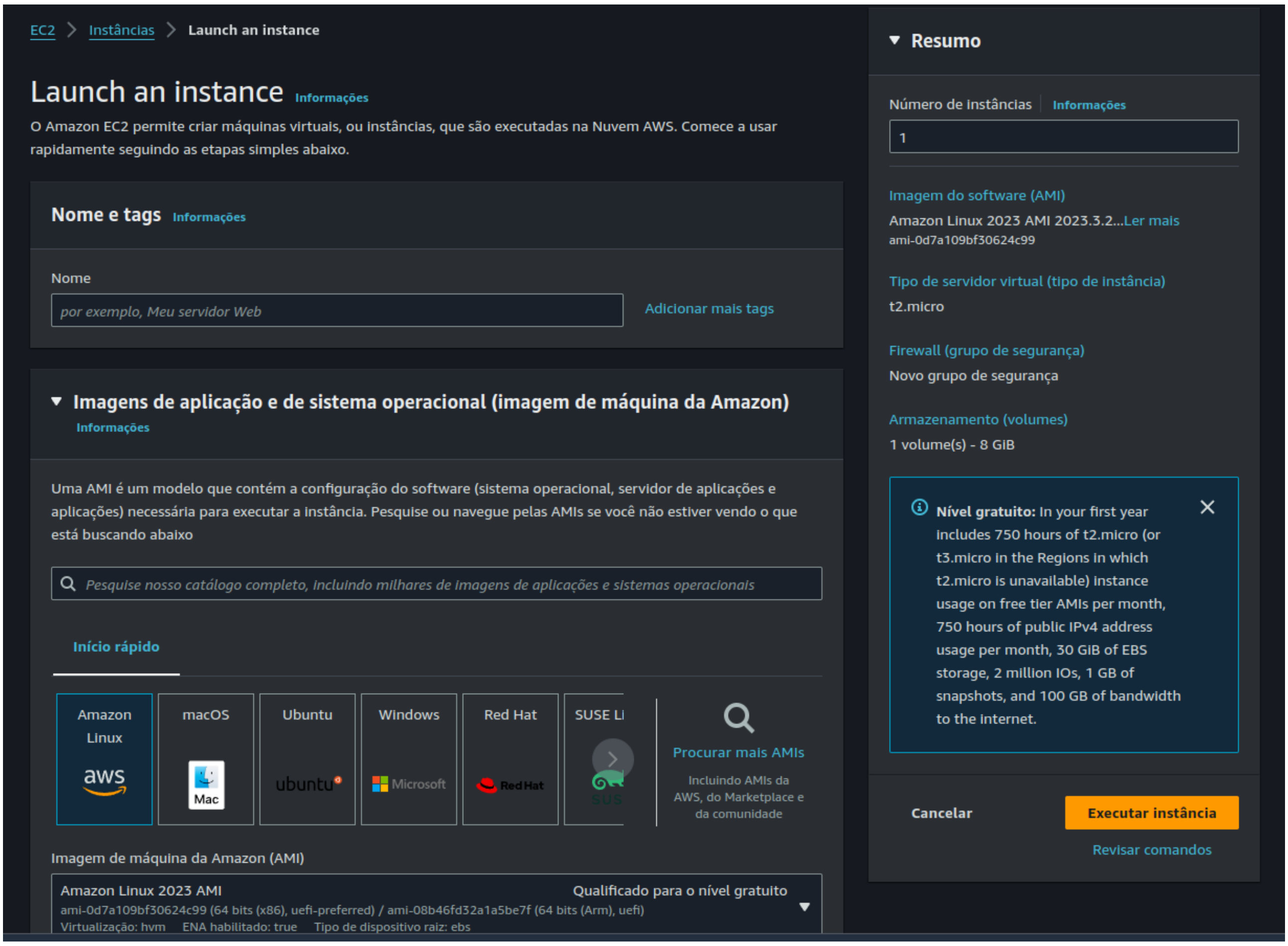
CI/CD to EC2

Step 1: Create a EC2 instance and download the key pais



Launch an instance

O Amazon EC2 permite criar máquinas virtuais, ou instâncias, que são executadas na Nuvem AWS. Comece a usar rapidamente seguindo as etapas simples abaixo.

Nome e tags

Nome: por exemplo, Meu servidor Web

Imagens de aplicação e de sistema operacional (imagem de máquina da Amazon)

Uma AMI é um modelo que contém a configuração do software (sistema operacional, servidor de aplicações e aplicações) necessária para executar a instância. Pesquise ou navegue pelas AMIs se você não estiver vendo o que está buscando abaixo.

Pesquise nosso catálogo completo, incluindo milhares de imagens de aplicações e sistemas operacionais

Imagem de máquina da Amazon (AMI)

Amazon Linux 2023 AMI — Qualificado para o nível gratuito
ami-0d7a109bf30624c99 (64 bits (x86), uefi-preferred) / ami-08b46fd32a1a5be7f (64 bits (Arm), uefi)
Virtualização: hvm ENA habilitado: true Tipo de dispositivo raiz: ebs

Resumo

Número de instâncias: 1

Imagem do software (AMI)
Amazon Linux 2023 AMI 2023.3.2...Ler mais
ami-0d7a109bf30624c99

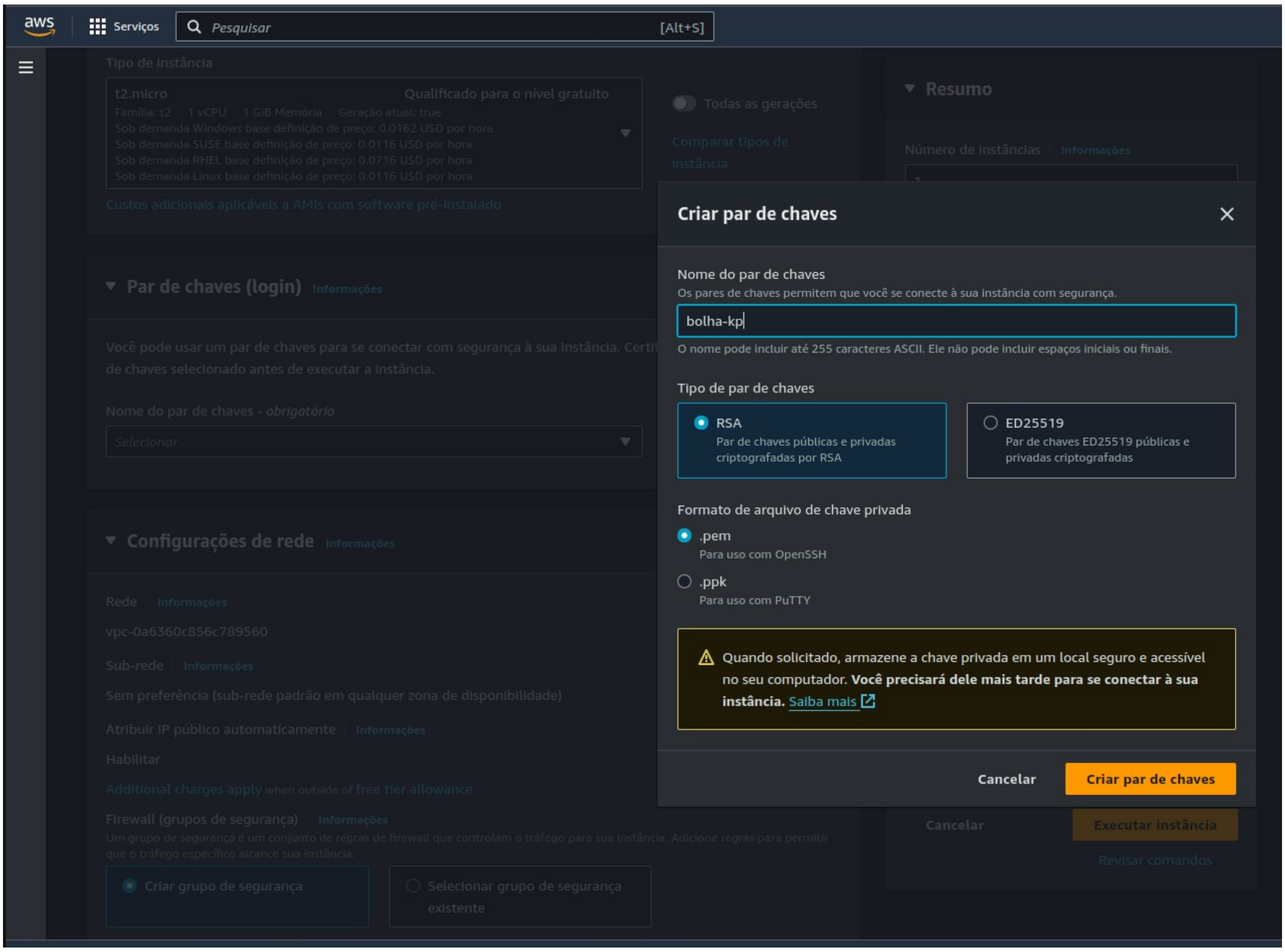
Tipo de servidor virtual (tipo de instância)
t2.micro

Firewall (grupo de segurança)
Novo grupo de segurança

Armazenamento (volumes)
1 volume(s) - 8 GiB

Nível gratuito: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

.



Serviços · Pesquisar [Alt+S]

Tipo de instância

t2.micro Qualificado para o nível gratuito
Família: t2 1 vCPU 1 GiB Memória Geração atual: true
Sob demanda Windows base definição de preço: 0.0162 USD por hora
Sob demanda SUSE base definição de preço: 0.0116 USD por hora
Sob demanda RHEL base definição de preço: 0.0716 USD por hora
Sob demanda Linux base definição de preço: 0.0116 USD por hora

Todas as gerações

Comparar tipos de instância

Custos adicionais aplicáveis a AMIs com software pré-instalado

▼ Par de chaves (login) Informações

Você pode usar um par de chaves para se conectar com segurança à sua instância. Certi
de chaves selecionado antes de executar a instância.

Nome do par de chaves - *obrigatório*

Selecionar ▼

▼ Configurações de rede Informações

Rede | Informações

vpc-0a6360c856c789560

Sub-rede | Informações

Sem preferência (sub-rede padrão em qualquer zona de disponibilidade)

Atribuir IP público automaticamente | Informações

Habilitar

Additional charges apply when outside of free tier allowance

Firewall (grupos de segurança) | Informações

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

● Criar grupo de segurança ○ Selecionar grupo de segurança existente

▼ Resumo

Número de instâncias | Informações

1

Cancelar · Executar instância

Revisar comandos

Criar par de chaves ✕

Nome do par de chaves

Os pares de chaves permitem que você se conecte à sua instância com segurança.

bolha-kp

O nome pode incluir até 255 caracteres ASCII. Ele não pode incluir espaços iniciais ou finais.

