8. Clique em "**Salvar**" para que as alterações sejam aplicadas com sucesso.

4.9. No console da função Lambda, vá até a aba "**Código**" e verifique que o nome do arquivo é Terminator.py. Role para baixo até a seção "**Configurações de tempo de execução**", clique em "**Editar**" e, no campo "**Manipulador**", modifique para "**Terminator.lambda_handler**", usando o nome do arquivo sem o .py. Depois, clique em "**Salvar**".

Configurações de tempo de execução | [Informações](#)

Tempo de execução

Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Python 3.9

Novo tempo de execução disponível

Um novo tempo de execução está disponível para o idioma de sua função. Python 3.13

Manipulador | [Informações](#)

Terminator.lambda_handler

Arquitetura | [Informações](#)

Escolha a arquitetura do conjunto de instruções desejada para o código da função.

☒ x86_64

☐ arm64

Você pode alterar o tempo de execução da função ou a arquitetura do conjunto de instruções em uma só atualização. Para atualizar ambos, repita o processo de atualização.

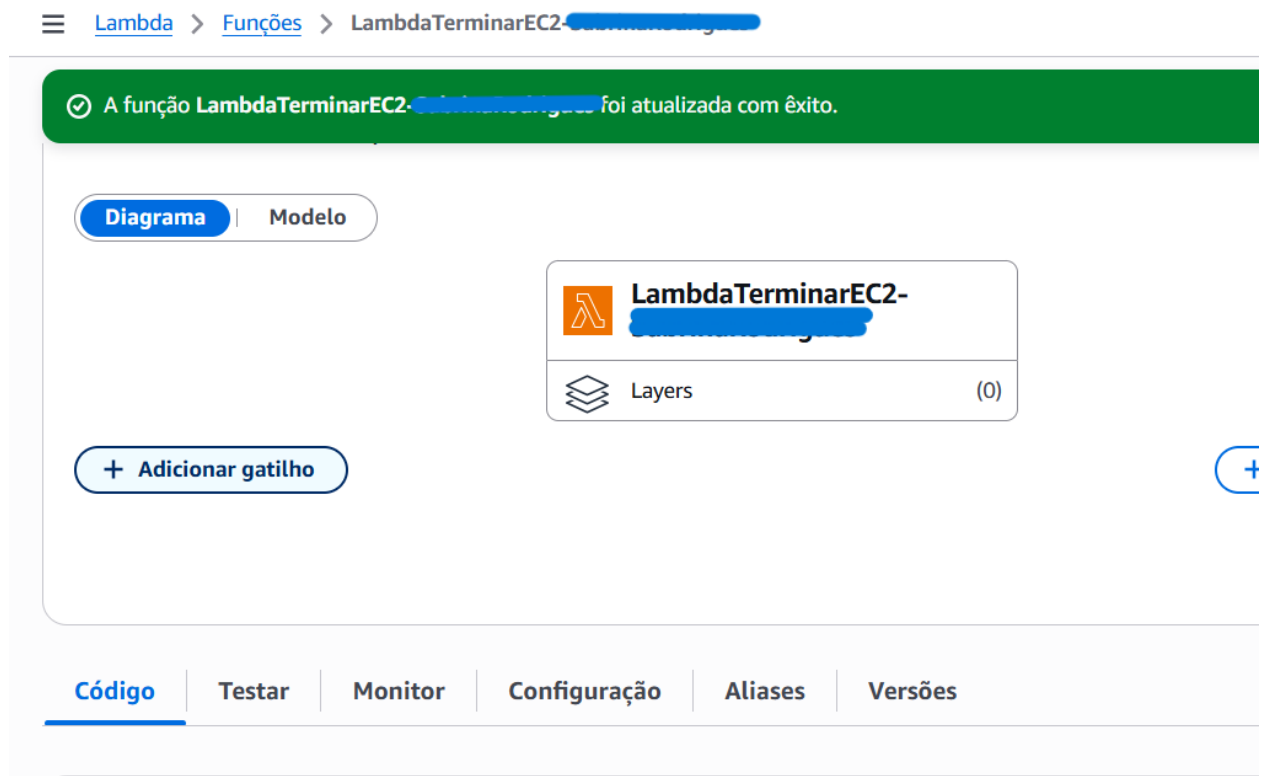
Para que a função Lambda seja executada corretamente, é necessário configurar o campo Manipulador (Handler) de acordo com o nome do arquivo principal e da função que será executada. O manipulador informa ao AWS Lambda qual arquivo e qual função deve ser usado como ponto de entrada da execução. Essa configuração é essencial para que o Lambda consiga localizar e executar corretamente o código. Caso o manipulador esteja incorreto, a execução resultará em erro.

5. Agendamento com EventBridge

Com o Lambda configurado corretamente, será necessário criar um gatilho para acionar a

função. Vamos utilizar o Amazon EventBridge para agendar a ativação do Lambda, garantindo que ele seja executado automaticamente em intervalos definidos

- 5.1. No canto superior da página da função Lambda, clique em "**Adicionar gatilho**" para configurar o evento que acionará a função.