Tipo de par de chaves

● RSA
Par de chaves públicas e privadas criptografadas por RSA

○ ED25519
Par de chaves ED25519 públicas e privadas criptografadas

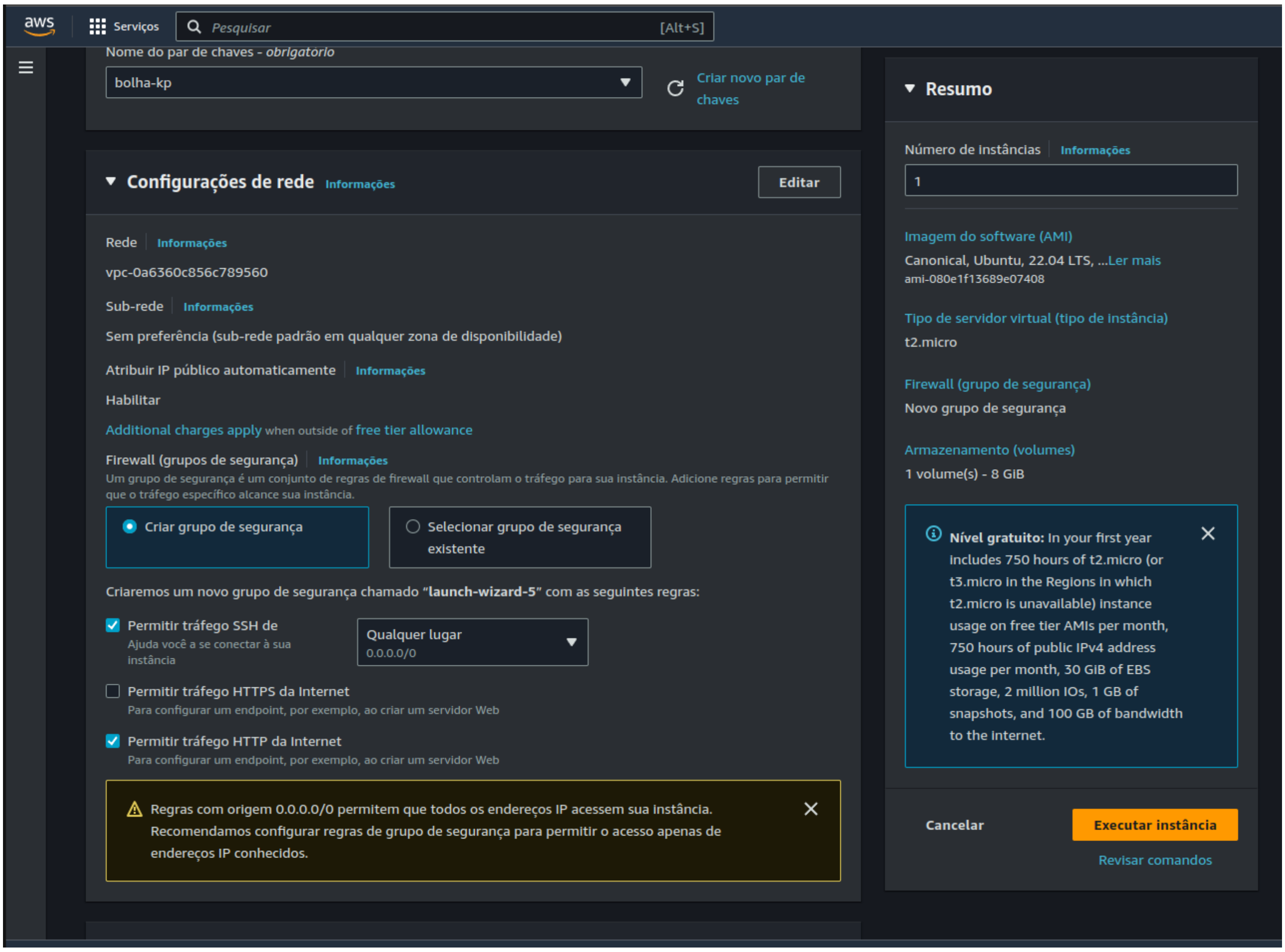
Formato de arquivo de chave privada

● .pem
Para uso com OpenSSH

○ .ppk
Para uso com PuTTY

⚠ Quando solicitado, armazene a chave privada em um local seguro e acessível no seu computador. **Você precisará dele mais tarde para se conectar à sua instância.** Saiba mais

Cancelar · Criar par de chaves



Nome do par de chaves - *obrigatório*

bolha-kp

Configurações de rede Informações

Rede | Informações

vpc-0a6360c856c789560

Sub-rede | Informações

Sem preferência (sub-rede padrão em qualquer zona de disponibilidade)

Atribuir IP público automaticamente | Informações

Habilitar

Additional charges apply when outside of free tier allowance

Firewall (grupos de segurança) | Informações

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

● Criar grupo de segurança ○ Selecionar grupo de segurança existente

Criaremos um novo grupo de segurança chamado "**launch-wizard-5**" com as seguintes regras:

☑ Permitir tráfego SSH de
Ajuda você a se conectar à sua instância
Qualquer lugar
0.0.0.0/0

□ Permitir tráfego HTTPS da Internet
Para configurar um endpoint, por exemplo, ao criar um servidor Web

☑ Permitir tráfego HTTP da Internet
Para configurar um endpoint, por exemplo, ao criar um servidor Web

⚠ Regras com origem 0.0.0.0/0 permitem que todos os endereços IP acessem sua instância. Recomendamos configurar regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos.

Resumo

Número de instâncias | Informações

1

Imagem do software (AMI)
Canonical, Ubuntu, 22.04 LTS, ...Ler mais
ami-080e1f13689e07408

Tipo de servidor virtual (tipo de instância)
t2.micro

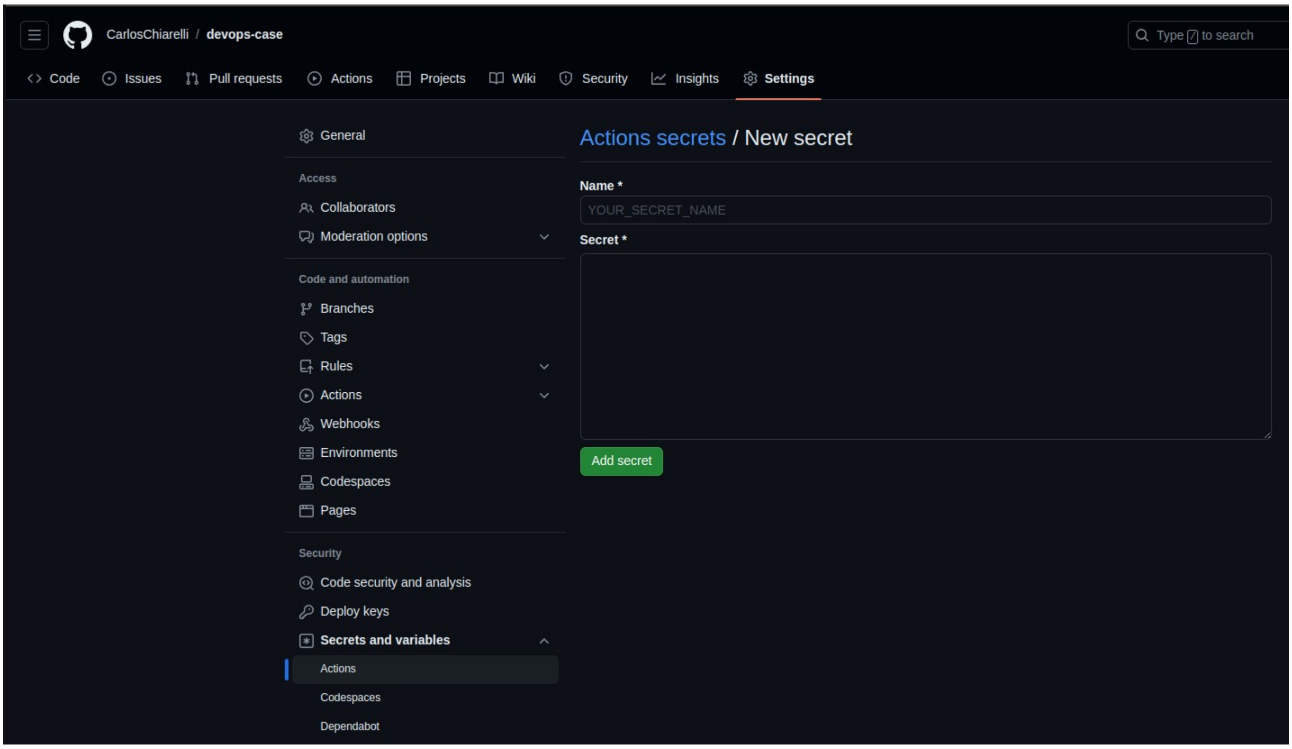
Firewall (grupo de segurança)
Novo grupo de segurança

Armazenamento (volumes)
1 volume(s) - 8 GiB

Nível gratuito: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Step 2: Create secrets in github for the repository

* EC2_SSH_KEY
* HOST_DNS
* USERNAME
* TARGET_DIR

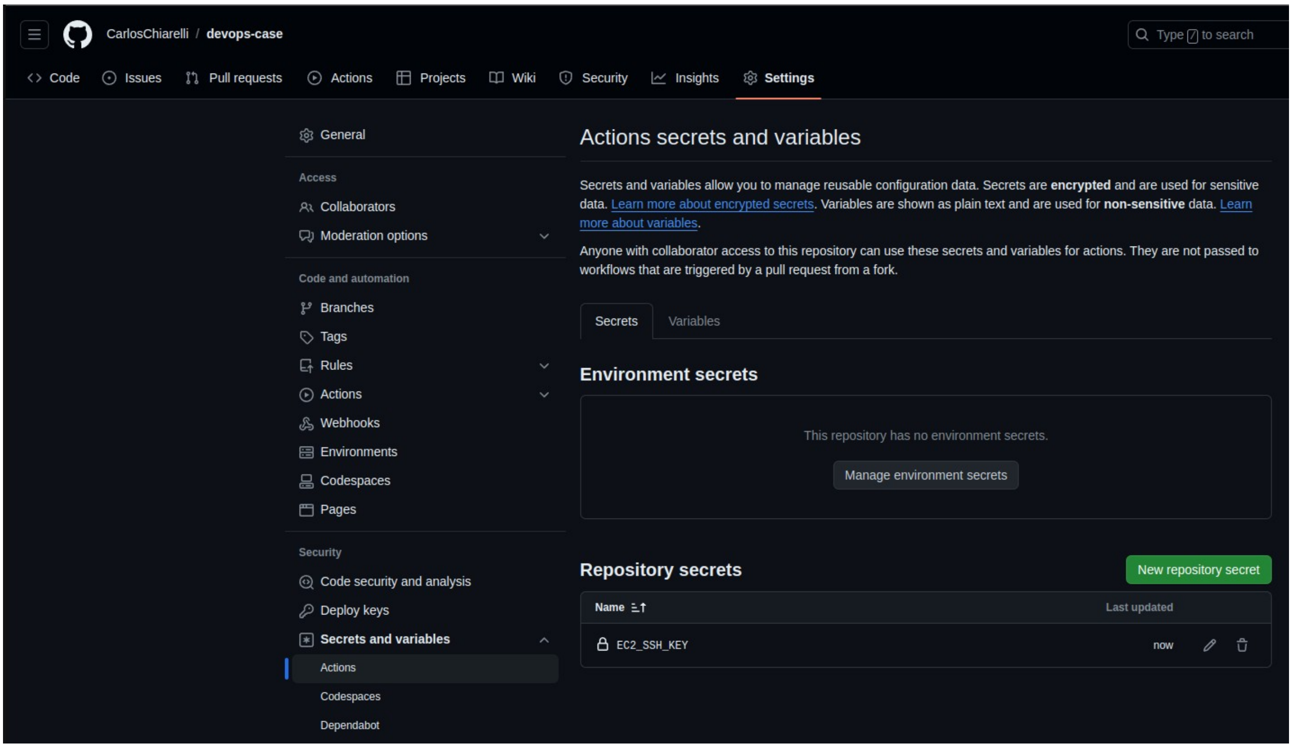


Actions secrets / New secret

Name *

YOUR_SECRET_NAME

Secret *



Actions secrets and variables

Secrets and variables allow you to manage reusable configuration data. Secrets are **encrypted** and are used for sensitive data. Learn more about encrypted secrets. Variables are shown as plain text and are used for **non-sensitive** data. Learn more about variables.