- 5.2. Na seção "**Configuração do gatilho**", pesquise por EventBridge e selecione-o. Em seguida, na seção "**Regra**", clique em "**Criar uma regra**" para configurar o agendamento


Adicionar gatilho

Configuração do gatilho [Informações](#)


Selecione uma origem


Batch/bulk data processing


 **EventBridge (CloudWatch Events)**
aws asynchronous schedule management-tools


 **SQS**
aws event-source-mapping polling queue

Real-time/streaming data

 **Amazon DocumentDB**
aws database event-source-mapping MongoDB nosql

 **Apache Kafka**
aws analytics Confluent event-source-mapping streaming

 **DynamoDB**
aws database event-source-mapping nosql polling

 **Kinesis**

- 5.3. No campo "**Nome da regra**", insira o nome "**GatilhoTerminarEC2-<seu nome e sobrenome>**" para identificar de forma única a regra criada.
- 5.4. Em "**Tipo de regra**", marque a opção "**Expressão de agendamento**". Isso abrirá o campo correspondente, onde você pode criar expressões Cron ou Rate para agendar a ativação da função Lambda. Expressão Cron: Permite definir um agendamento mais complexo, como uma execução em horários específicos. Já Rate define um intervalo fixo de tempo para a execução da função, como a cada 5 minutos, uma vez por dia.
- 5.5. No campo "**Expressão de programação**", você pode definir quando a função Lambda será acionada:
 - 5.5.1. Para agendar a execução a cada 12 horas, utilize a expressão **rate(12 hours)**
 - 5.5.2. Se preferir agendar a execução a cada 5 minutos, utilize a expressão **rate(5 minutes)**

Nome da regra
Insira um nome exclusivo de identificação da sua regra.

GatilhoTerminarEC2-XXXXXXXXXX

Descrição da regra
Forneça uma descrição opcional para a regra.

Tipo de regra
Ação o destino com base em um padrão de evento ou programação automática.

☐ Padrão de evento

☒ Expressão de programação

Expressão de programação
Ação automaticamente seu destino em uma programação automatizada usando expressões [Cron ou rate](#). As expressões Cron estão em UTC.

rate(5 minutes)

Por exemplo, rate(1 day), cron(0 17 ? * MON-FRI *)

O Lambda adicionará as permissões necessárias para que Amazon EventBridge (CloudWatch Events) seja capaz de invocar a função do Lambda a partir deste acionador Lambda.

- 5.6. Por fim, clique em "**Adicionar**" para concluir a configuração do gatilho e garantir que a função Lambda seja acionada conforme o agendamento definido.
- 5.7. Caso você tenha escolhido o agendamento de 5 minutos para verificar a função em ação, basta criar uma instância EC2 e aguardar a execução da função Lambda. A função será acionada automaticamente após o intervalo de tempo configurado e realizará a ação de terminação da instância EC2 conforme o esperado

☰ [Lambda](#) > [Funções](#) > LambdaTerminarEC2-XXXXXXXXXX

LambdaTerminarEC2-XXXXXXXXXX [Controlar](#) [Copiar ARN](#) [Ação](#)

✔ O gatilho GatilhoTerminarEC2-XXXXXXXXXX foi adicionado com êxito à função LambdaTerminarEC2-XXXXXXXXXX. A função agora recebe eventos do gatilho.

▼ **Visão geral da função** [Informações](#)

[Diagrama](#) [Modelo](#)

EventBridge (CloudWatch Events) [+ Adicionar destino](#)

[+ Adicionar gatilho](#)

[Exportar para o Infrastructure Composer](#) [Fazer download](#)

Descrição
-

Última modificação
há 10 minutos

ARN da função
 arn:aws:lambda:us-east-2:281156594695:function:LambdaTerminarEC2-XXXXXXXXXX

URL da função [Informações](#)
-

[Código](#) [Testar](#) [Monitor](#) [Configuração](#) [Aliases](#) [Versões](#)

6. Exclusão dos recursos

- 6.1. Para deletar a função Lambda, acesse o menu hambúrguer no canto superior esquerdo do console da AWS, clique em "**Funções**" na seção Lambda, selecione a função desejada, clique em "**Ações**" no topo da página e, no menu suspenso,

escolha "**Excluir**". Em seguida, confirme a exclusão quando solicitado para remover a função Lambda permanentemente.

- 6.2. Acesse o painel do IAM, no menu à esquerda, procure por "**Funções**", pesquise pela função "**RoleTerminarEC2-<seu nome e sobrenome>**", selecione-a e, no canto superior, clique no botão "**Excluir**". Em seguida, confirme a exclusão quando solicitado para remover a role permanentemente.
- 6.3. Agora, acesse "**Políticas**" no menu à esquerda, pesquise pela política "**PoliticaTerminarEC2-<seu nome e sobrenome>**", selecione-a e clique no botão "**Excluir**". Quando aparecer a janela de confirmação, siga os passos para concluir a remoção.
- 6.4. Por fim, pesquise por "**Amazon EventBridge**" na barra de pesquisa, no menu à esquerda, na seção "**Barramentos**", clique em "**Regras**", selecione a sua regra e clique em "**Excluir**" para removê-la permanentemente.
- 6.5. No canto superior direito do console de gerenciamento da AWS, clique em cima do seu nome de usuário que está em azul, depois clique em "**Sair**" que aparece mais abaixo.
- 6.6. Pronto! Laboratório concluído com sucesso!