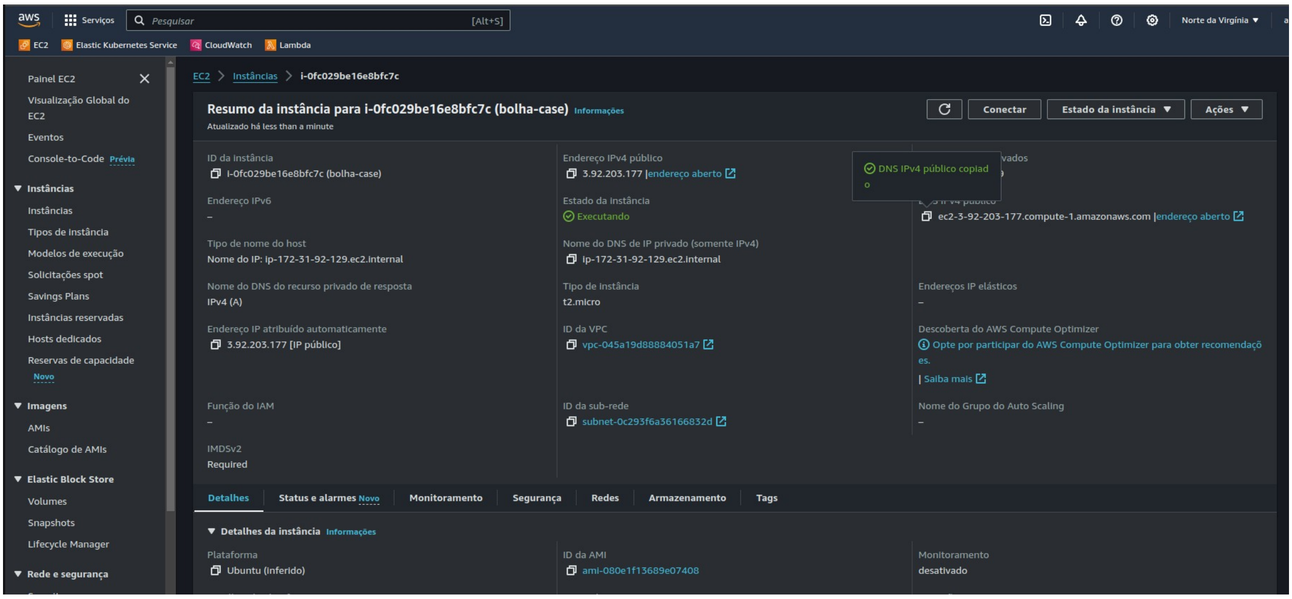
Anyone with collaborator access to this repository can use these secrets and variables for actions. They are not passed to workflows that are triggered by a pull request from a fork.

Environment secrets

This repository has no environment secrets.

Repository secrets

Name	Last updated
EC2_SSH_KEY	now



Resumo da instância para i-0fc029be16e8bfc7c (bolha-case) Informações

Atualizado há less than a minute

ID da instância
i-0fc029be16e8bfc7c (bolha-case)

Endereço IPv4 público
3.92.203.177 |endereço aberto

DNS IPv4 público copiado

Endereço IPv6
–

Estado da instância
Executando

DNS IPv4 público
ec2-3-92-203-177.compute-1.amazonaws.com |endereço aberto

Tipo de nome do host
Nome do IP: ip-172-31-92-129.ec2.internal

Nome do DNS de IP privado (somente IPv4)
ip-172-31-92-129.ec2.internal

Nome do DNS do recurso privado de resposta
IPv4 (A)

Tipo de instância
t2.micro

Endereços IP elásticos
–

Endereço IP atribuído automaticamente
3.92.203.177 [IP público]

ID da VPC
vpc-045a19d88884051a7

Descoberta do AWS Compute Optimizer
Opte por participar do AWS Compute Optimizer para obter recomendações. | Saiba mais

Função do IAM
–

ID da sub-rede
subnet-0c293f6a36166832d

Nome do Grupo do Auto Scaling
–

IMDSv2
Required

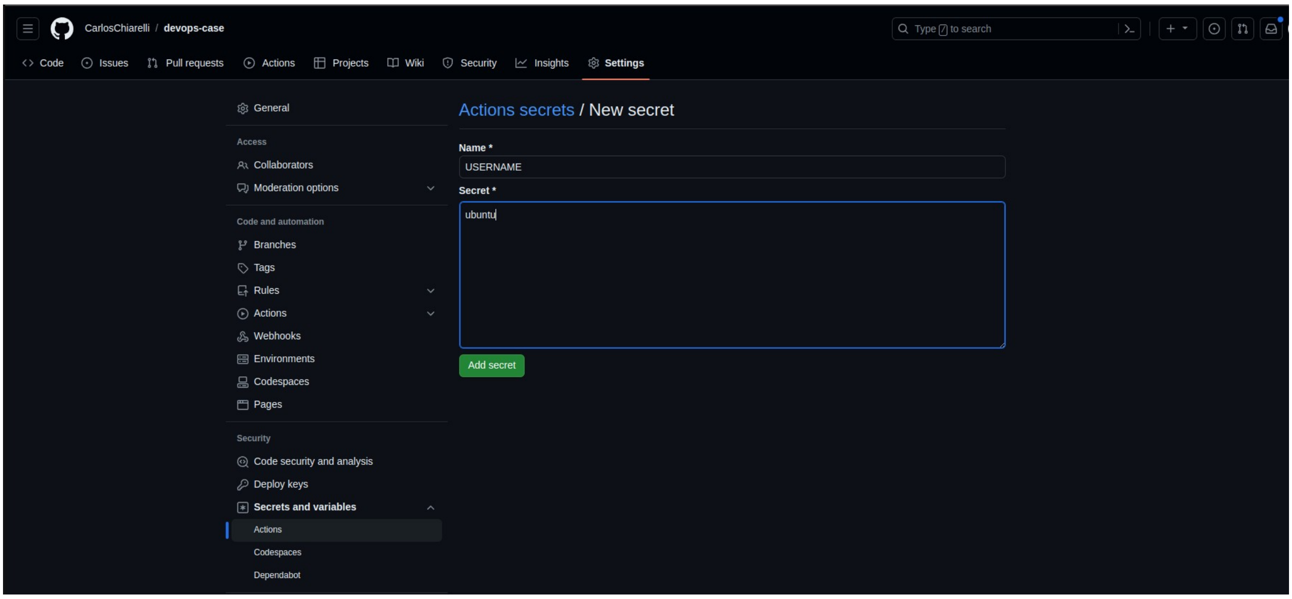
Detalhes da instância Informações

Plataforma
Ubuntu (Inferido)

ID da AMI
ami-080e1f13689e07408

Monitoramento
desativado

-

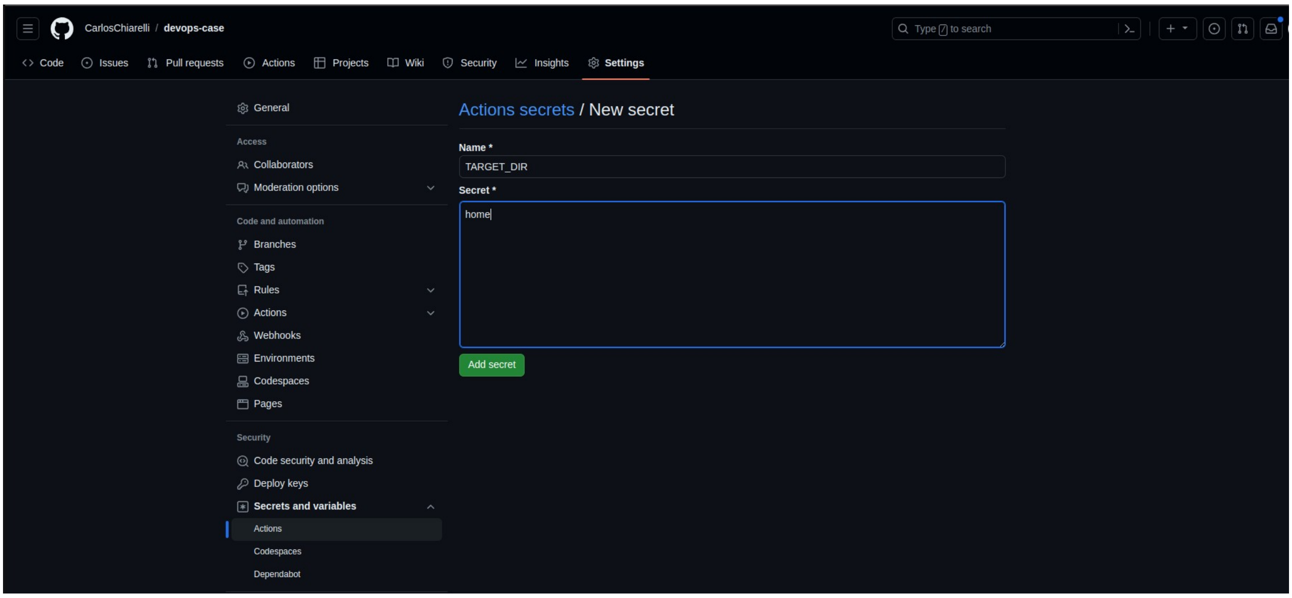


Actions secrets / New secret

Name *
USERNAME

Secret *
ubuntu

-



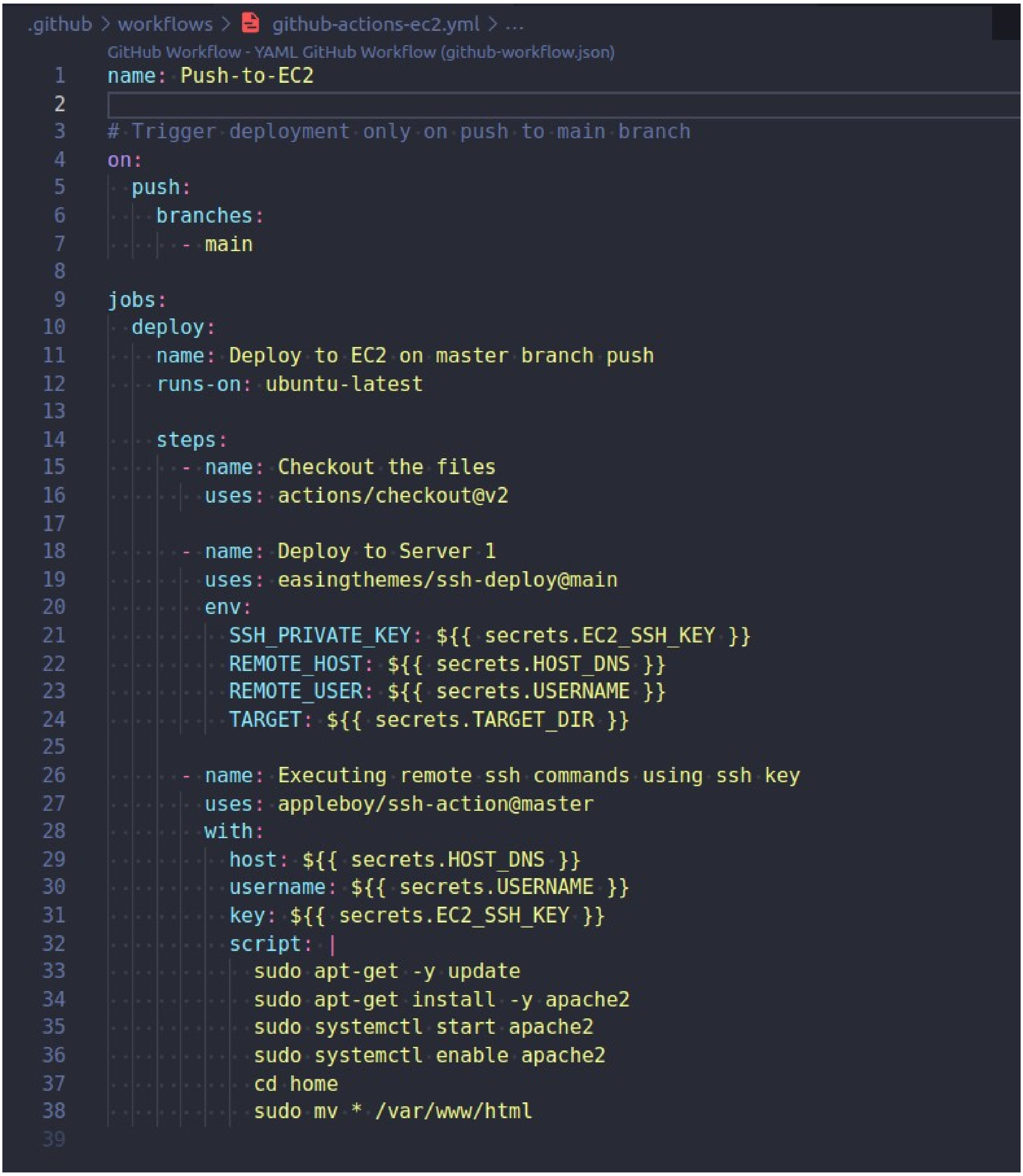
Actions secrets / New secret

Name *
TARGET_DIR

Secret *
home

-

Step 3: Creating workflow

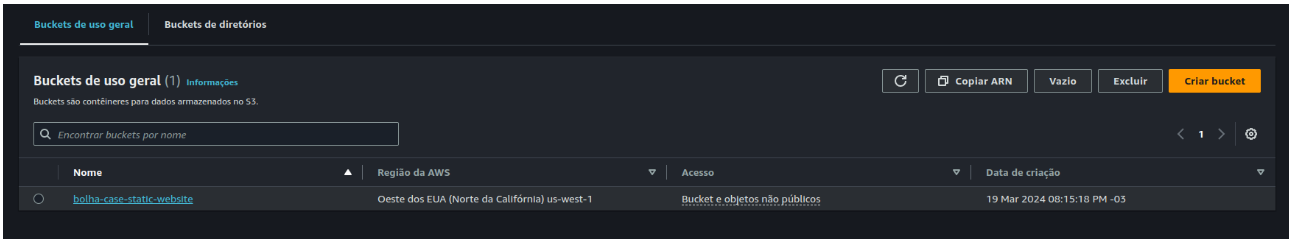

.github > workflows > github-actions-ec2.yml > ...
GitHub Workflow - YAML GitHub Workflow (github-workflow.json)

```yaml
name: Push-to-EC2

# Trigger deployment only on push to main branch
on:
  push:
    branches:
      - main

jobs:
  deploy:
    name: Deploy to EC2 on master branch push
    runs-on: ubuntu-latest

    steps:
      - name: Checkout the files
        uses: actions/checkout@v2

      - name: Deploy to Server 1
        uses: easingthemes/ssh-deploy@main
        env:
          SSH_PRIVATE_KEY: ${{ secrets.EC2_SSH_KEY }}
          REMOTE_HOST: ${{ secrets.HOST_DNS }}
          REMOTE_USER: ${{ secrets.USERNAME }}
          TARGET: ${{ secrets.TARGET_DIR }}

      - name: Executing remote ssh commands using ssh key
        uses: appleboy/ssh-action@master
        with:
          host: ${{ secrets.HOST_DNS }}
          username: ${{ secrets.USERNAME }}
          key: ${{ secrets.EC2_SSH_KEY }}
          script: |
            sudo apt-get -y update
            sudo apt-get install -y apache2
            sudo systemctl start apache2
            sudo systemctl enable apache2
            cd home
            sudo mv * /var/www/html
```

.

CI/CD to S3

Step 1: Create a S3 bucket



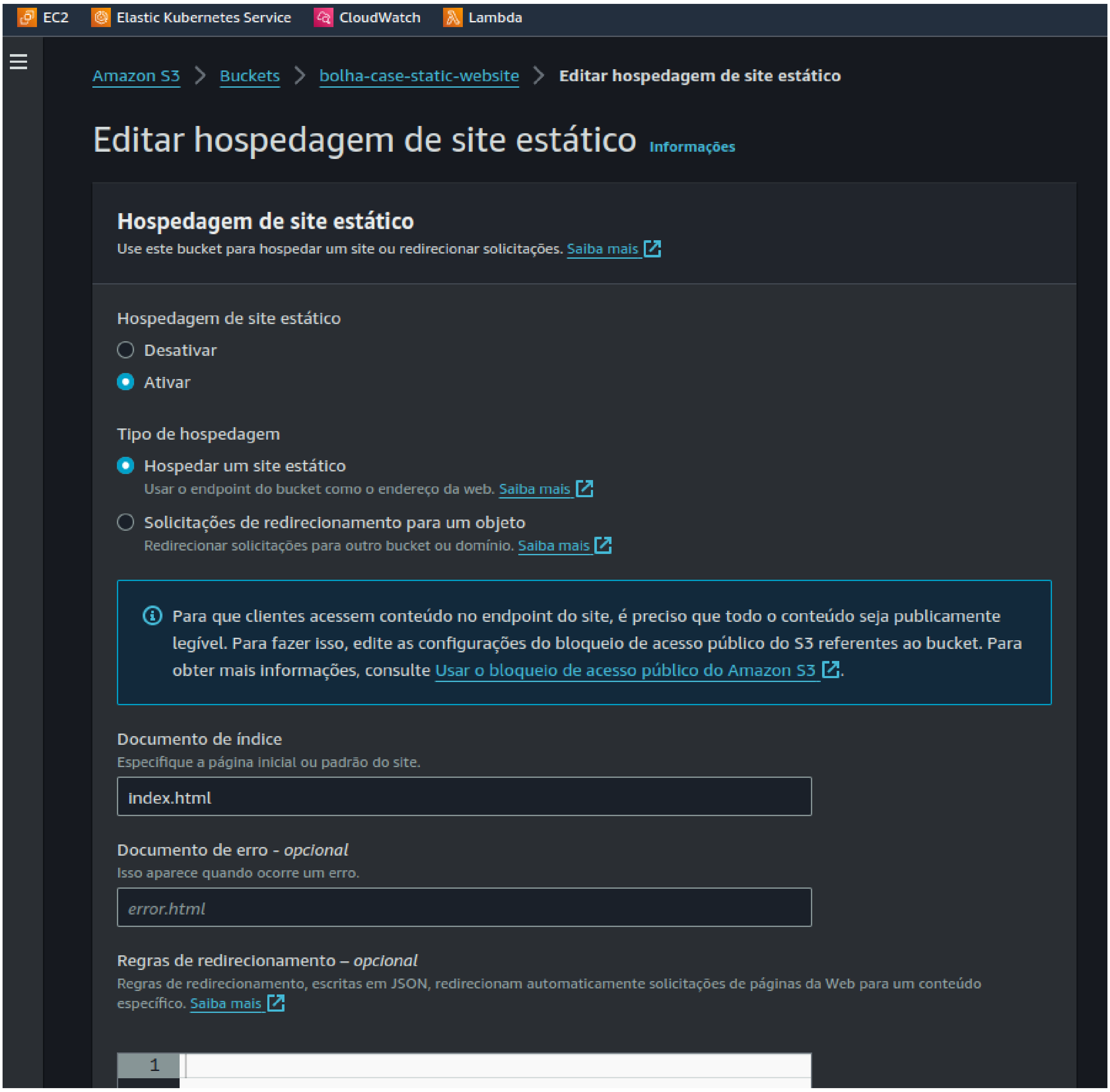
Buckets de uso geral (1) Informações

Buckets são contêineres para dados armazenados no S3.

Nome	Região da AWS	Acesso	Data de criação
○ bolha-case-static-website	Oeste dos EUA (Norte da Califórnia) us-west-1	Bucket e objetos não públicos	19 Mar 2024 08:15:18 PM -03

.

Step 2: Edit static website hosting


EC2
Elastic Kubernetes Service
CloudWatch
Lambda
Amazon S3 > Buckets > bolha-case-static-website > Editar hospedagem de site estático

Editar hospedagem de site estático Informações

Hospedagem de site estático

Use este bucket para hospedar um site ou redirecionar solicitações. Saiba mais

Hospedagem de site estático

○ Desativar

● Ativar

Tipo de hospedagem

● Hospedar um site estático

Usar o endpoint do bucket como o endereço da web. Saiba mais

○ Solicitações de redirecionamento para um objeto

Redirecionar solicitações para outro bucket ou domínio. Saiba mais

Para que clientes acessem conteúdo no endpoint do site, é preciso que todo o conteúdo seja publicamente legível. Para fazer isso, edite as configurações do bloqueio de acesso público do S3 referentes ao bucket. Para obter mais informações, consulte Usar o bloqueio de acesso público do Amazon S3.

Documento de índice

Especifique a página inicial ou padrão do site.

index.html

Documento de erro - *opcional*

Isso aparece quando ocorre um erro.

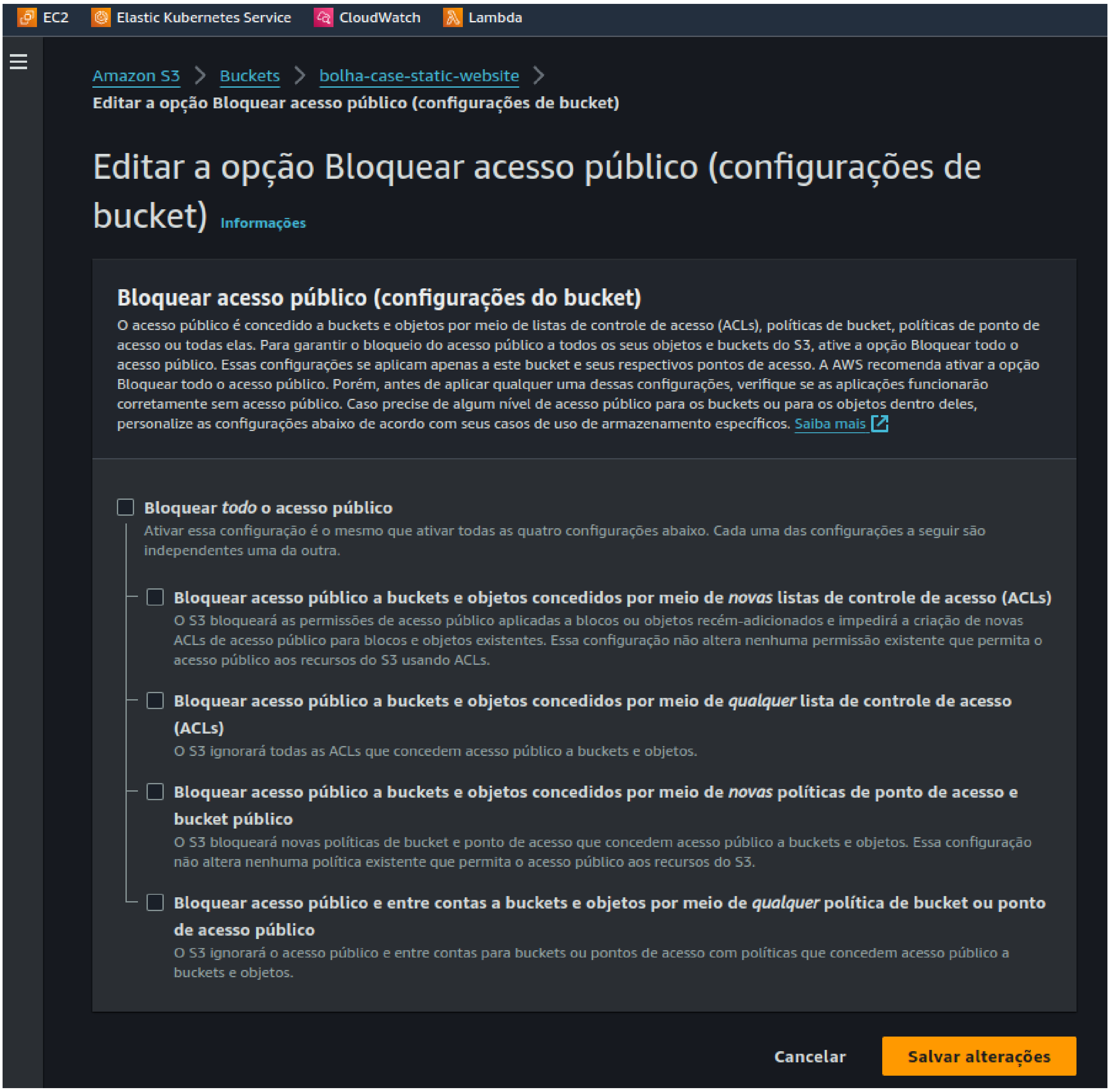
error.html

Regras de redirecionamento – *opcional*

Regras de redirecionamento, escritas em JSON, redirecionam automaticamente solicitações de páginas da Web para um conteúdo específico. Saiba mais

.

Step 3: Edit permissions



Editar a opção Bloquear acesso público (configurações de bucket)

Editar a opção Bloquear acesso público (configurações de bucket) Informações

Bloquear acesso público (configurações do bucket)

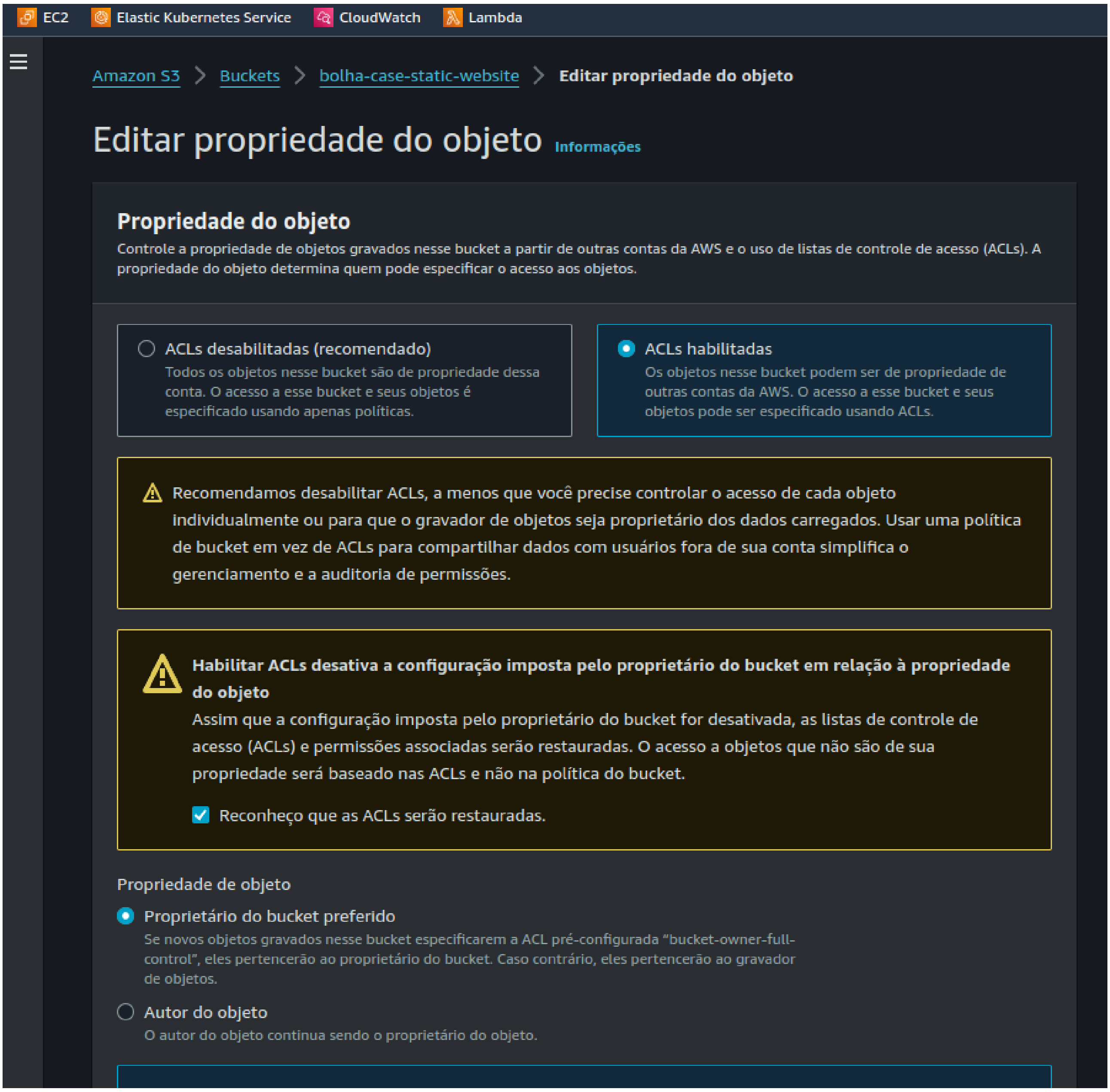
O acesso público é concedido a buckets e objetos por meio de listas de controle de acesso (ACLs), políticas de bucket, políticas de ponto de acesso ou todas elas. Para garantir o bloqueio do acesso público a todos os seus objetos e buckets do S3, ative a opção Bloquear todo o acesso público. Essas configurações se aplicam apenas a este bucket e seus respectivos pontos de acesso. A AWS recomenda ativar a opção Bloquear todo o acesso público. Porém, antes de aplicar qualquer uma dessas configurações, verifique se as aplicações funcionarão corretamente sem acesso público. Caso precise de algum nível de acesso público para os buckets ou para os objetos dentro deles, personalize as configurações abaixo de acordo com seus casos de uso de armazenamento específicos. Saiba mais

□ **Bloquear *todo* o acesso público**
Ativar essa configuração é o mesmo que ativar todas as quatro configurações abaixo. Cada uma das configurações a seguir são independentes uma da outra.

- □ **Bloquear acesso público a buckets e objetos concedidos por meio de *novas* listas de controle de acesso (ACLs)**
  O S3 bloqueará as permissões de acesso público aplicadas a blocos ou objetos recém-adicionados e impedirá a criação de novas ACLs de acesso público para blocos e objetos existentes. Essa configuração não altera nenhuma permissão existente que permita o acesso público aos recursos do S3 usando ACLs.
- □ **Bloquear acesso público a buckets e objetos concedidos por meio de *qualquer* lista de controle de acesso (ACLs)**
  O S3 ignorará todas as ACLs que concedem acesso público a buckets e objetos.
- □ **Bloquear acesso público a buckets e objetos concedidos por meio de *novas* políticas de ponto de acesso e bucket público**
  O S3 bloqueará novas políticas de bucket e ponto de acesso que concedem acesso público a buckets e objetos. Essa configuração não altera nenhuma política existente que permita o acesso público aos recursos do S3.
- □ **Bloquear acesso público e entre contas a buckets e objetos por meio de *qualquer* política de bucket ou ponto de acesso público**
  O S3 ignorará o acesso público e entre contas para buckets ou pontos de acesso com políticas que concedem acesso público a buckets e objetos.

.

Step 4: Edit object ownership


EC2
Elastic Kubernetes Service
CloudWatch
Lambda
Amazon S3 > Buckets > bolha-case-static-website > Editar propriedade do objeto
Informações

Editar propriedade do objeto

Propriedade do objeto

Controle a propriedade de objetos gravados nesse bucket a partir de outras contas da AWS e o uso de listas de controle de acesso (ACLs). A propriedade do objeto determina quem pode especificar o acesso aos objetos.

○ ACLs desabilitadas (recomendado)
Todos os objetos nesse bucket são de propriedade dessa conta. O acesso a esse bucket e seus objetos é especificado usando apenas políticas.

● ACLs habilitadas
Os objetos nesse bucket podem ser de propriedade de outras contas da AWS. O acesso a esse bucket e seus objetos pode ser especificado usando ACLs.

⚠ Recomendamos desabilitar ACLs, a menos que você precise controlar o acesso de cada objeto individualmente ou para que o gravador de objetos seja proprietário dos dados carregados. Usar uma política de bucket em vez de ACLs para compartilhar dados com usuários fora de sua conta simplifica o gerenciamento e a auditoria de permissões.

⚠ **Habilitar ACLs desativa a configuração imposta pelo proprietário do bucket em relação à propriedade do objeto**
Assim que a configuração imposta pelo proprietário do bucket for desativada, as listas de controle de acesso (ACLs) e permissões associadas serão restauradas. O acesso a objetos que não são de sua propriedade será baseado nas ACLs e não na política do bucket.

☑ Reconheço que as ACLs serão restauradas.

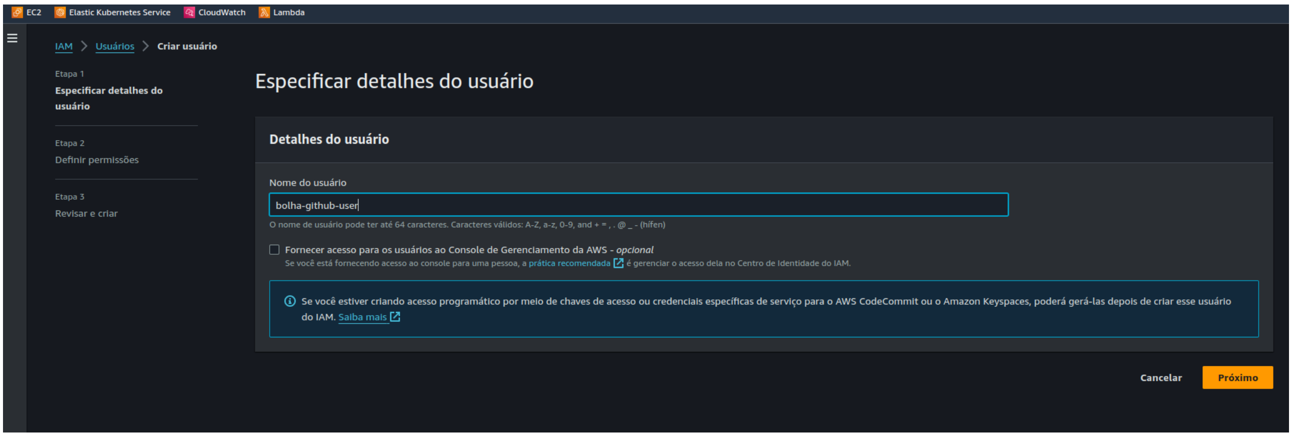
Propriedade de objeto

● Proprietário do bucket preferido
Se novos objetos gravados nesse bucket especificarem a ACL pré-configurada "bucket-owner-full-control", eles pertencerão ao proprietário do bucket. Caso contrário, eles pertencerão ao gravador de objetos.

○ Autor do objeto
O autor do objeto continua sendo o proprietário do objeto.

.

Step 5: Create user IAM



Especificar detalhes do usuário

Detalhes do usuário

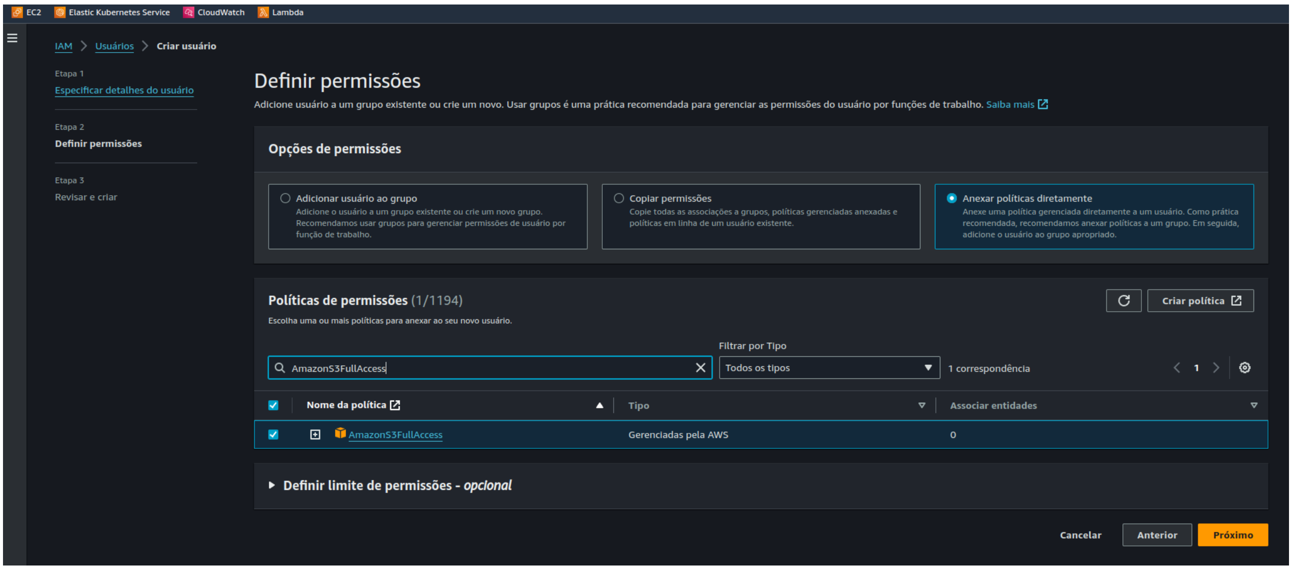
Nome do usuário: bolha-github-user

O nome de usuário pode ter até 64 caracteres. Caracteres válidos: A-Z, a-z, 0-9, and + = , . @ _ - (hífen)

□ Fornecer acesso para os usuários ao Console de Gerenciamento da AWS - *opcional*
Se você está fornecendo acesso ao console para uma pessoa, a prática recomendada é gerenciar o acesso dela no Centro de Identidade do IAM.

ⓘ Se você estiver criando acesso programático por meio de chaves de acesso ou credenciais específicas de serviço para o AWS CodeCommit ou o Amazon Keyspaces, poderá gerá-las depois de criar esse usuário do IAM. Saiba mais

.



Etapa 1
Especificar detalhes do usuário

Etapa 2
Definir permissões

Etapa 3
Revisar e criar

Definir permissões

Adicione usuário a um grupo existente ou crie um novo. Usar grupos é uma prática recomendada para gerenciar as permissões do usuário por funções de trabalho. Saiba mais

Opções de permissões

○ Adicionar usuário ao grupo
Adicione o usuário a um grupo existente ou crie um novo grupo. Recomendamos usar grupos para gerenciar permissões de usuário por função de trabalho.

○ Copiar permissões
Copie todas as associações a grupos, políticas gerenciadas anexadas e políticas em linha de um usuário existente.

● Anexar políticas diretamente
Anexe uma política gerenciada diretamente a um usuário. Como prática recomendada, recomendamos anexar políticas a um grupo. Em seguida, adicione o usuário ao grupo apropriado.

Políticas de permissões (1/1194)

Escolha uma ou mais políticas para anexar ao seu novo usuário.

AmazonS3FullAccess

Filtrar por Tipo: Todos os tipos

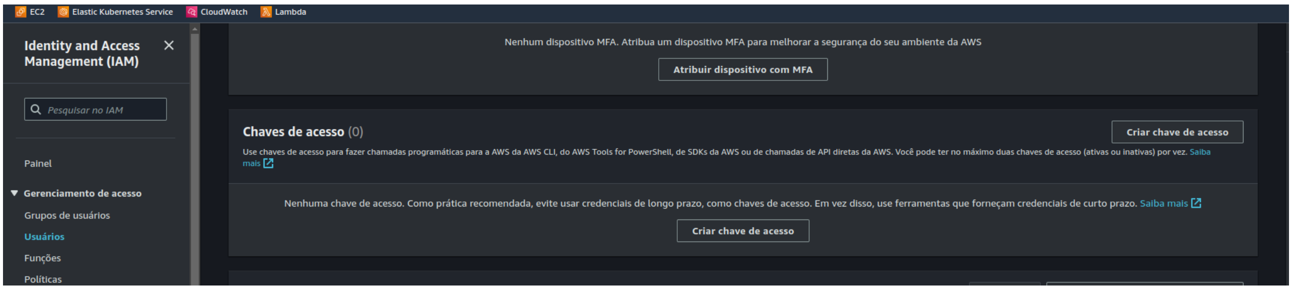
1 correspondência

☑	Nome da política	Tipo	Associar entidades
☑	AmazonS3FullAccess	Gerenciadas pela AWS	0

▸ Definir limite de permissões - *opcional*

•

Step 6: Create access key for new user



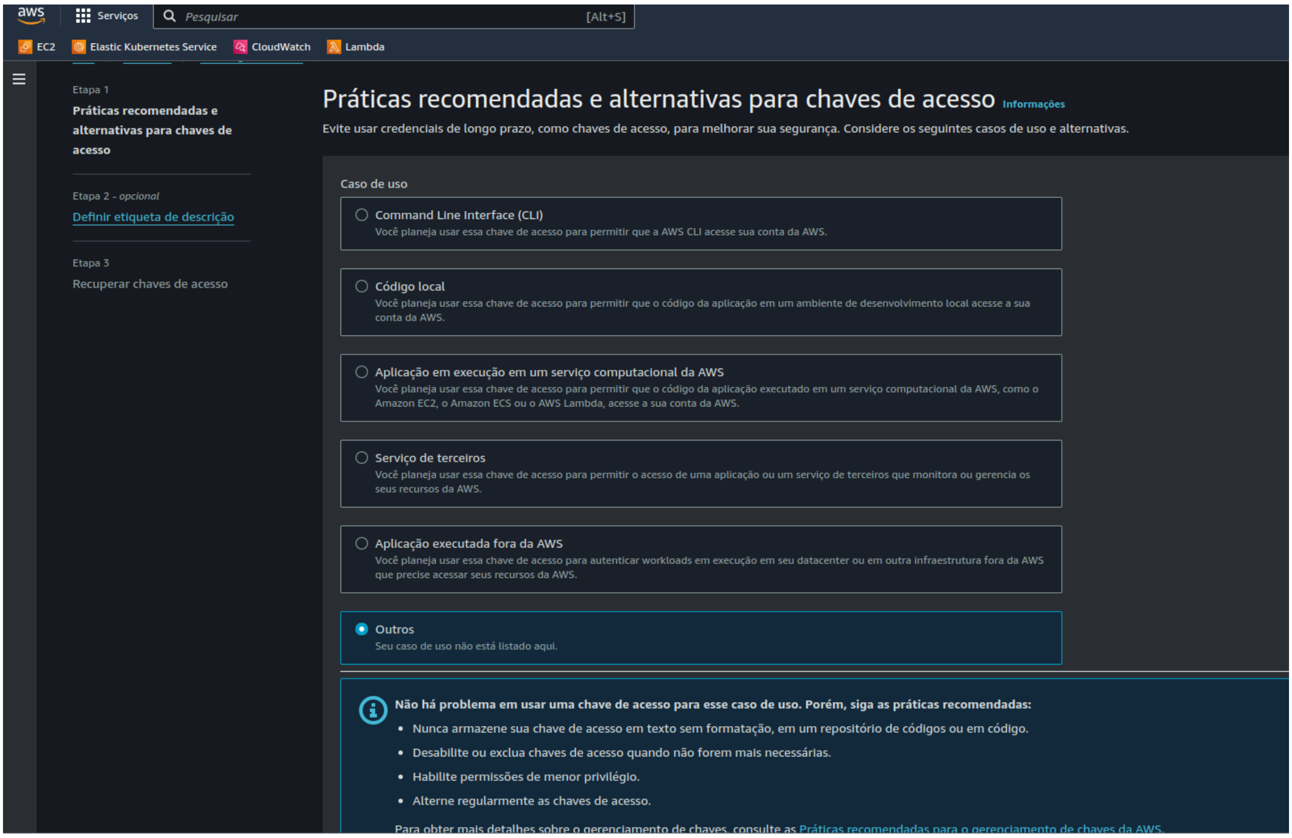
Nenhum dispositivo MFA. Atribua um dispositivo MFA para melhorar a segurança do seu ambiente da AWS

Chaves de acesso (0)

Use chaves de acesso para fazer chamadas programáticas para a AWS da AWS CLI, do AWS Tools for PowerShell, de SDKs da AWS ou de chamadas de API diretas da AWS. Você pode ter no máximo duas chaves de acesso (ativas ou inativas) por vez. Saiba mais

Nenhuma chave de acesso. Como prática recomendada, evite usar credenciais de longo prazo, como chaves de acesso. Em vez disso, use ferramentas que forneçam credenciais de curto prazo. Saiba mais

•



Etapa 1
Práticas recomendadas e alternativas para chaves de acesso

Etapa 2 - *opcional*
Definir etiqueta de descrição

Etapa 3
Recuperar chaves de acesso

Práticas recomendadas e alternativas para chaves de acesso

Evite usar credenciais de longo prazo, como chaves de acesso, para melhorar sua segurança. Considere os seguintes casos de uso e alternativas.

Caso de uso

○ Command Line Interface (CLI)
Você planeja usar essa chave de acesso para permitir que a AWS CLI acesse sua conta da AWS.

○ Código local
Você planeja usar essa chave de acesso para permitir que o código da aplicação em um ambiente de desenvolvimento local acesse a sua conta da AWS.

○ Aplicação em execução em um serviço computacional da AWS
Você planeja usar essa chave de acesso para permitir que o código da aplicação executado em um serviço computacional da AWS, como o Amazon EC2, o Amazon ECS ou o AWS Lambda, acesse a sua conta da AWS.

○ Serviço de terceiros
Você planeja usar essa chave de acesso para permitir o acesso de uma aplicação ou um serviço de terceiros que monitora ou gerencia os seus recursos da AWS.

○ Aplicação executada fora da AWS
Você planeja usar essa chave de acesso para autenticar workloads em execução em seu datacenter ou em outra infraestrutura fora da AWS que precise acessar seus recursos da AWS.

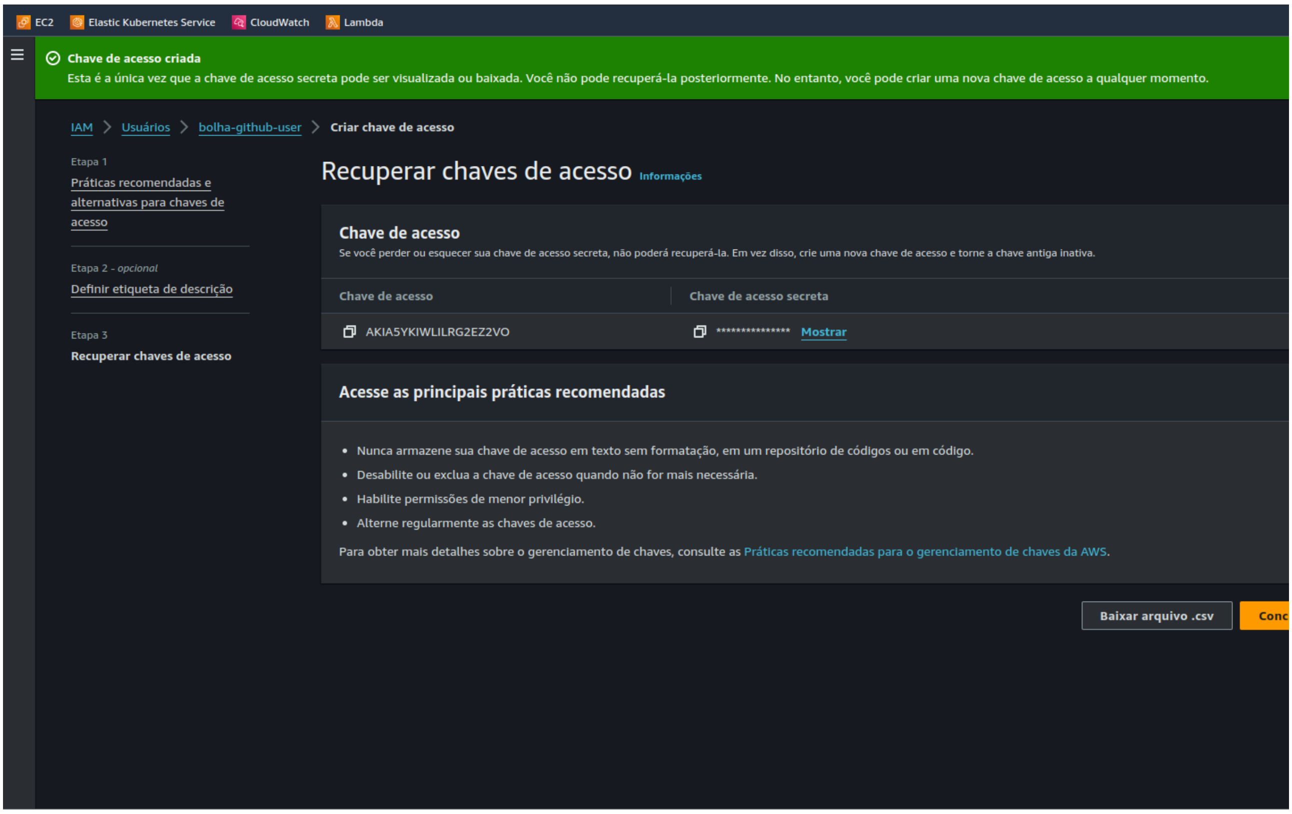
● Outros
Seu caso de uso não está listado aqui.

Não há problema em usar uma chave de acesso para esse caso de uso. Porém, siga as práticas recomendadas:

- Nunca armazene sua chave de acesso em texto sem formatação, em um repositório de códigos ou em código.
- Desabilite ou exclua chaves de acesso quando não forem mais necessárias.
- Habilite permissões de menor privilégio.
- Alterne regularmente as chaves de acesso.

Para obter mais detalhes sobre o gerenciamento de chaves, consulte as Práticas recomendadas para o gerenciamento de chaves da AWS.

•



Chave de acesso criada

Esta é a única vez que a chave de acesso secreta pode ser visualizada ou baixada. Você não pode recuperá-la posteriormente. No entanto, você pode criar uma nova chave de acesso a qualquer momento.

IAM > Usuários > bolha-github-user > Criar chave de acesso

Etapa 1
Práticas recomendadas e alternativas para chaves de acesso

Etapa 2 - *opcional*
Definir etiqueta de descrição

Etapa 3
Recuperar chaves de acesso

Recuperar chaves de acesso Informações

Chave de acesso

Se você perder ou esquecer sua chave de acesso secreta, não poderá recuperá-la. Em vez disso, crie uma nova chave de acesso e torne a chave antiga inativa.

Chave de acesso	Chave de acesso secreta
AKIA5YKIWLILRG2EZ2VO	*************** Mostrar

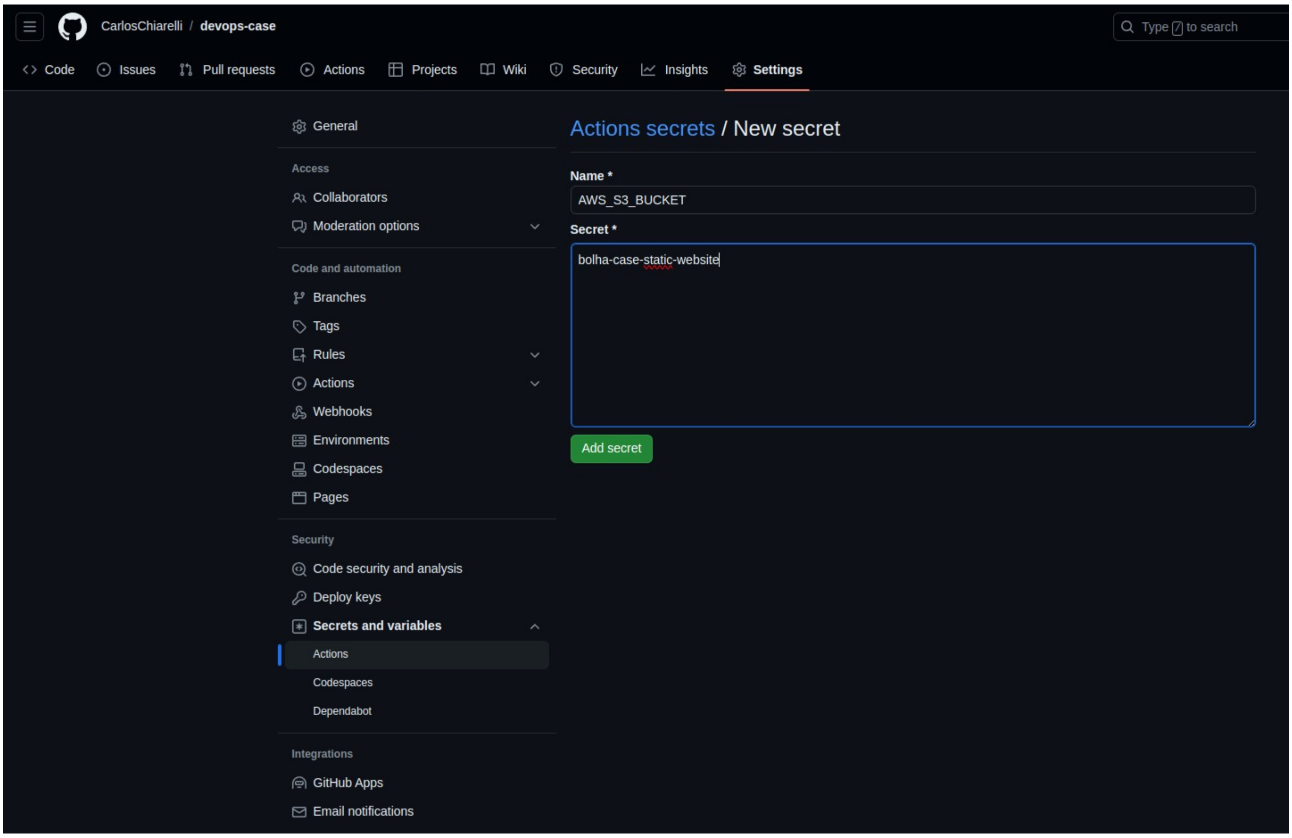
Acesse as principais práticas recomendadas

- Nunca armazene sua chave de acesso em texto sem formatação, em um repositório de códigos ou em código.
- Desabilite ou exclua a chave de acesso quando não for mais necessária.
- Habilite permissões de menor privilégio.
- Alterne regularmente as chaves de acesso.

Para obter mais detalhes sobre o gerenciamento de chaves, consulte as Práticas recomendadas para o gerenciamento de chaves da AWS.

Step 7: Create secrets in github

* AWS_S3_BUCKET
* AWS_ACCESS_KEY_ID
* AWS_SECRET_ACCESS_KEY
* AWS_REGION
* SOURCE_DIR



Actions secrets / New secret

Name *

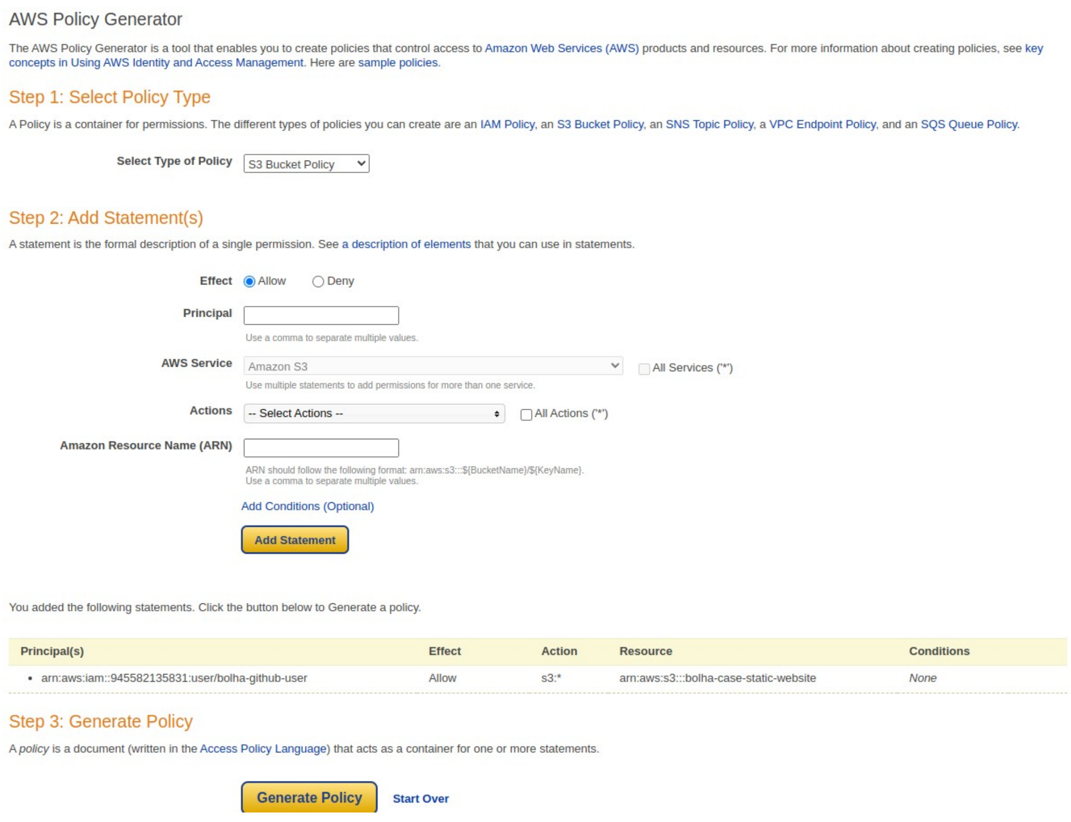
AWS_S3_BUCKET

Secret *

bolha-case-static-website

•

Step 8: Edit policy bucket



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect: ● Allow ○ Deny

Principal:

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions: -- Select Actions -- □ All Actions ('*')

Amazon Resource Name (ARN):

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

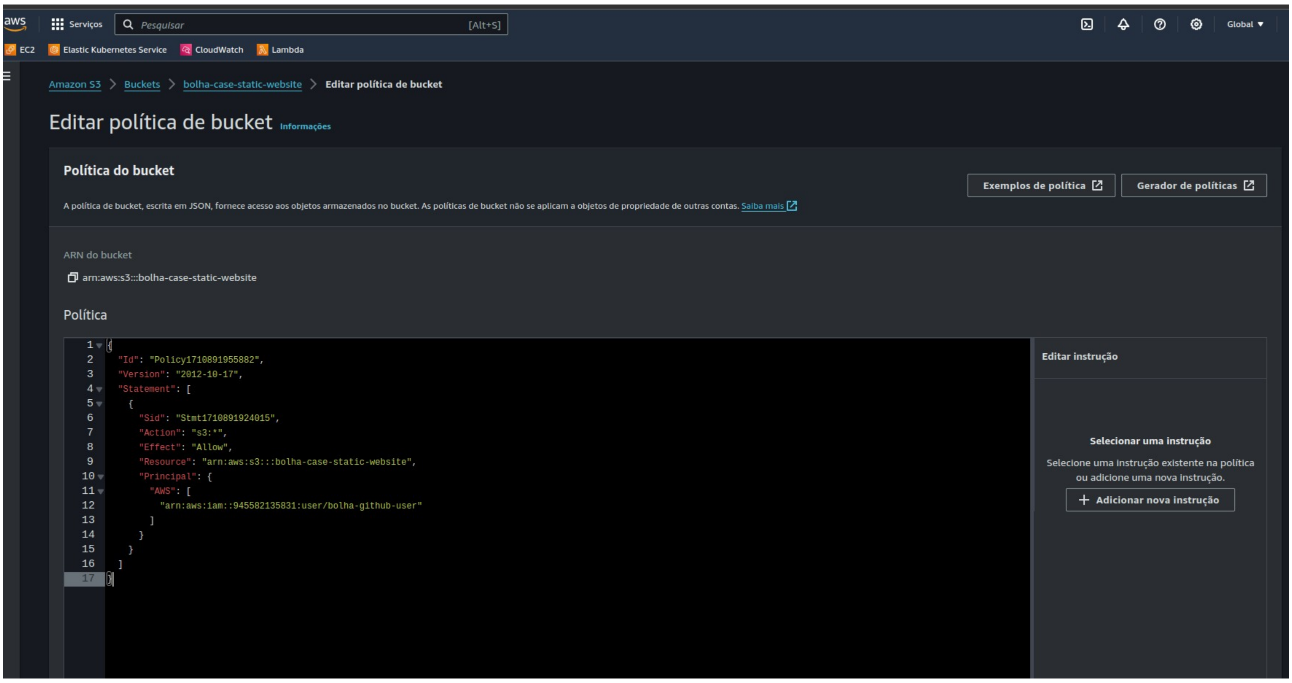
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• arn:aws:iam::945582135831:user/bolha-github-user	Allow	s3:*	arn:aws:s3:::bolha-case-static-website	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

•



aws
Serviços
Pesquisar
[Alt+S]
Global
EC2
Elastic Kubernetes Service
CloudWatch
Lambda
Amazon S3 > Buckets > bolha-case-static-website > Editar política de bucket

Editar política de bucket Informações

Política do bucket

Exemplos de política
Gerador de políticas

A política de bucket, escrita em JSON, fornece acesso aos objetos armazenados no bucket. As políticas de bucket não se aplicam a objetos de propriedade de outras contas. Saiba mais

ARN do bucket

arn:aws:s3:::bolha-case-static-website

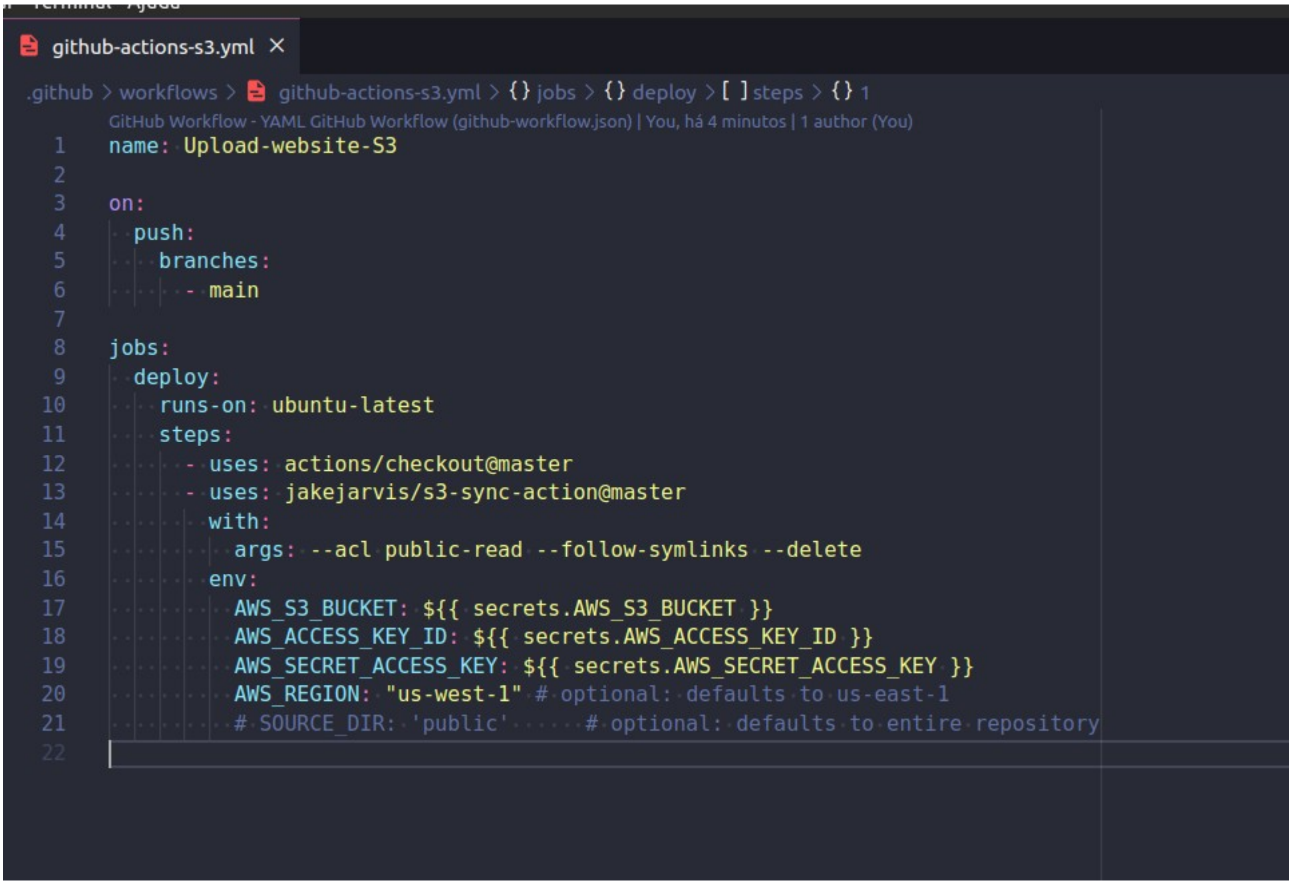
Política

```json
{
  "Id": "Policy1710891955882",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1710891924015",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bolha-case-static-website",
      "Principal": {
        "AWS": [
          "arn:aws:iam::945582135831:user/bolha-github-user"
        ]
      }
    }
  ]
}
```

Editar instrução
Selecionar uma instrução
Selecione uma instrução existente na política ou adicione uma nova instrução.
+ Adicionar nova instrução

.

Step 9: Creating workflow



Terminal Ajuda
github-actions-s3.yml ×
.github > workflows > github-actions-s3.yml > {} jobs > {} deploy > [ ] steps > {} 1
GitHub Workflow - YAML GitHub Workflow (github-workflow.json) | You, há 4 minutos | 1 author (You)

```yaml
name: Upload-website-S3

on:
  push:
    branches:
      - main

jobs:
  deploy:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@master
      - uses: jakejarvis/s3-sync-action@master
        with:
          args: --acl public-read --follow-symlinks --delete
        env:
          AWS_S3_BUCKET: ${{ secrets.AWS_S3_BUCKET }}
          AWS_ACCESS_KEY_ID: ${{ secrets.AWS_ACCESS_KEY_ID }}
          AWS_SECRET_ACCESS_KEY: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
          AWS_REGION: "us-west-1" # optional: defaults to us-east-1
          # SOURCE_DIR: 'public'      # optional: defaults to entire repository
```